

Briselē, 21.4.2021.
COM(2021) 206 final

2021/0106 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

**KAS NOSAKA SASKAŅOTAS NORMAS MĀKSLĪGĀ INTELEKTA JOMĀ
(MĀKSLĪGĀ INTELEKTA AKTS) UN GROZA DAŽUS SAVIENĪBAS
LĒGISLATĪVOS AKTUS**

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

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

1.1. Priekšlikuma pamatojums un mērķi

Šis paskaidrojuma raksts ir pievienots regulas priekšlikumam, kas nosaka saskaņotus noteikumus mākslīgā intelekta jomā (Mākslīgā intelekta akts). Mākslīgais intelekts ("AI", arī "MI") ir tehnoloģiju saime, kas strauji attīstās un var dot visdažādāko saimniecisko un sabiedrisko ieguvumu visās nozarēs un sabiedriskās darbībās. Uzlabojot prognozēšanas spēju, optimalizējot darbības un resursu sadali un personalizējot pakalpojumu sniegšanu, mākslīgā intelekta izmantošana var sekmēt sabiedrībai un videi labvēlīgus rezultātus un sagādāt būtiskas konkurences priekšrocības uzņēmumiem un Eiropas ekonomikai. Tāda rīcība ir sevišķi nepieciešama jomās, kurām ir liela ietekme, ieskaitot klimata pārmaiņu, vides un veselības jomu, publisko sektoru, finanses, mobilitāti, iekšlietas un lauksaimniecību. Tomēr tie paši elementi un metodes, kas nodrošina AI nesto sociālekonomisko ieguvumu, var radīt arī jaunu risku vai negatīvas sekas indivīdiem vai sabiedrībai. Ņemot vērā tehnoloģisko pārmaiņu straujumu un iespējamās problēmas, ES ir pilna apņēmības cēsties nodrošināt līdzsvarotu pieeju. Savienības interesēs ir saglabāt ES vadošo pozīciju tehnoloģiju jomā un nodrošināt to, ka Eiropas iedzīvotāji var gūt labumu no jaunām tehnoloģijām, kas izstrādātas un darbojas saskaņā ar Savienības vērtībām, pamattiesībām un principiem.

Šis priekšlikums īsteno priekšsēdētājas fon der Leienas politisko apņemšanos, kas pausta viņas politikas pamatnostādņēs Komisijai (2019.–2024. gadam) "Eiropas Savienība, kas tiecas uz augstākiem mērķiem"¹, kurās viņa paziņoja, ka Komisija ierosinās tiesību aktu priekšlikumus par koordinētu Eiropas pieeju attiecībā uz AI ietekmi uz cilvēkiem un ētiskajiem aspektiem. Pamatojoties uz minēto paziņojumu, 2020. gada 19. februārī Komisija publicēja "Balto grāmatu par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās"². Baltajā grāmatā ir aprakstīti politiskie risinājumi, kā sasniegt divējādu mērķi – veicināt AI ieviešanu un novērst briesmas, kas saistītas ar dažiem šo tehnoloģiju lietojumiem. Šis priekšlikums tiecas īstenot otro mērķi uzticības pilnas ekosistēmas radīšanai, ierosinot tiesisko regulējumu uzticamam AI. Priekšlikums ir balstīts uz ES vērtībām un pamattiesībām, un tā nolūks ir sniegt indivīdiem un citiem lietotājiem pārliecību, kas nepieciešama uz AI balstītu risinājumu pieņemšanai, un vienlaikus mudināt uzņēmumus šādus risinājumus izstrādāt. AI vajadzētu būt cilvēkiem domātam instrumentam un labā virzītājspēkam sabiedrībā, kura galvenais mērķis ir vairogt cilvēku labklājību. Tāpēc, lai cilvēki varētu būt pārliecināti, ka AI tehnoloģija tiek izmantota drošā veidā un saskaņā ar tiesību aktiem, ieskaitot pamattiesību ievērošanu, noteikumiem attiecībā uz AI risinājumiem, kas pieejami Savienības tirgū vai kā citādi ietekmē Savienības iedzīvotājus, vajadzētu būt orientētiem uz cilvēkiem. Pēc baltās grāmatas publicēšanas Komisija sāka plašu apspriešanos ar ieinteresētajām personām, un tā izraisīja lielu interesi daudzās ieinteresētajās personās, kuras lielākoties atbalstīja regulatīvu iejaukšanos ar mērķi risināt problēmas un bažas, ko izraisa arvien pieaugošā AI izmantošana.

Priekšlikums arī reaģē uz skaidriem Eiropas Parlamenta (EP) un Eiropadomes lūgumiem; abas iestādes ir vairākkārt atkārtājušas aicinājumu pieņemt tiesību aktus, lai nodrošinātu tādu labi funkcionējošu iekšējo tirgu mākslīgā intelekta sistēmām ("AI sistēmas"), kurā gan AI radītie ieguvumi, gan riski ir adekvāti risināti Savienības līmenī. Tas atbalsta Eiropadomes

¹ https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_lv.pdf.

² Eiropas Komisija (2020), "Baltā grāmata par mākslīgo intelektu. Eiropiska pieeja – izcilība un uzticēšanās", COM(2020) 65 final.

nosprausto mērķi³ – Savienībai būt pasaules līderei droša, uzticama un ētiska mākslīgā intelekta attīstīšanā – un nodrošina ētikas principu aizsardzību, kā īpaši lūdzis Eiropas Parlaments⁴.

2017. gadā Eiropadome puda pārliecību, ka “ir steidzami jāpievēršas jaunām tendencēm,” ieskaitot “tādus jautājumus kā mākslīgā intelekta .. tehnoloģijas, vienlaikus nodrošinot augstu datu aizsardzības, digitālo tiesību un ētikas normu līmeni”⁵. Turklāt 2019. gada secinājumos par koordinēto Eiropā radīta mākslīgā intelekta izstrādes un izmantošanas plānu⁶ Padome uzsvēra, cik svarīgi ir nodrošināt Eiropas pilsoņu tiesību pilnīgu ievērošanu, un aicināja pārskatīt esošos attiecīgos tiesību aktus, lai nodrošinātu, ka tie atbilst mērķim – izmantot AI radītās jaunās iespējas un risināt ar to saistītās problēmas. Eiropadome ir arī aicinājusi skaidri definēt mākslīgā intelekta lietojumus, kas būtu uzskatāmi par augsta riska lietojumiem⁷.

Jaunākajos 2020. gada 21. oktobra secinājumos aicināts risināt tādas problēmas kā nepārredzamība, sarežģītība, aizspriedumi, zināma neprognozējamības pakāpe un dažu AI sistēmu daļēji autonoma darbība, lai nodrošinātu šo sistēmu saderību ar pamattiesībām un atvieglotu tiesību normu izpildi⁸.

Arī Eiropas Parlaments ir veicis ievērojamu darbu AI jomā. 2020. gada oktobrī tas pieņēma vairākas ar AI saistītas rezolūcijas, tostarp par ētiku⁹, atbildību¹⁰ un autortiesībām¹¹. 2021. gadā tām sekoja rezolūcijas par AI krimināllietās¹² un izglītībā, kultūrā un audiovizuālajā nozarē¹³. EP rezolūcijā par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru ir īpaši ieteikts Komisijai ierosināt tiesību aktus AI piedāvāto iespēju un ieguvumu izmantošanai, bet arī ētisko principu aizsardzības nodrošināšanai. Rezolūcija satur tiesību akta priekšlikuma tekstu regulai par AI, robotikas un ar to saistīto tehnoloģiju izstrādes, ieviešanas un izmantošanas ētikas principiem. Attiecībā uz Eiropas Parlamenta rezolūcijām, kas pieņemtas saskaņā ar LESD 225. pantu, saskaņā ar Komisijas priekšsēdētājas fon der Leienas politisko apņemšanos, kas pausta viņas politikas pamatnostādnēs, šajā

³ Eiropadome (2020), [Eiropadomes ārkārtas sanāksme \(2020. gada 1. un 2. oktobrī\) – secinājumi](#), EUCO 13/20, 6. lpp.

⁴ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un [ar tiem] saistīto tehnoloģiju ētisko aspektu satvaru, 2020/2012(INL).

⁵ Eiropadome (2017), [Eiropadomes sanāksme \(2017. gada 19. oktobrī\) – secinājumi](#), EUCO 14/17, 8. lpp.

⁶ Eiropas Savienības Padome (2019), [Mākslīgais intelekts. b\) Secinājumi par koordinēto mākslīgā intelekta plānu – pieņemšana](#), 6177/19.

⁷ Eiropadome (2020), [Eiropadomes ārkārtas sanāksme \(2020. gada 1. un 2. oktobrī\) – secinājumi](#), EUCO 13/20.

⁸ Eiropas Savienības Padome (2020), [Prezidentvalsts secinājumi – Pamattiesību harta saistībā ar mākslīgo intelektu un digitālajām pārmaiņām](#), 11481/20.

⁹ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru, [2020/2012\(INL\)](#).

¹⁰ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgajam intelektam piemērojamo civiltiesiskās atbildības režīmu, [2020/2014\(INL\)](#).

¹¹ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija par intelektuālā īpašuma tiesībām saistībā ar mākslīgā intelekta tehnoloģiju attīstību, [2020/2015\(INI\)](#).

¹² Eiropas Parlamenta ziņojuma projekts par mākslīgo intelektu krimināltiesībās un policijas un tiesu iestāžu īstenoto mākslīgā intelekta izmantošanu krimināllietās, [2020/2016\(INI\)](#).

¹³ Eiropas Parlamenta ziņojuma projekts par mākslīgo intelektu izglītības, kultūras un audiovizuālajā nozarē, [2020/2017\(INI\)](#). Šajā ziņā Komisija pieņēma Digitālās izglītības rīcības plānu 2021.–2027. gadam “Izglītības un apmācības pārveide digitālajam laikmetam”, kura ietvaros paredzēts izstrādāt ētikas pamatnostādnēs par AI un datu izmantošanu izglītībā (Komisijas paziņojums COM(2020) 624 final).

priekšlikumā ņemta vērā iepriekš minētā Eiropas Parlamenta rezolūcija, pilnīgi ievērojot proporcionalitātes, subsidiaritātes un labāka regulējuma principus.

Šajā politiskajā kontekstā Komisija ierosina mākslīgā intelekta tiesisko regulējumu ar šādiem **specifiskiem mērķiem**:

- nodrošināt, ka Savienības tirgū laistās un izmantotās AI sistēmas ir drošas un atbilst pašreizējiem tiesību aktiem par pamattiesībām un Savienības vērtībām,
- nodrošināt juridisko noteiktību, lai veicinātu ieguldījumus AI un ar to saistītu inovāciju,
- uzlabot pārvaldi un to pašreizējo AI sistēmām piemērojamo tiesību aktu efektīvu izpildi, kuros noteiktas pamattiesības un drošuma prasības,
- veicināt vienota tirgus attīstību likumīgiem, drošiem un uzticamiem AI lietojumiem un novērst tirgus sadrumstalotību.

Lai sasniegtu minētos mērķus, šis priekšlikums piedāvā līdzsvarotu un samērīgu horizontālu pieeju AI regulējumam, kas aprobežojas ar minimālajām nepieciešamajām prasībām ar AI saistīto risku un problēmu risināšanai, nepamatoti neierobežojot un nekavējot tehnoloģiju attīstību un citādā veidā nesamērīgi nepaaugstinot AI risinājumu tirgū laišanas izmaksas. Priekšlikums nosaka grodu un elastīgu tiesisko regulējumu. No vienas puses, tas ir vispusīgs un nākotnes prasībām atbilstošs regulatīvajās pamata izvēlēs, tostarp uz principiem pamatotajās prasībās, kas AI sistēmām ir jāizpilda. No otras puses, tas iedibina samērīgu regulatīvo sistēmu, kas centrēta uz skaidri noteiktu, uz risku balstītu regulatīvo pieeju, kura nerada liekus tirdzniecības ierobežojumus un kurā juridiska iejaukšanās ir pielāgota konkrētajām situācijām, kurās ir skaidrs pamats bažām vai ir paredzams, ka bažas radīsies tuvākajā nākotnē. Tajā pašā laikā tiesiskajā regulējumā iekļauti elastīgi mehānismi, kuri ļauj to dinamiski pielāgot tehnoloģiju attīstībai un jaunām situācijām, kam jāpievēršas.

Priekšlikums nosaka saskaņotus noteikumus AI sistēmu izstrādei, laišanai tirgū un izmantošanai Savienībā saskaņā ar samērīgu, uz risku balstītu pieeju. Tas ierosina vienotu, nākotnes prasībām atbilstošu AI definīciju. Dažu veidu īpaši kaitīga AI prakse tiek aizliegta, jo tā pārkāpj Savienības vērtības, bet saistībā ar dažiem biometriskās tālidentifikācijas sistēmu lietojumiem tiesībaizsardzībā tiek ierosināti noteikti ierobežojumi un aizsardzības pasākumi. Priekšlikumā noteikta stingra metodika tādu “augsta riska” AI sistēmu definēšanai, kuras rada ievērojamus riskus personu veselībai un drošībai vai pamattiesībām. Tādām AI sistēmām būs jāatbilst obligātu horizontālo uzticama AI prasību kopai un jāizpilda atbilstības novērtēšanas procedūras, pirms šīs sistēmas varēs laist Savienības tirgū. Paredzami, samērīgi un skaidri pienākumi tiek noteikti arī minēto sistēmu sagādātājiem un lietotājiem ar mērķi garantēt drošību un esošo ar pamattiesību aizsardzību saistīto tiesību aktu ievērošanu visā AI sistēmu darbībā. Dažām specifiskām AI sistēmām ir ierosinātas tikai minimālās pārredzamības prasības, it īpaši sarunbotu vai dziļviltojumu izmantošanā.

Ierosinātie noteikumi tiks izpildīti caur dalībvalstu līmeņa pārvaldes sistēmu, balstoties uz jau pastāvošajām struktūrām, un sadarbības mehānismu Savienības līmenī, izveidojot Eiropas Mākslīgā intelekta padomi. Ierosināti arī papildu pasākumi inovācijas atbalstam, sevišķi AI “regulatīvās smilškastēs” un citi pasākumi regulatīvā sloga mazināšanai un mazo un vidējo uzņēmumu (MVU) un jaunuzņēmumu atbalstam.

1.2. Saskaņība ar attiecīgajā politikas jomā pastāvošajiem noteikumiem

Priekšlikuma horizontālajam raksturam nepieciešama pilnīga saskaņība ar esošajiem Savienības tiesību aktiem, kuri attiecas uz nozarēm, kurās jau izmanto augsta riska AI sistēmas vai paredzams, ka izmantos tās tuvākajā nākotnē.

Ir nodrošināta saskanība arī ES Pamattiesību hartu un esošajiem sekundārajiem Savienības tiesību aktiem datu aizsardzības, patērētāju tiesību aizsardzības, nediskriminēšanas un dzimumu līdztiesības jomā. Priekšlikums neskar Vispārīgo datu aizsardzības regulu (Regulu (ES) 2016/679) un Tiesībaizsardzības direktīvu (Direktīvu (ES) 2016/680) un papildina tās ar saskaņotu noteikumu kopumu, kas attiecas uz dažu augsta riska AI sistēmu projektēšanu, izstrādi un izmantošanu, un ierobežojumiem attiecībā uz dažiem biometriskās tālidentifikācijas sistēmu lietojumiem. Turklāt priekšlikums papildina esošos Savienības tiesību aktus nediskriminēšanas jomā ar specifiskām prasībām, kuru mērķis ir minimizēt algoritmiskas diskriminācijas risku, it īpaši saistībā ar AI sistēmu izstrādē izmantoto datu kopu uzbūvi un kvalitāti, līdztekus pienākumiem attiecībā uz testēšanu, riska pārvaldību, dokumentāciju un cilvēka virsvadību visā AI sistēmu darbībā. Šis priekšlikums neskar Savienības konkurences tiesību aktu piemērošanu.

Attiecībā uz augsta riska AI sistēmām, kuras ir produktu drošības sastāvdaļas, šis priekšlikums tiks integrēts esošajos ar drošumu saistītajos nozares tiesību aktos ar mērķi nodrošināt saskanību, novērst dublēšanos un minimizēt papildu slogus. Tā, attiecībā uz augsta riska AI sistēmām produktos, uz kuriem attiecas Jaunā tiesiskā regulējuma (JTR) tiesību akti (piemēram, mašīnās, medicīniskās ierīcēs, rotaļlietās), šajā priekšlikumā noteiktās prasības AI sistēmām tiks pārbaudītas pastāvošo atbilstības novērtēšanas procedūru ietvaros saskaņā ar attiecīgajiem JTR tiesību aktiem. Attiecībā uz prasību mijiedarbību, lai gan AI sistēmām raksturīgos drošības riskus plānots iekļaut šajā priekšlikumā noteiktajās prasībās, JTR tiesību aktu mērķis ir nodrošināt gatavā produkta vispārējo drošumu, līdz ar to tajos var būt noteiktas īpašas prasības AI sistēmas drošai integrēšanai gatavā produktā. Priekšlikums Mašīnu regulai, kas pieņemts tajā pašā dienā, kurā pieņemts šis priekšlikums, pilnā mērā atspoguļo minēto pieeju. Šis priekšlikums tieši neattieksies uz augsta riska AI sistēmām produktos, uz kuriem attiecas attiecīgie vecās pieejas tiesību akti (piemēram, aviācija, automobiļi). Tomēr šajā priekšlikumā noteiktās būtiskās priekšprasības augsta riska AI sistēmām būs jāņem vērā, pieņemot attiecīgus īstenošanas aktus vai deleģētos aktus saskaņā ar iepriekš minētajiem tiesību aktiem.

Attiecībā uz AI sistēmām, ko sagādā vai izmanto regulētas kredītiestādes, Savienības finanšu pakalpojumu tiesību aktu uzraudzības iestādes būtu jāieceļ par kompetentajām iestādēm šā priekšlikuma prasību izpildes uzraudzībai ar mērķi nodrošināt šajā priekšlikumā un Savienības finanšu pakalpojumu tiesību aktos noteikto pienākumu saskaņotu izpildi, jo minētajos tiesību aktos AI sistēmas zināmā mērā ir netieši regulētas saistībā ar kredītiestāžu iekšējās pārvaldes sistēmu. Lai vēl vairāk uzlabotu saskanību, šajā priekšlikumā noteiktā atbilstības novērtēšanas procedūra un daži sagādātāju procesuālie pienākumi ir integrēti procedūrās, kas noteiktas Direktīvā 2013/36/ES par piekļuvi kredītiestāžu darbībai un prudenciālo uzraudzību¹⁴.

Šis priekšlikums saskan arī ar piemērojamiem Savienības tiesību aktiem pakalpojumu jomā, ieskaitot starpnieku pakalpojumus, kurus regulē Direktīva 2000/31/EK par elektronisko

¹⁴ Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (Dokuments attiecas uz EEZ) (OV L 176, 27.6.2013., 338.–436. lpp.).

tirdzniecību¹⁵ un Komisijas nesenis priekšlikums digitālo pakalpojumu tiesību aktam (DSA)¹⁶.

Attiecībā uz AI sistēmām, kuras ir lielapjoma IT sistēmu sastāvdaļas brīvības, drošības un tiesiskuma telpā, ko pārvalda Eiropas Savienības Aģentūra lielapjoma IT sistēmu darbības pārvaldībai (*eu-LISA*), priekšlikums neattieksies uz tām AI sistēmām, kuras ir laistas tirgū vai nodotas ekspluatācijā, pirms ir pagājis viens gads kopš šīs regulas piemērošanas dienas, ja vien iepriekš minēto tiesību aktu aizstāšana vai grozīšana nerada būtiskas izmaiņas attiecīgās AI sistēmas vai AI sistēmu uzbūvē vai tām paredzētajā nolūkā.

1.3. Saskaņība ar citām Savienības politikas jomām

Priekšlikums ir daļa no plašāka visaptveroša tādu pasākumu kopuma, kuri risina AI izstrādes un izmantošanas radītās problēmas, kas izskatītas Baltajā grāmatā par mākslīgo intelektu. Līdz ar to ir nodrošināta saskaņība un papildināmība ar citām esošajām vai plānotajām Komisijas iniciatīvām, kuru mērķis arī ir risināt minētās problēmas, ieskaitot nozaru tiesību aktu par produktiem (piemēram, Mašīnu direktīvas, Produktu vispārējās drošības direktīvas) pārskatīšanu un iniciatīvas, kurās tiek risināti atbildības jautājumi saistībā ar jaunajām tehnoloģijām, tostarp AI sistēmām. Minētās iniciatīvas balstīsies uz šo priekšlikumu un to papildinās, lai nodrošinātu juridisko noteiktību un sekmētu tādas ekosistēmas veidošanos Eiropā, kurā valda uzticēšanās AI.

Priekšlikums saskan arī ar Komisijas vispārējo digitālo stratēģiju attiecībā uz tās ieguldījumu tehnoloģijas, kas darbojas cilvēku labā, veicināšanā, kas ir viens no trīs galvenajiem pīlāriem politikas nostādnes un mērķos, kas pausti Komisijas paziņojumā “Eiropas digitālās nākotnes veidošana”¹⁷. Tas nosaka saskaņotu, efektīvu un samērīgu satvaru, kura mērķis ir nodrošināt, ka AI tiek izstrādāts, ievērojot cilvēku tiesības un gūstot viņu uzticēšanos, veidojot digitālajam laikmetam gatavu Eiropu un pārvēršot nākamos desmit gadus **digitālajā desmitgadē**¹⁸.

Turklāt AI virzītas inovācijas veicināšana ir cieši saistīta ar **Datu pārvaldības aktu**¹⁹, **Atvērto datu direktīvu**²⁰ un citām **Eiropas Datu stratēģijas**²¹ iniciatīvām, kuras izveidos uzticamus mehānismus un pakalpojumus datu atkalizmantošanai, kopīgošanai un apvienošanai, kas ir būtiski uz datiem balstītu augstas kvalitātes AI modeļu izstrādei.

Priekšlikums arī ievērojami stiprina Savienības lomu globālo normu un standartu veidošanā un tāda uzticama AI veicināšanā, kurš saskan ar Savienības vērtībām un interesēm. Tas nodrošina Savienībai spēcīgu pamatu turpmākai sadarbībai ar tās ārējiem partneriem, tostarp trešām valstīm, un darbībai starptautiskajos forumos ar AI saistītos jautājumos.

¹⁵ Eiropas Parlamenta un Padomes Direktīva 2000/31/EK (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) (OV L 178, 17.7.2000., 1.–16. lpp.).

¹⁶ Sk. priekšlikumu EIROPAS PARLAMENTA UN PADOMES REGULAI par digitālo pakalpojumu vienoto tirgu (digitālo pakalpojumu tiesību akts), ar ko groza Direktīvu 2000/31/EK, COM(2020) 825 final.

¹⁷ Komisijas paziņojums “Eiropas digitālās nākotnes veidošana”, COM(2020) 67 final.

¹⁸ [2030 Digital Compass: the European way for the Digital Decade](#).

¹⁹ Priekšlikums "Regula par Eiropas datu pārvaldi (Datu pārvaldes akts)", [COM/2020/767](#).

²⁰ Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1024 (2019. gada 20. jūnijs) par atvērtajiem datiem un publiskā sektora informācijas atkalizmantošanu, PE/28/2019/REV/1 (OV L 172, 26.6.2019., 56.–83. lpp.).

²¹ [Komisijas paziņojums “Eiropas Datu stratēģija”](#), COM(2020) 66 final.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

2.1. Juridiskais pamats

Priekšlikuma juridiskais pamats pirmām kārtām ir Līguma par Eiropas Savienības darbību (LESD) 114. pants, kurš paredz pieņemt pasākumus iekšējā tirgus izveides un darbības nodrošināšanai.

Šis priekšlikums ir ES digitālā vienotā tirgus stratēģijas nozīmīga daļa. Šā priekšlikuma galvenais mērķis ir nodrošināt iekšējā tirgus pareizu darbību, nosakot saskaņotus noteikumus, sevišķi tādu produktu un pakalpojumu izstrādei, laišanai Savienības tirgū un izmantošanai, kuros ietvertas AI tehnoloģijas vai kurus piedāvā kā savrupas AI sistēmas. Dažas dalībvalstis jau apsver valsts līmeņa noteikumus ar mērķi nodrošināt, ka AI ir drošs un to izstrādā un izmanto saskaņā ar pamattiesību pienākumiem. Paredzams, ka tas radīs divas galvenās problēmas: i) iekšējā tirgus sadrumstalotību būtiskos aspektos, sevišķi saistībā ar prasībām AI produktiem un pakalpojumiem, to tirdzniecību, izmantošanu, atbildību un publiskā sektora iestāžu uzraudzību; un ii) juridiskās noteiktības būtisku samazināšanos gan AI sistēmu sagādātājiem, gan lietotājiem attiecībā uz to, kā esošos un jaunos noteikumus piemēros minētajām sistēmām Savienībā. Ņemot vērā produktu un pakalpojumu plašo apriti pāri robežām, abas minētās problēmas vislabāk var atrisināt ar saskaņojamiem ES tiesību aktiem.

Priekšlikums nosaka kopīgas obligātās prasības noteiktu AI sistēmu projektēšanai un izstrādei pirms to laišanas tirgū; šīs prasības tiks sīkāk precizētas caur saskaņotiem tehniskajiem standartiem. Priekšlikums attiecas arī uz situāciju pēc AI sistēmu laišanas tirgū – tiek saskaņots veids, kā veicama pēckontrole.

Turklāt, ņemot vērā, ka šis priekšlikums satur dažus specifiskus noteikumus par privātpersonu aizsardzību attiecībā uz persondatu apstrādi, īpaši AI sistēmu izmantošanas ierobežojumus reāllaika biometriskajā tālidentifikācijā sabiedriskās vietās tiesībaizsardzības nolūkos, ir piemēroti par šīs regulas pamatu noteikt LESD 16. pantu, ciktāl tas attiecas uz minētajiem specifiskajiem noteikumiem.

2.2. Subsidiaritāte (neekskluzīvas kompetences gadījumā)

AI būtība – tas bieži ir balstīts uz apjomīgām un dažādām datu kopām un var būt iegulsts jebkādā produktā vai pakalpojumā, kas ir brīvā aprītē iekšējā tirgū, – nosaka to, ka dalībvalstis, rīkojoties atsevišķi, nevar iedarbīgi sasniegt šā priekšlikuma mērķus. Turklāt potenciāli atšķirīgu valstu noteikumu sadrumstalots kopums kavēs ar AI sistēmām saistītu produktu un pakalpojumu netraucētu apriti ES un nevarēs efektīvi garantēt drošību un pamattiesību un Savienības vērtību aizsardzību dažādajās dalībvalstīs. Valstu pieejas problēmu risināšanai tikai radīs papildu juridisko nenoteiktību un šķēršļus un kavēs AI ieviešanu tirgū.

Šā priekšlikuma mērķus iespējams labāk sasniegt Savienības līmenī, izvairoties no turpmākas vienotā tirgus sadrumstalošanās potenciāli pretrunīgās valstu sistēmās, kas kavēs AI saturošu preču un pakalpojumu brīvu apriti. Stingrs Eiropas tiesiskais regulējums uzticamam AI nodrošinās arī vienlīdzīgus konkurences apstākļus un aizsargās visus cilvēkus, vienlaikus stiprinot Eiropas konkurētspēju un rūpniecisko bāzi AI jomā. Tāpat tikai kopīga rīcība Savienības līmenī var aizsargāt Savienības digitālo suverenitāti un palīdzēt izmantot tās rīkus un regulatīvās pilnvaras globālo noteikumu un standartu veidošanā.

2.3. Proporcionalitāte

Priekšlikums pamatojas uz esošajiem tiesiskajiem regulējumiem un ir proporcionāls un nepieciešams tā mērķu sasniegšanai, jo īsteno uz risku balstītu pieeju un uzliek regulatīvo slogu tikai gadījumos, kad AI sistēma varētu radīt augstus riskus pamattiesībām un drošībai.

Citām AI sistēmām, kuras nav augsta riska sistēmas, ir noteikti tikai ļoti ierobežoti pārredzamības pienākumi, piemēram, attiecībā uz informācijas sniegšanu situācijās, kad jānorāda uz to, ka saskarsmē ar cilvēkiem tiek izmantota AI sistēma. Augsta riska AI sistēmu gadījumā prasības attiecībā uz augstas kvalitātes datiem, dokumentāciju un izsekojamību, pārredzamību, cilvēka virsvadību, precizitāti un noturību noteikti ir vajadzīgas, lai mazinātu tos AI radītos riskus pamattiesībām un drošībai, kas nav skarti citos esošajos tiesiskajos regulējumos. Saskaņoti standarti, kā arī atbalsta norādījumi un atbilstības nodrošināšanas rīki palīdzēs sagādātājiem un lietotājiem izpildīt priekšlikumā noteiktās prasības un minimalizēt izmaksas. Ekonomikas dalībniekiem radušās izmaksas ir proporcionālas sasniegtajiem mērķiem un ekonomiskajiem un reputācijas ieguvumiem, kurus tirgus dalībnieki var sagaidīt no šā priekšlikuma.

2.4. Juridiskā instrumenta izvēle

Regulas kā juridiskā instrumenta izvēli pamato nepieciešamība vienoti piemērot jaunus noteikumus, piemēram, AI definīciju, atsevišķu kaitīgas AI balstītas prakses veidu aizliegumu un noteiktu AI sistēmu klasifikāciju. Regulas tiešā piemērojamība saskaņā ar LESD 288. pantu samazinās juridisko sadrumstalotību un veicinās vienota tirgus attīstību likumīgām, drošām un uzticamām AI sistēmām. Regula to paveiks, ieviešot saskaņotu pamatprasību kopu AI sistēmām, kas klasificētas kā augsta riska sistēmas, un pienākumus šo sistēmu sagādātājiem un lietotājiem, uzlabojot pamattiesību aizsardzību un nodrošinot juridisko noteiktību gan ekonomikas dalībniekiem, gan patērētājiem.

Tajā pašā laikā regulas noteikumi nav pārlietu preskriptīvi un ļauj veikt dažāda līmeņa dalībvalstu darbības saistībā ar tiem elementiem, kuri nekavē iniciatīvas mērķu sasniegšanu, sevišķi tirgus uzraudzības sistēmas iekšēju organizāciju un pasākumu īstenošanu inovācijas veicināšanai.

3. RETROSPEKTĪVO IZVĒRTĒJUMU, APSPIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

3.1. Apspriešanās ar ieinteresētajām personām

Šis priekšlikums izstrādāts pēc plašas apspriešanās ar visām galvenajām ieinteresētajām personām, kuras gaitā Komisija ievēroja vispārīgos principus un minimālos standartus attiecībā uz apspriešanos ar ieinteresētajām personām.

Līdztekus Baltās grāmatas par mākslīgo intelektu publicēšanai 2020. gada 19. februārī tika sāкта **sabiedriskā apspriešana tiešsaistē**, tā noritēja līdz 2020. gada 14. jūnijam. Minētās apspriešanas mērķis bija apkopot viedokļus un uzskatus par balto grāmatu. Tā bija vērsta uz visām publiskā un privātā sektora ieinteresētajām personām, ieskaitot valdības, pašvaldības, komerciālas un nekomerciālas organizācijas, sociālos partnerus, ekspertus, akadēmiskās aprindas un iedzīvotājus. Pēc visu saņemto atbilžu analīzes Komisija savā tīmekļa vietnē publicēja rezultātu kopsavilkumu un individuālās atbildes²².

Kopumā tika saņemtas 1215 atbildes, 352 no tām – no uzņēmumiem vai uzņēmēju organizācijām/apvienībām, 406 – no privātpersonām (92 % no privātpersonām bija no ES), 152 – akadēmisko/pētniecības iestāžu vārdā un 73 – no publiskā sektora iestādēm. Pilsonisko sabiedrību pārstāvēja 160 respondenti (to starpā 9 patērētāju organizācijas, 129 nevalstiskās organizācijas un 22 arodbiedrības), 72 respondenti atbildes iesniedza kategorijā “citi

²²

[Visus apspriešanas rezultātus skatīt šeit.](#)

respondenti”. No 352 uzņēmējdarbības un nozares pārstāvjiem 222 bija uzņēmumi un uzņēmumu pārstāvji, 41,5 % no kuriem bija mikrouzņēmumi, mazi un vidēji uzņēmumi. Pārējās bija uzņēmēju apvienības. Kopumā 84 % no uzņēmējdarbības un nozares pārstāvju atbildēm nāca no ES-27. Atkarā no jautājuma 81 līdz 598 respondenti izmantoja brīvā teksta iespēju piezīmju paušanai. Caur *EUSurvey* tīmekļa vietni tika iesniegts vairāk nekā 450 nostājas dokumentu vai nu papildus atbildēm uz anketas jautājumiem (vairāk nekā 400), vai atsevišķi (vairāk nekā 50).

Kopumā ieinteresētās personas ir vienisprātis par nepieciešamību rīkoties. Lielākā daļa ieinteresēto personu piekrīt tam, ka pastāv nepilnības likumdošanā vai ka nepieciešami jauni tiesību akti. Tomēr vairākas ieinteresētās personas brīdina Komisiju par nepieciešamību izvairīties no dublēšanās, pretrunīgiem pienākumiem un pārmērīga regulējuma. Daudzās piezīmēs bija uzsvērti tehnoloģiski neitrāla un samērīga tiesiskā regulējuma nozīme.

Ieinteresētās personas lielākoties pieprasīja šauru, skaidru un precīzu AI definīciju. Ieinteresētās personas arī uzsvēra, ka papildus AI jēdziena precizēšanai ir svarīgi definēt jēdzienus “risks”, “augsts risks”, “zems risks”, “biometriskā tālidentifikācija” un “kaitējums”.

Lielākā daļa respondentu skaidri norādīja, ka dod priekšroku uz risku balstītai pieejai. Uz risku balstīta regulējuma izmantošana tika uzskatīta par labāku risinājumu nekā vienāds regulējums visām AI sistēmām. Risku un apdraudējumu veidus būtu jāizvērtē katrā nozarē un katrā gadījumā atsevišķi. Tāpat riski būtu jānovērtē, ņemot vērā ietekmi uz tiesībām un drošību.

“Regulatīvās smilškastēs” varētu būt ļoti noderīgas AI veicināšanai, un daļa ieinteresēto personu, īpaši uzņēmējdarbības apvienības, tās vērtē atzinīgi.

Vairāk nekā 50 % no tiem, kas pauda viedokli par izpildes modeļiem, īpaši uzņēmēju apvienības, attiecībā uz augsta riska AI sistēmām deva priekšroku iepriekšējās riska pašnovērtēšanas un pēcizpildes kombinēšanai.

3.2. Ekspertu atzinumu pieprasīšana un izmantošana

Priekšlikums pamatojas uz divu gadu gaitā veiktu analīzi un ieinteresēto personu ciešu iesaisti – to vidū bija akadēmisko aprindu pārstāvji, uzņēmumi, sociālie partneri, nevalstiskās organizācijas, dalībvalstis un iedzīvotāji. Sagatavošanās darbs sākās 2018. gadā, izveidojot **Mākslīgā intelekta augsta līmeņa ekspertu grupu (ALEG)**, kuras iekļaujošajā un plašajā sastāvā bija 52 labi pazīstami eksperti, kuru uzdevums bija konsultēt Komisiju Mākslīgā intelekta stratēģijas īstenošanā. 2019. gada aprīlī Komisija atbalstīja²³ galvenās prasības, kas izklāstītas ALEG ētikas vadlīnijās uzticamam AI²⁴, kuras tika pārskatītas, lai ņemtu vērā vairāk nekā 500 iesniegumu no ieinteresētajām personām. Galvenās prasības atspoguļo plaši izplatītu un kopīgu pieeju, kā to apliecina virkne ētikas kodeksu un principu, kurus izstrādājušas daudzas publiskas un privātas organizācijas Eiropā un ārpus tās un kuros noteikts, ka AI izstrādē un izmantošanā būtu jāvadās pēc dažiem būtiskiem, uz vērtībām orientētiem principiem. Uzticama mākslīgā intelekta novērtējuma saraksts (*The Assessment List for Trustworthy Artificial Intelligence, ALTAI*)²⁵ iedzīvināja minētās prasības darbībā izmēģinājuma procesā, kurā piedalījās vairāk nekā 350 organizācijas.

²³ Eiropas Komisija, “*Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam*”, COM(2019) 168.

²⁴ ALEG (2019), “*Ētikas vadlīnijas uzticamam AI*”.

²⁵ ALEG (2020), “*Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*”.

Papildus tika izveidota **Mākslīgā intelekta alianse**²⁶ – platforma AI tehnoloģisko un sociālo seku apspriešanai, kurā piedalās aptuveni 4000 ieinteresēto personu un kuras kulminācija ir ikgadējā AI asambleja.

Baltajā grāmatā par mākslīgo intelektu šī iekļaujošā pieeja tika izstrādāta sīkāk, saņemot piezīmes no vairāk nekā 1250 ieinteresētajām personām, tostarp papildus saņemot vairāk nekā 450 nostājas dokumentus. Tā rezultātā Komisija publicēja sākotnējo ietekmes novērtējumu, par kuru savukārt tika saņemts vairāk nekā 130 piezīmju²⁷. Tika organizēti arī **papildu ieinteresēto personu darbsemināri un pasākumi**, kuru rezultāti apstiprina ietekmes novērtējumā veikto analīzi un šajā priekšlikumā izdarītās politikas izvēles²⁸. Ietekmes novērtējuma izstrādāšanai tika pasūtīts arī **ārējais pētījums**.

3.3. Ietekmes novērtējums

Saskaņā ar labāka regulējuma politiku Komisija veica šā priekšlikuma ietekmes novērtējumu, kuru izskatīja Komisijas Regulējuma kontroles padome. 2020. gada 16. decembrī notika sanāksme ar Regulējuma kontroles padomi, pēc kuras tika sniegts negatīvs atzinums. Pēc apjomīgas ietekmes novērtējuma pārskatīšanas ar mērķi novērst saņemtajās piezīmēs norādītos trūkumus un ietekmes novērtējuma atkārtotas iesniegšanas Regulējuma kontroles padome 2021. gada 21. martā sniedza pozitīvu atzinumu. Regulējuma kontroles padomes atzinumi, ieteikumi un skaidrojums par to, kā tie ņemti vērā, ir atspoguļoti ietekmes novērtējuma 1. pielikumā.

Komisija izskatīja dažādus politikas variantus, ar ko varētu sasniegt priekšlikuma vispārīgo mērķi – **nodrošināt pareizu vienotā tirgus darbību**, Savienībā radot uzticama AI izstrādei un izmantošanai nepieciešamos apstākļus.

Tika novērtēti četri politikas varianti ar atšķirīgu regulatīvās iejaukšanās pakāpi:

- **1. variants:** ES likumdošanas instruments, ar ko izveido brīvprātīgu marķējuma sistēmu,
- **2. variants:** speciāla sektoriāla pieeja,
- **3. variants:** horizontāls ES likumdošanas instruments, kas atbilst samērīgai, uz risku balstītai pieejai,
- **3.+ variants:** horizontāls ES likumdošanas instruments, kas atbilst samērīgai, uz risku balstītai pieejai, un rīcības kodeksi AI sistēmām, kuras nerada augstu risku,
- **4. variants:** horizontāls ES likumdošanas instruments, kurā noteiktas obligātās prasības visām AI sistēmām neatkarīgi no riska pakāpes.

Saskaņā ar Komisijas iedibināto metodiku tika izvērtēta katra politikas varianta ekonomiskā un sociālā ietekme, īpaši koncentrējoties uz ietekmi uz pamattiesībām. Vēlamais variants ir 3.+ variants – tiesiskais regulējums tikai augsta riska AI sistēmām ar iespēju visiem tādu AI sistēmu sagādātājiem, kuras nerada augstu risku, īstenot rīcības kodeksu. Prasības attieksies uz datiem, dokumentāciju un izsekojamību, informācijas sniegšanu par pārredzamību, cilvēka

²⁶ Mākslīgā intelekta alianse ir 2018. gada jūnijā izveidots ieinteresēto personu forums, <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

²⁷ Eiropas Komisija, “*Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence*”.

²⁸ Sīkāku informāciju par visām notikušajām apspriešanām skatīt ietekmes novērtējuma 2. pielikumā.

virsvadību, noturību un precizitāti, un tās būs obligātas augsta riska AI sistēmām. Uzņēmumi, kas ieviestu rīcības kodeksus attiecībā uz citām AI sistēmām, to darītu brīvprātīgi.

Vēlamais variants tika uzskatīts par piemērotu šā priekšlikuma mērķu sasniegšanai visefektīvākajā veidā. Pieprasot AI izstrādātājiem un lietotājiem veikt ierobežotu, taču efektīvu darbību kopumu, vēlamais variants ierobežo pamattiesību un cilvēku drošības pārkāpšanas risku un sekmē efektīvu uzraudzību un izpildi, prasības nosakot tikai tām sistēmām, kurās pastāv augsts minēto pārkāpumu risks. Tā rezultātā atbilstības nodrošināšanas izmaksas minētā varianta ietvaros ir minimālas, un tādējādi sistēmu ieviešana netiek lieki kavēta ar augstākām cenām un atbilstības nodrošināšanas izmaksām. Lai risinātu iespējamus trūkumus MVU gadījumā, šis variants ietver vairākus noteikumus atbilstības sekmēšanai un izmaksu samazināšanai, tostarp “regulatīvo smilškastu” izveidi un pienākumu ņemt vērā MVU intereses, nosakot ar atbilstības novērtēšanu saistīto maksu apmēru.

Vēlamais variants vairo cilvēku uzticēšanos AI, uzņēmumi gūs juridisko noteiktību, un dalībvalstīm nebūs iemesla veikt vienpusējas darbības, kas varētu sadrumstalot vienoto tirgu. Augstākam uzticēšanās līmenim radot augstāku pieprasījumu, juridiskajai noteiktībai radot vairāk pieejamu piedāvājumu un nepastāvot šķēršļiem AI sistēmu pārrobežu aprītei, AI vienotais tirgus, visticamāk, plauks. Eiropas Savienība turpinās attīstīt strauji augošu AI ekosistēmu inovatīviem, AI tehnoloģijas saturošiem produktiem un pakalpojumiem vai savrupām AI sistēmām, tā vairojot digitālo autonomiju.

Uzņēmumiem vai publiskā sektora iestādēm, kas izstrādā vai izmanto AI lietojumus, kuri rada augstu risku iedzīvotāju drošībai vai pamattiesībām, būs jāizpilda specifiskas prasības un pienākumi. Atbilstības šīm prasībām nodrošināšana radītu izmaksas aptuveni 6000–7000 EUR apmērā par parastas augsta riska AI sistēmas piegādi aptuveni 170 000 EUR vērtībā līdz 2025. gadam. AI lietotājiem rastos ikgadējās izmaksas par laiku, kas veltīts cilvēka virsvadības nodrošināšanai attiecīgā gadījumā atkarā no lietojuma. Aplēsts, ka minētās izmaksas varētu būt aptuveni 5000–8000 EUR gadā. Pārbaudes izmaksas augsta riska AI piegādātājiem varētu būt vēl 3000–7500 EUR. Uzņēmumiem vai publiskā sektora iestādēm, kas izstrādā vai izmanto AI lietojumus, kuri nav klasificēti kā augsta riska lietojumi, būti vienīgi minimāli informēšanas pienākumi. Tomēr tie varētu izvēlēties apvienoties un kopīgi pieņemt rīcības kodeksu, lai izpildītu attiecīgas prasības un nodrošinātu, ka to AI sistēmas ir uzticamas. Minētajā gadījumā maksimālās izmaksas varētu būt tikpat lielas kā saistībā ar augsta riska AI sistēmām, taču, visticamāk, tās būtu zemākas.

Politikas variantu ietekme uz dažādām ieinteresēto personu kategorijām (ekonomikas dalībnieki / uzņēmumi; atbilstības novērtēšanas struktūras, standartizācijas iestādes un citas publiskas struktūras; privātpersonas/iedzīvotāji; pētnieki) ir sīki paskaidrota šim priekšlikumam pievienotā ietekmes novērtējuma 3. pielikumā.

3.4. Normatīvā atbilstība un vienkāršošana

Šis priekšlikums nosaka pienākumus, kas attieksies uz augsta riska AI sistēmu sagādātājiem un lietotājiem. Tiem sagādātājiem, kuri šādas sistēmas izstrādā un laiž Savienības tirgū, priekšlikums dos juridisko noteiktību un novērsīs šķēršļus ar AI saistītu pakalpojumu un produktu pārrobežu aprītei. Uzņēmumiem, kuri izmanto AI, tas vairo klientu uzticēšanos. No valstu publiskās pārvaldes iestāžu viedokļa – tas vairo sabiedrības uzticēšanos AI izmantošanai un stiprinās izpildes panākšanas mehānismus (ieviešot Eiropas koordinācijas mehānismu, paredzot pienācīgas spējas un vienkāršojot AI sistēmu revīzijas ar jaunām prasībām par dokumentāciju, izsekojamību un pārredzamību). Turklāt regulējums paredzēs specifiskus pasākumus inovācijas atbalstam, to starpā “regulatīvās smilškastes”, un specifiskus pasākumus, kas palīdzēs mazapjoma lietotājiem un augsta riska AI sistēmu sagādātājiem izpildīt jaunus noteikumus.

Tāpat priekšlikuma īpašs mērķis ir stiprināt Eiropas konkurētspēju un rūpniecisko bāzi AI jomā. Ir nodrošināta pilnīga atbilstība pašreizējiem Savienības nozaru tiesību aktiem, kuri attiecas uz AI sistēmām (piemēram, par produktiem un pakalpojumiem), tādējādi radot lielāku skaidrību un vienkāršojot jauno noteikumu izpildi.

3.5. Pamattiesības

AI izmantošana, ņemot vērā tam raksturīgās iezīmes (piemēram, nepārredzamība, sarežģītība, atkarība no datiem, autonoma darbība), var negatīvi ietekmēt virkni pamattiesību, kas nostiprinātas ES Pamattiesību hartā ("Pamattiesību harta"). Šā priekšlikuma nolūks ir nodrošināt minēto pamattiesību aizsardzību augstā līmenī, un tā mērķis ir risināt dažādus risku avotus caur skaidri noteiktu, uz risku balstītu pieeju. Ar prasību kopumu uzticamam AI un samērīgiem pienākumiem visiem vērtības ķēdes dalībniekiem priekšlikums uzlabos un veicinās Pamattiesību hartā nostiprināto tiesību aizsardzību: cilvēka cieņas aizsardzību (1. pants), privātās dzīves neaizskaramību un persondatu aizsardzību (7. un 8. pants), nediskriminēšanu (21. pants) un sieviešu un vīriešu līdztiesību (23. pants). Tā mērķis ir novērst atturošu ietekmi uz tiesībām uz vārda brīvību (11. pants) un pulcēšanās brīvību (12. pants), nodrošināt tiesību uz efektīvu tiesību aizsardzību un taisnīgu tiesu, tiesību uz aizstāvību un nevainīguma prezumpcijas (47. un 48. pants) aizsardzību, kā arī vispārējā labas pārvaldības principa aizsardzību. Turklāt, tā kā priekšlikumu piemēro noteiktās jomās, tas pozitīvi ietekmēs vairāku īpašu grupu tiesības, piemēram, darba ņēmēju tiesības uz godīgiem un taisnīgiem darba apstākļiem (31. pants), augstu patērētāju tiesību aizsardzības līmeni (28. pants), bērnu tiesības (24. pants) un invalīdu integrāciju (26. pants). Tas skar arī tiesības uz augstu vides aizsardzības līmeni un vides kvalitātes uzlabošanu (37. pants), tostarp attiecībā uz cilvēku veselību un drošību. Priekštestēšanas, riska pārvaldības un cilvēka virsvadības pienākumi veicinās arī citu pamattiesību ievērošanu, minimalizējot kļūdainu vai neobjektīvu AI balstītu lēmumu pieņemšanu tādās īpaši svarīgās jomās kā izglītība un apmācība, nodarbinātība, svarīgi pakalpojumi, tiesībaizsardzība un tiesu vara. Ja pamattiesības tomēr tikušas pārkāptas, pārkāpumu skartajām personām būs pieejama iedarbīga tiesiskā aizsardzība, jo tiks nodrošināta AI sistēmu pārredzamība un izsekojamība līdztekus stingrām pēcpārbaudēm.

Šis priekšlikums nosaka dažus darījumdarbības brīvības (16. pants) un humanitāro un eksakto zinātņu brīvības (13. pants) ierobežojumus ar mērķi augsta riska AI tehnoloģiju izstrādē un izmantošanā nodrošināt atbilstību tādiem sevišķi svarīgu vispārības interešu apsvērumiem kā veselība, drošība, patērētāju aizsardzība un citu pamattiesību aizsardzība ("atbildīga inovācija"). Minētie ierobežojumi ir samērīgi un aprobežojas ar būtisku drošības risku un iespējamu pamattiesību pārkāpumu novēršanai un mazināšanai nepieciešamo minimumu.

Arī pastiprinātie pārredzamības pienākumi nesamērīgi neietekmēs tiesības uz intelektuālā īpašuma aizsardzību (17. panta 2. punkts), jo tie aprobežosies ar informācijas minimumu, kas privātpersonām nepieciešama savu tiesību uz efektīvu tiesību aizsardzību īstenošanai, un ar nepieciešamo pārredzamību attiecībā uz uzraudzības un izpildes iestādēm saskaņā ar to pilnvarām. Jebkāda informācijas izpaušana notiks saskaņā ar attiecīgajiem jomas tiesību aktiem, ieskaitot Direktīvu (ES) 2016/943 par zinātnības un darījumdarbības neizpaužamas informācijas (komercnoslēpumu) aizsardzību pret nelikumīgu iegūšanu, izmantošanu un izpaušanu. Gadījumos, kad piekļuve konfidencialai informācijai vai pirmkodam ir jāpiešķir publiskā sektora iestādēm un pieteiktajām struktūrām, lai tās varētu pārbaudīt būtisku pienākumu izpildi, tām nosaka saistošus konfidencialitātes pienākumus.

4. IETEKME UZ BUDŽETU

Dalībvalstīm būs jānorīko uzraudzības iestādes, kuras atbildēs par regulatīvo prasību īstenošanu. To pienākumu izpilde uzraudzības jomā varētu būt balstīta jau esošā kārtībā, piemēram, saistībā ar atbilstības novērtēšanas struktūrām vai tirgus uzraudzību, taču tai būtu nepieciešama pietiekama tehnoloģiskā zinātība, cilvēkresursi un finanšu resursi. Atkarā no katrā dalībvalstī jau izveidotajām struktūrām tam varētu būt nepieciešams 1 līdz 25 pilnslodzes ekvivalenti uz vienu dalībvalsti.

Detalizēts pārskats par attiecīgajām izmaksām ir sniegts šim priekšlikumam pievienotajā finanšu pārskatā.

5. CITI ELEMENTI

5.1. Īstenošanas plāni un uzraudzības, izvērtēšanas un ziņošanas kārtība

Stingra uzraudzības un izvērtēšanas mehānisma ieviešana ir ļoti svarīga, lai panāktu to, ka priekšlikums efektīvi sasniedz savus specifiskos mērķus. Komisija atbildēs par priekšlikuma ietekmes uzraudzību. Tā izveidos sistēmu savrupu augsta riska AI lietojumu reģistrēšanai publiskā ES mēroga datubāzē. Minētā reģistrēšana ļaus arī kompetentajām iestādēm, lietotājiem un citiem ieinteresētajiem indivīdiem pārbaudīt, vai attiecīgā augsta riska AI sistēma atbilst priekšlikumā noteiktajām prasībām, un īstenot pastiprinātu to AI sistēmu uzraudzību, kuras rada augstus riskus pamattiesībām. Lai nodrošinātu minētās datubāzes saturu, AI sagādātājiem būs pienākums sniegt būtisko informāciju par savām sistēmām un to atbilstības novērtējumu.

Turklāt AI sagādātājiem būs jāinformē valstu kompetentās iestādes par nopietniem incidentiem vai darbības traucējumiem, kas pārkāpj ar pamattiesībām saistītos pienākumus, tiklīdz viņiem tie kļūs zināmi, kā arī par jebkādu AI sistēmu atsaukšanu vai izņemšanu no tirgus. Valstu kompetentās iestādes izmeklēs šos incidentus / darbības traucējumus, apkopos visu nepieciešamo informāciju un regulāri to nodos Komisijai kopā ar atbilstošiem metadatiem. Komisija šo informāciju par incidentiem papildinās ar visaptverošu kopējā AI tirgus analīzi.

Komisija publicēs ziņojumu par ierosinātā regulējuma izvērtēšanu un pārskatīšanu piecus gadus pēc dienas, kad tas kļūs piemērojams.

5.2. Detalizēts priekšlikuma specifisko noteikumu skaidrojums

5.2.1. DARBĪBAS JOMA UN DEFINĪCIJAS (I SADAĻA)

I sadaļā definēts regulas priekšmets un jauno noteikumu piemērošanas joma, kas aptver AI sistēmu laišanu tirgū, nodošanu ekspluatācijā un izmantošanu. Tajā arī sniegtas aktā izmantotās definīcijas. AI sistēmas definīcija veidota iespējami tehnoloģiski neitrāla un nākotnes prasībām atbilstoša, ņemot vērā ar AI saistīto tehnoloģiju un tirgus straujo attīstību. Lai nodrošinātu nepieciešamo juridisko noteiktību, I sadaļu papildina I pielikums, kurš satur detalizētu AI izstrādes pieeju un metožu sarakstu, kuru Komisija pielāgos atbilstoši tehnoloģiju attīstībai. Skaidri definēti ir arī tādi AI vērtības ķēdes galvenie dalībnieki kā AI sistēmu sagādātāji un lietotāji, kas ietver gan publiskus, gan privātus dalībniekus vienlīdzīgu konkurences apstākļu nodrošināšanai.

5.2.2. AIZLIEGTA MĀKSLĪGĀ INTELEKTA PRAKSE (II SADAĻA)

II sadaļā noteikts aizliegta AI saraksts. Regulā īstenota uz risku balstīta pieeja, nošķirot AI lietojumus, kuru riska līmenis ir (i) nepieņemams; (ii) augsts; vai (iii) zems vai minimāls. Aizliegtās prakses saraksts II sadaļā ietver visas tās AI sistēmas, kuru izmantošanu uzskata

par nepieņemamu, jo tā ir pretrunā Savienības vērtībām, piemēram, pārkāpj pamattiesības. Aizliegumi ietver praksi, kurai var būt ievērojams potenciāls manipulēt ar personām, izmantojot subliminālus paņēmienus, personām to neapzinoties, vai izmantojot kādu neaizsargātu grupu, piemēram, bērnu vai invalīdu, ietekmējamību ar mērķi būtiski iespaidot viņu uzvedību veidā, kas var nodarīt fizisku vai psiholoģisku kaitējumu viņiem vai kādai citai personai. Citāda manipulatīva vai ekspluatatīva prakse, kas ietekmē pieaugušos un ko var veicināt AI sistēmas, varētu tikt iekļauta esošajos datu aizsardzības, patērētāju aizsardzības un digitālo pakalpojumu tiesību aktos, kuri garantē fizisku personu pienācīgu informēšanu un brīvu izvēli netikt pakļautām profilēšanai vai citai praksei, kas var ietekmēt viņu uzvedību. Priekšlikums arī aizliedz AI bāzētu sociālo novērtēšanu, ko vispārējiem mērķiem veic publiskā sektora iestādes. Visbeidzot, aizliegta ir arī reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībaizsardzības nolūkos, ja vien nav piemērojami kādi ierobežoti izņēmumi.

5.2.3. *AUGSTA RISKĀ AI SISTĒMAS (III SADAĻA)*

III sadaļā ir specifiski noteikumi par AI sistēmām, kuras rada augstu risku fizisku personu veselībai un drošībai vai pamattiesībām. Atbilstoši uz risku balstītai pieejai šādas augsta riska AI sistēmas ir atļautas Eiropas tirgū, ja ir nodrošināta atbilstība noteiktām obligātām prasībām un veikta atbilstības priekšnovērtēšana. AI sistēmu klasificē kā augsta riska sistēmu, pamatojoties uz attiecīgās AI sistēmas paredzēto nolūku saskaņā ar esošo produktu drošuma regulējumu. Tādējādi AI sistēmu klasificē kā augsta riska sistēmu ne tikai atkarā no AI sistēmas veiktās funkcijas, bet arī pamatojoties uz īpašo lietojumu un kārtību, kādā sistēmu izmanto.

III sadaļas 1. nodaļā aprakstīti klasifikācijas noteikumi un noteiktas divas galvenās augsta riska AI sistēmu kategorijas:

- AI sistēmas, kuras paredzēts izmantot kā drošības sastāvdaļas produktos, kas pakļauti trešo personu atbilstības priekšnovērtēšanai,
- citas savrupas AI sistēmas, kurām galvenokārt ir ietekme uz pamattiesībām un kuras ir skaidri uzskaitītas III pielikumā.

Augsta riska AI sistēmu sarakstā III pielikumā norādīts ierobežots skaits AI sistēmu, kuru riski jau ir realizējušies vai, visticamāk, realizēsies tuvākā nākotnē. Lai nodrošinātu, ka regulu iespējams pielāgot AI jauna veida izmantošanai un lietojumiem, Komisija var paplašināt augsta riska AI sistēmu sarakstu kādu iepriekš noteiktu jomu ietvaros, piemērojot kritēriju kopumu un riska novērtēšanas metodiku.

2. nodaļā aprakstītas juridiskās prasības augsta riska AI sistēmām saistībā ar datiem un datu pārvaldi, dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu lietotājiem, cilvēka virsvadību, noturību, precizitāti un drošību. Ierosinātās minimālās prasības daudzi rūpīgi ekonomikas dalībnieki faktiski izpilda jau tagad, un tās ir divus gadus ilga sagatavošanās darba rezultāts, kas izriet no ALEG ētikas vadlīnijām²⁹, kuras tika izmēģinātas vairāk nekā 350 organizācijās³⁰. Tāpat tās lielā mērā saskan ar citiem starptautiskiem ieteikumiem un principiem, kas nodrošina to, ka ierosinātais AI regulējums ir saderīgs ar ES starptautiskās tirdzniecības partneru pieņemto regulējumu. Precīzus tehniskos risinājumus atbilstības prasībām nodrošināšanai var noteikt standartos vai citās tehniskajās specifikācijās vai izstrādāt citā veidā saskaņā ar vispārējām inženierzinātnes vai zinātniskajām atziņām pēc AI sistēmas sagādātāja ieskatiem. Šī elastība ir īpaši svarīga, jo tā ļauj AI sistēmu

²⁹ Mākslīgā intelekta augsta līmeņa ekspertu grupa (2019), [Ētikas vadlīnijas uzticamam AI](#).

³⁰ Tās apstiprināja arī Komisija savā 2019. gada paziņojumā par antropocentrisku pieeju AI.

sagādātājiem izvēlēties veidu, kas atbilst viņu prasībām, ņemot vērā jaunāko tehnoloģisko un zinātnisko progresu šajā jomā.

3. nodaļā noteikti skaidrs horizontālu pienākumu kopums augsta riska AI sistēmu sagādātājiem. Samērīgus pienākumus nosaka arī lietotājiem un citiem AI vērtības ķēdes dalībniekiem (piemēram, importētājiem, izplatītājiem, pilnvarotajiem pārstāvjiem).

4. nodaļā noteikta sistēma pieteikto struktūru kā neatkarīgu trešo personu iesaistei atbilstības novērtēšanas procedūrās, savukārt 5. nodaļā sīki paskaidrotas atbilstības novērtēšanas procedūras katram augsta riska AI sistēmas veidam. Atbilstības novērtēšanas pieejas mērķis ir minimalizēt slogu ekonomikas dalībniekiem, kā arī pieteiktajām struktūrām, kuru spējas ir pakāpeniski jāpalielina laika gaitā. Uz AI sistēmām, kuras paredzēts izmantot kā drošības sastāvdaļas produktos, kurus regulē Jaunā tiesiskā regulējuma tiesību akti (piemēram, mašīnās, rotaļlietās, medicīniskās ierīcēs utt.), attieksies tādi paši iepriekšēji un pēcāki atbilstības un izpildes mehānismi, kā uz produktiem, kuru sastāvā minētās sistēmas iekļautas. Galvenā atšķirība ir tāda, ka iepriekšējās un pēcākas kontroles mehānismi nodrošinās atbilstību ne tikai nozaru tiesību aktos noteiktajām prasībām, bet arī šajā regulā noteiktajām prasībām.

Savrupām augsta riska AI sistēmām, kuras minētas III pielikumā, tiks izveidota jauna atbilstības un izpildes sistēma. Tas atbilst Jaunā tiesiskā regulējuma modelim, kuru īsteno caur iekšējām kontroles pārbaudēm, ko veic sagādātāji; izņēmums ir biometriskas tālidentifikācijas sistēmas, uz kurām attiektos trešās personas veikta atbilstības novērtēšana. Visaptveroša atbilstības priekšnovērtēšana iekšējās pārbaudēs kombinācijā ar spēcīgu pēcāku izpildes panākšanu varētu būt iedarbīgs un saprātīgs risinājums minēto sistēmu gadījumā, ņemot vērā regulatīvās iejaukšanās agrīno stadiju un to, ka AI nozare ir ļoti inovatīva un revīzijas zinātība vēl tikai tiek uzkrāta. Savrupu augsta riska AI sistēmu novērtēšanai caur iekšējām pārbaudēm būtu nepieciešama pilnīga, iedarbīga un pienācīgi dokumentēta iepriekšēja atbilstība visām regulas prasībām un atbilstība stingrām kvalitātes un riska pārvaldības sistēmām un pēctirgus uzraudzībai. Pēc attiecīgās atbilstības novērtēšanas pabeigšanas sagādātājam būtu jāreģistrē minētās savrupās augsta riska AI sistēmas ES datubāzē, kuru pārvaldīs Komisija, ar nolūku vairojot publisko pārskatāmību un pārraudzību un stiprināt kompetento iestāžu veikto pēcāko uzraudzību. Turpretī, lai nodrošinātu saskanību ar esošajiem produktu drošuma tiesību aktiem, uz AI sistēmu, kuras izmanto kā drošības sastāvdaļas produktos, atbilstības novērtēšanu attieksies sistēma, kuru veido trešās personas veiktas atbilstības novērtēšanas procedūras, kas jau noteiktas attiecīgo nozaru produktu drošuma tiesību aktos. No jauna veikta atbilstības atkārtota priekšnovērtēšana būs nepieciešama gadījumā, ja tiks veiktas būtiskas modifikācijas AI sistēmās (īpaši, ja izmaiņas pārsniegs to, ko sagādātājs iepriekš noteicis savā tehniskajā dokumentācijā atbilstības priekšnovērtēšanas brīdī).

5.2.4. PĀRREDZAMĪBAS PIENĀKUMI, KAS ATTIECAS UZ NOTEIKTĀM AI SISTĒMĀM (IV SADAĻA)

IV sadaļa attiecas uz noteiktām AI sistēmām ar mērķi ņemt vērā to radīto īpašo manipulācijas risku. Pārredzamības pienākumi attieksies uz sistēmām, kuras (i) ir saskarsmē ar cilvēkiem; (ii) izmanto emociju konstatēšanai vai saiknes noteikšanai ar (sociālajām) kategorijām, pamatojoties uz biometriskajiem datiem; vai (iii) rada vai manipulē saturu ("dziļviltošana"). Kad cilvēki ir saskarsmē ar AI sistēmu vai viņu emocijas vai iezīmes tiek noteiktas ar automatizētiem līdzekļiem, viņi par to ir jāinformē. Ja AI sistēmu izmanto attēla, audio vai video satura radīšanai vai manipulēšanai un tās radītais rezultāts ievērojami atgādina autentisku saturu, būtu jānosaka pienākums izpaust to, ka saturs radīts ar automatizētiem

līdzekļiem, leģitīmu nolūku (tiesībaizsardzība, vārda brīvība) gadījumā piemērojot izņēmumus. Tas ļauj personām izdarīt apzinātu izvēli vai pamest attiecīgo situāciju.

5.2.5. *PASĀKUMI INOVĀCIJAS ATBALSTAM (V SADAĻA)*

V sadaļa sekmē mērķi radīt tādu tiesisko regulējumu, kurš ir inovācijai labvēlīgs, nākotnes prasībām atbilstošs un noturīgs pret traucējumiem. Šim nolūkam minētajā sadaļā valstu kompetentās iestādes ir mudinātas izveidot “regulatīvās smilškastes” un noteikta pamata sistēma attiecībā uz pārvaldi, uzraudzību un atbildību. AI “regulatīvās smilškastes” rada kontrolētu vidi inovatīvu tehnoloģiju testēšanai ierobežotā laikposmā, pamatojoties uz testēšanas plānu, kas saskaņots ar kompetentajām iestādēm. V sadaļa satur arī pasākumus regulatīvā sloga mazināšanai MVU un jaunuzņēmumiem.

5.2.6. *PĀRVALDE UN ĪSTENOŠANA (VI, VII UN VIII SADAĻA)*

VI sadaļā noteiktas pārvaldes sistēmas Savienības un valstu līmenī. Savienības līmenī ar šo priekšlikumu izveido Eiropas Mākslīgā intelekta padomi (“AI padome”), kurā piedalās dalībvalstu un Komisijas pārstāvji. AI padome veicinās šīs regulas netraucētu, efektīvu un saskaņotu īstenošanu, sekmējot valstu uzraudzības iestāžu un Komisijas produktīvu sadarbību un nodrošinot Komisijai ieteikumus un zinātību. Tāpat tā apkopos dalībvalstu paraugpraksi un dalīsies ar to.

Valstu līmenī dalībvalstīm būs jānorīko viena vai vairākas valsts kompetentās iestādes, savukārt no to vidus – valsts uzraudzības iestāde regulas piemērošanas un īstenošanas uzraudzībai. Eiropas Datu aizsardzības uzraudzītājs darbosies kā kompetentā iestāde Savienības iestāžu, aģentūru un struktūru uzraudzībai gadījumos, kad uz tām attieksies šīs regulas noteikumi.

VII sadaļas mērķis ir atvieglot Komisijas un valstu iestāžu veikto uzraudzību, izveidojot tādu savrupu augsta riska AI sistēmu ES mēroga datubāzi, kurām ir ietekme galvenokārt uz pamattiesībām. Datubāzi uzturēs Komisija, un datus sniegs tie AI sistēmu sagādātāji, kuriem būs pienākums reģistrēt savas sistēmas pirms to laišanas tirgū vai nodošanas ekspluatācijā citā veidā.

VIII sadaļā noteikti uzraudzības un ziņošanas pienākumi AI sistēmu sagādātājiem attiecībā uz pēctirgus uzraudzību un ziņošanu un ar AI saistītu incidentu un darbības traucējumu izmeklēšanu. Tirgus uzraudzības iestādes arī kontrolētu tirgu un izmeklētu visu jau tirgū laisto augsta riska AI sistēmu atbilstību prasībām un pienākumiem. Tirgus uzraudzības iestādēm būtu visas pilnvaras saskaņā ar Regulu (ES) 2019/1020 par tirgus uzraudzību. Izpildes panākšanai pēc AI sistēmas laišanas tirgū jānodrošina, ka publiskā sektora iestādēm ir nepieciešamās pilnvaras un resursi, lai varētu iejauktos gadījumā, ja AI sistēmas rada neparedzētus riskus, kuru novēršana prasa ātru rīcību. Minētās iestādes arī uzraudzīs, vai ekonomikas dalībnieki izpilda attiecīgos pienākumus saskaņā ar šo regulu. Priekšlikumā nav paredzēta automātiska jaunu iestāžu vai struktūru veidošana dalībvalstu līmenī. Dalībvalstis var izraudzīties jau pastāvošas nozaru iestādes (un izmantot to zinātību), kurām piešķirt arī pilnvaras uzraudzīt un panākt šīs regulas noteikumu izpildi.

Iepriekš minētais neskar pastāvošās sistēmas un pēctirgus izpildes nodrošināšanas pilnvaru sadalījumu attiecībā uz pienākumiem dalībvalstīs, kas saistīti ar pamattiesībām. Kad tas nepieciešams to funkciju veikšanai, esošās uzraudzības un izpildes iestādes būs arī pilnvarotas pieprasīt jebkādu dokumentāciju, kas tiek saglabāta saskaņā ar šo regulu, un piekļūt tai, un nepieciešamības gadījumā lūgt tirgus uzraudzības iestādēm organizēt augsta riska AI sistēmas testēšanu ar tehniskiem līdzekļiem.

5.2.7. RĪCĪBAS KODEKSI (IX SADAĻA)

IX sadaļā izveidota sistēma tādu rīcības kodeksu izstrādei, kuru mērķis ir mudināt zema riska AI sistēmu sagādātājus brīvprātīgi piemērot tās prasības, kas augsta riska AI sistēmām ir obligātas (noteiktas III sadaļā). Tādu AI sistēmu sagādātāji, kas nav augsta riska sistēmas, var paši izstrādāt un īstenot rīcības kodeksus. Minētie kodeksi var ietvert brīvprātīgas saistības, piemēram, attiecībā uz vides ilgtspēju, pieejamību invalīdiem, ieinteresēto personu līdzdalību AI sistēmu projektēšanā un izstrādē un daudzveidību izstrādes grupās.

5.2.8. NOBEIGUMA NOTEIKUMI (X, XI UN XII SADAĻA)

X sadaļā uzsvērts visu iesaistīto personu pienākums ievērot datu un informācijas konfidencialitāti un izklāstīti noteikumi regulas īstenošanas laikā iegūtās informācijas apmaiņai. X sadaļa ietver arī pasākumus regulas efektīvas īstenošanas nodrošināšanai, nosakot iedarbīgus, samērīgus un atturošus sodus par noteikumu pārkāpumiem.

XI sadaļā izklāstīti noteikumi par deleģēšanas un īstenošanas pilnvaru izmantošanu. Priekšlikums pilnvaro Komisiju pieņemt īstenošanas aktus ar mērķi nodrošināt regulas vienotu piemērošanu vai deleģētos aktus I–VII pielikuma sarakstu atjaunināšanai vai papildināšanai.

XII sadaļā noteikts Komisijas pienākums regulāri novērtēt nepieciešamību atjaunināt III pielikumu un sagatavot regulārus ziņojumus par regulas izvērtēšanu un pārskatīšanu. Tāpat tajā izklāstīti nobeiguma noteikumi, ieskaitot diferencētu pārejas periodu regulas piemērošanas sākuma dienai ar mērķi atbalstīt sekmīgu īstenošanu visām iesaistītajām personām.

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA**KAS NOSAKA SASKAŅOTAS NORMAS MĀKSLĪGĀ INTELEKTA JOMĀ
(MĀKSLĪGĀ INTELEKTA AKTS) UN GROZA DAŽUS SAVIENĪBAS
LĒGISLATĪVOS AKTUS**

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. un 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu³¹,

ņemot vērā Reģionu komitejas atzinumu³²,

saskaņā ar parasto likumdošanas procedūru,

tā kā:

- (1) Šīs regulas mērķis ir uzlabot iekšējā tirgus darbību, nosakot vienotu tiesisko regulējumu, it īpaši mākslīgā intelekta izstrādei, laišanai tirgū un izmantošanai saskaņā ar Savienības vērtībām. Šī regula kalpo virknei sevišķi svarīgu vispārības interešu, piemēram, veicina augstu veselības, drošības un pamattiesību aizsardzības līmeni, un nodrošina uz AI bāzētu preču un pakalpojumu brīvu pārvietošanos pāri robežām, tādējādi nepieļaujot dalībvalstu ierobežojumus AI sistēmu izstrādei, laišanai tirgū un izmantošanai, ja tie šajā regulā nav nepārprotami atļauti.
- (2) Mākslīgā intelekta sistēmas (AI sistēmas) var viegli ieviest vairākās ekonomikas nozarēs un sabiedrībā, arī pāri robežām, un tās var būt aprītē visā Savienībā. Dažas dalībvalstis jau ir izskatījušas iespēju pieņemt valsts līmeņa noteikumus ar mērķi nodrošināt to, ka mākslīgais intelekts ir drošs un to izstrādā un izmanto saskaņā ar pienākumiem ievērot pamattiesības. Atšķirīgi valsts noteikumi var izraisīt iekšējā tirgus sadrumstalotību un mazināt juridisko noteiktību ekonomikas dalībniekiem, kuri izstrādā vai izmanto AI sistēmas. Tāpēc visā Savienībā būtu jānodrošina konsekvents un augsts aizsardzības līmenis, turpretim atšķirības, kuras kavē AI sistēmu un saistīto produktu brīvu apriti iekšējā tirgū, būtu jānovērš, nosakot vienotus pienākumus operatoriem un visā iekšējā tirgū garantējot sevišķi svarīgu vispārības interešu un personu tiesību vienotu aizsardzību, pamatojoties uz Līguma par Eiropas Savienības darbību (LESD) 114. pantu. Ciktāl šī regula satur īpašus noteikumus par privātpersonu aizsardzību attiecībā uz persondatu apstrādi saistībā ar AI sistēmu izmantošanu reāllaika biometriskajai tālidentifikācijai sabiedriskās vietās tiesībaizsardzības nolūkos, ir piemēroti par šīs regulas pamatu noteikt LESD 16. pantu, ciktāl tas attiecas uz minētajiem īpašajiem noteikumiem. Ņemot vērā minētos īpašos noteikumus un

³¹ OV C [...], [...], [...]. lpp.

³² OV C [...], [...], [...]. lpp.

LESD 16. panta izmantošanu, ir lietderīgi apspriesties ar Eiropas Datu aizsardzības kolēģiju.

- (3) Mākslīgais intelekts ir tehnoloģiju kopa, kas strauji attīstās un var sniegt dažādus ekonomiskos un sociālos ieguvumus visās nozarēs un sociālajās darbībās. Uzlabojot prognozēšanas spēju, optimizējot darbības un resursu sadali un personalizējot indivīdiem un organizācijām pieejamos digitālos risinājumus, mākslīgā intelekta izmantošana var nodrošināt būtiskas konkurences priekšrocības uzņēmumiem un sekmēt sabiedrībai un videi labvēlīgus rezultātus, piemēram, veselības aprūpē, lauksaimniecībā, izglītībā un apmācībā, infrastruktūras apsaimniekošanā, enerģētikā, transportā un loģistikā, sabiedriskajos pakalpojumos, drošībā, tieslietās, resursefektivitātē un energoefektivitātē un klimata pārmaiņu mazināšanas un pielāgošanās jomā.
- (4) Tajā pašā laikā atkarā no mākslīgā intelekta konkrētā lietojuma un izmantošanas apstākļiem tas var radīt riskus un nodarīt kaitējumu vispārības interesēm un tiesībām, kuras aizsargā Savienības tiesību akti. Minētais kaitējums var būt materiāls vai nemateriāls.
- (5) Tāpēc ir nepieciešams Savienības tiesiskais regulējums, kas nosaka saskaņotus noteikumus mākslīgā intelekta jomā ar mērķi veicināt mākslīgā intelekta izstrādi, ieviešanu un izmantošanu iekšējā tirgū, vienlaikus nodrošinot augstu aizsardzības līmeni tādām vispārības interesēm kā veselība un drošība, un pamattiesību aizsardzība, kā tas atzīts un aizsargāts Savienības tiesību aktos. Lai sasniegtu minēto mērķi, būtu jānosaka noteikumi par noteiktu AI sistēmu laišanu tirgū un nodošanu ekspluatācijā, tādējādi nodrošinot netraucētu iekšējā tirgus darbību un ļaujot saistībā ar minētajām sistēmām izmantot preču un pakalpojumu brīvas pārvietošanās principa radītos ieguvumus. Nosakot minētos noteikumus, šī regula atbalsta Eiropadomes nosprausto Savienības mērķi³³ – Savienībai būt pasaules līderei droša, uzticama un ētiska mākslīgā intelekta attīstīšanā – un nodrošina ētikas principu aizsardzību, kā to īpaši lūdzis Eiropas Parlaments³⁴.
- (6) AI sistēmas jēdziens būtu skaidri jādefinē juridiskās noteiktības labad, vienlaikus nodrošinot elastību, kas vajadzīga, lai pielāgotos tehnoloģiju attīstībai nākotnē. Definīcija būtu jāpamato uz programmatūras galvenajām funkcionālajām iezīmēm, it sevišķi spēju konkrēta cilvēku noteikta mērķu kopuma ietvaros radīt tādas iznākumus kā saturs, prognozes, ieteikumi vai lēmumi, kuri ietekmē vidi, ar ko sistēma mijiedarbojas fiziskā vai digitālā dimensijā. AI sistēmas var projektēt darbībai dažādās autonomijas pakāpēs, un tās var izmantot kā savrupas sistēmas vai kā produkta sastāvdaļu neatkarīgi no tā, vai sistēma ir fiziski integrēta produktā (iegulta) vai nodrošina produkta funkcionalitāti, nebūdama tajā integrēta (neiegulta). AI sistēmas definīcija būtu jāpapildina ar konkrētu tās izstrādē izmantotu metožu un pieeju sarakstu, kurš būtu jāatjaunina saskaņā ar tirgus un tehnoloģiju attīstību, Komisijai pieņemot deleģētos aktus minētā saraksta grozīšanai.

³³ Eiropadome (2020), Eiropadomes ārkārtas sanāksme (2020. gada 1. un 2. oktobrī) – secinājumi, EUCO 13/20, 6. lpp.

³⁴ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru, 2020/2012(INL).

- (7) Šajā regulā izmantotais biometrisko datu jēdziens saskan ar biometrisko datu jēdziena definīciju Eiropas Parlamenta un Padomes Regulas (ES) 2016/679³⁵ 4. panta 14. punktā, Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725³⁶ 3. panta 18. punktā un Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680³⁷ 3. panta 13. punktā un būtu jāinterpretē saskaņā ar to.
- (8) Biometriskās tālidentifikācijas sistēmas jēdziens, kā tas izmantots šajā regulā, būtu jādefinē funkcionāli kā AI sistēma, kas paredzēta fizisku personu identifikācijai no attāluma, salīdzinot personas biometriskos datus ar atsaucēs datubāzē esošiem biometriskajiem datiem, iepriekš nezinot, vai attiecīgā persona atradīsies attiecīgajā vietā un var tikt identificēta, neatkarīgi no izmantotās tehnoloģijas, procesa vai biometrisko datu veida. Ņemot vērā to atšķirīgās iezīmes un izmantošanas veidus, kā arī dažādos saistītos riskus, būtu jānošķir “reāllaika” un “vēlāklaika” biometriskās tālidentifikācijas sistēmas. Reāllaika sistēmu gadījumā biometrisko datu iegūšana, salīdzināšana un identifikācija notiek uzreiz, gandrīz uzreiz vai, jebkurā gadījumā, bez būtiskas aiztures. Šajā ziņā nevajadzētu būt iespējai apiet šīs regulas noteikumus par attiecīgo AI sistēmu izmantošanu reāllaikā, iestrādājot sistēmā nelielu aizturi. Reāllaika sistēmās izmanto “tiešraides” vai “gandrīz tiešraides” materiālu, piemēram, videomateriālu, ko uzņem kamera vai cita ierīce ar līdzīgu funkciju. Turpretī vēlāklaika sistēmu gadījumā biometriskie dati jau ir iegūti, un salīdzināšana un identifikācija notiek tikai pēc būtiskas aiztures. Tās izmanto materiālu, piemēram, attēlus vai videomateriālus, ko uzņēmušas videonovērošanas sistēmas kameras vai privātas ierīces pirms sistēmas izmantošanas attiecībā uz attiecīgajām fiziskajām personām.
- (9) Šajā regulā sabiedriskas vietas jēdziens būtu jāsaprot kā fiziska vieta, kas ir publiski pieejama neatkarīgi no tā, vai minētā vieta ir publiska vai privāts īpašums. Tāpēc šis jēdziens neietver privāta rakstura vietas, piemēram, mājokļus, privātus klubus, birojus, noliktavas un rūpnīcas, kuras parasti nav brīvi pieejamas trešām personām, ieskaitot tiesībsargāšanas iestādes, ja vien šīs personas nav īpaši aicinātas vai attiecīgi pilnvarotas. Arī tiešsaistes vietas nav ietvertas, jo tās nav fiziskas vietas. Tomēr tas vien, ka piekļuvi vietai ierobežo zināmi nosacījumi, piemēram, ieejas biļete vai vecuma ierobežojums, nenozīmē, ka vieta nav sabiedriskā vieta šīs regulas nozīmē. Līdz ar to papildus tādām sabiedriskām vietām kā ielas, attiecīgās valdības ēku daļas un lielākā daļa transporta infrastruktūras tādas vietas kā kinoteātri, teātri, veikali un iepirkšanās centri parasti arī ir sabiedriskas vietas. Tomēr tas, vai konkrēta vieta ir sabiedriskā vieta, būtu jānosaka katrā gadījumā atsevišķi, ņemot vērā konkrētās individuālās situācijas specifiku.

³⁵ Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

³⁶ Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

³⁷ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (Tiesībsargāšanas direktīva) (OV L 119, 4.5.2016., 89. lpp.).

- (10) Lai nodrošinātu vienlīdzīgus konkurences apstākļus un indivīdu tiesību un brīvību efektīvu aizsardzību visā Savienībā, šīs regulas noteikumiem būtu jāattiecas uz AI sistēmu sagādātājiem nediskriminējošā veidā neatkarīgi no tā, vai tie iedibināti Savienībā vai trešā valstī, un uz Savienībā esošiem AI sistēmu lietotājiem.
- (11) Ņemot vērā to digitālo raksturu, šai regulai būtu jāattiecas uz dažām AI sistēmām, pat ja tās nav ne laistas tirgū, ne nodotas ekspluatācijā, ne izmantotas Savienībā. Tā tas ir, piemēram, ja Savienībā iedibināts ekonomikas dalībnieks iepērk pakalpojumus no ārpus Savienības ekonomikas dalībnieka saistībā ar darbību, ko veic AI sistēma, kura uzskatāma par augsta riska sistēmu un ietekmē fiziskas personas Savienībā. Minētajos apstākļos ārpus Savienības esošā ekonomikas dalībnieka izmantotā AI sistēma varētu apstrādāt datus, kas likumīgi savākti Savienībā un nosūtīti ārpus tās, un nodot pakalpojumus iepirkušajam Savienības ekonomikas dalībniekam attiecīgās AI sistēmas iznākumus, kas izriet no minētās datu apstrādes, nelaižot attiecīgo AI sistēmu tirgū, nenododot to ekspluatācijā vai neizmantojot to Savienībā. Lai novērstu šīs regulas noteikumu apiešanu un nodrošinātu iedarbīgu Savienībā esošo fizisko personu aizsardzību, šai regulai būtu jāattiecas uz AI sistēmu sagādātājiem un lietotājiem, kuri iedibināti trešā valstī, ciktāl attiecīgo sistēmu radītie iznākumi tiek izmantoti Savienībā. Tomēr, lai ņemtu vērā esošo kārtību un īpašu nepieciešamību sadarboties ar ārvalstu partneriem, ar kuriem notiek informācijas un pierādījumu apmaiņa, šai regulai nebūtu jāattiecas uz trešo valstu publiskā sektora iestādēm un starptautiskām organizācijām, ja darbība notiek tādu starptautisku nolīgumu ietvaros, kas noslēgti valstu vai Eiropas līmenī tiesībaizsardzības un tiesu iestāžu sadarbības nolūkā ar Savienību vai tās dalībvalstīm. Šādi nolīgumi ir noslēgti divpusēji starp dalībvalstīm un trešām valstīm vai starp Eiropas Savienību, Eiropolu un citām ES aģentūrām un trešām valstīm vai starptautiskām organizācijām.
- (12) Šai regulai būtu jāattiecas arī uz Savienības iestādēm, birojiem, struktūrām un aģentūrām, kad tās rīkojas kā AI sistēmas sagādātājs vai lietotājs. AI sistēmas, ko izstrādā vai izmanto tikai militāriem nolūkiem, būtu jāizslēdz no šīs regulas darbības jomas, ja attiecīgā izmantošana ietilpst kopīgās ārpolitikas un drošības politikas ekskluzīvā kompetencē, ko regulē Līguma par Eiropas Savienību (LES) V sadaļa. Šai regulai nevajadzētu skart noteikumus par starpnieku pakalpojumu sniedzēju atbildību, kas izklāstīti Eiropas Parlamenta un Padomes Direktīvā 2000/31/EK (kas grozīta ar digitālo pakalpojumu tiesību aktu).
- (13) Lai nodrošinātu konsekventu un augstu vispārības interešu aizsardzības līmeni attiecībā uz veselību, drošību un pamattiesībām, būtu jāizveido kopīgi normatīvie standarti visām augsta riska AI sistēmām. Minētajiem standartiem būtu jāsaucas ar Eiropas Savienības Pamattiesību hartu ("Pamattiesību harta"), jābūt nediskriminējošiem un saskaņā ar Savienības starptautiskās tirdzniecības saistībām.
- (14) Lai ieviestu samērīgu un iedarbīgu saistošu noteikumu kopumu AI sistēmām, būtu jāizmanto skaidri noteikta, uz risku balstīta pieeja. Minētajai pieejai šādu noteikumu veids un saturs būtu jāpielāgo AI sistēmu potenciāli radīto risku intensitātei un apmēram. Tāpēc ir nepieciešams aizliegt dažas mākslīgā intelekta prakses, noteikt prasības augsta riska AI sistēmām un pienākumus attiecīgajiem operatoriem un noteikt pārredzamības pienākumus attiecībā uz noteiktām AI sistēmām.
- (15) Līdztekus daudziem lietderīgiem mākslīgā intelekta izmantošanas veidiem šo tehnoloģiju var arī izmantot ļaunprātīgi, un tā var sniegt nebijušus un spēcīgus rīkus manipulatīvas, ekspluatatīvas un sociālās kontroles prakses īstenošanai. Šāda prakse ir īpaši kaitējoša un būtu jāaizliedz, jo tā ir pretrunā Savienības vērtībām attiecībā uz

cilvēka cieņu, brīvību, līdztiesību, demokrātiju un tiesiskumu un Savienības pamattiesībām, ieskaitot tiesības uz nediskriminēšanu, datu aizsardzību un privātumu un bērna tiesības.

- (16) Jāaizliedz laist tirgū, nodot ekspluatācijā vai izmantot noteiktas cilvēka uzvedības iespaidošanai domātas AI sistēmas, kuru dēļ var rasties fizisks vai psiholoģisks kaitējums. Tādas AI sistēmas izmanto zemapziņai adresētus elementus, kurus indivīdi nespēj uztvert, vai izmanto bērna un tādu cilvēku ietekmējamību, kas rodas viņu vecuma vai fiziskas vai garīgas nevarības dēļ. Sistēmas to dara ar nolūku būtiski iespaidot personas uzvedību un tā, ka tiek nodarīts vai var tikt nodarīts kaitējums attiecīgajai personai vai citai personai. Nevar pieņemt, ka nolūks pastāv, ja cilvēka uzvedības iespaidošana izriet no AI sistēmai ārpusējiem faktoriem, kuri nav sistēmas sagādātāja vai lietotāja varā. Aizliegumam nebūtu jākavē ar šādām AI sistēmām saistītu pētniecību leģitīmos nolūkos, ja šīs pētniecības ietvaros AI sistēma netiek izmantota cilvēka un mašīnas saskarsmē, kas fiziskas personas pakļauj kaitējumam, un pētniecību veic saskaņā ar atzītiem ētiskajiem standartiem zinātniskās pētniecības jomā.
- (17) AI sistēmas, kas publiskā sektora iestādēm vai to vārdā vispārējiem mērķiem nodrošina fizisko personu sociālo novērtēšanu, var radīt diskriminējošus iznākumus un dažu grupu atstumtību. Tās var pārkāpt tiesības uz cilvēka cieņas neaizskaramību un nediskriminēšanu un līdztiesības un tiesiskuma vērtības. Šādas AI sistēmas izvērtē vai klasificē fizisku personu uzticamību, pamatojoties uz viņu sociālo uzvedību dažādos kontekstos vai zināmām vai prognozētām personiskajām vai rakstura iezīmēm. Šādu AI sistēmu radītais sociālā novērtējuma rezultāts var izraisīt kaitējošu vai nelabvēlīgu attieksmi pret fiziskām personām vai veselām fizisku personu grupām sociālos kontekstos, kas nav saistīti ar to kontekstu, kurā dati tika sākotnēji radīti vai savākti, vai kaitējošu attieksmi, kas nav pamatota vai samērīga ar personu sociālās uzvedības “smagumu”. Tāpēc šādas AI sistēmas būtu jāaizliedz.
- (18) AI sistēmu izmantošanu fizisku personu reāllaika biometriskajai tālidentifikācijai sabiedriskās vietās tiesībaizsardzības nolūkos uzskata par īpaši aizskarošu attiecībā uz konkrēto personu tiesībām un brīvībām, ciktāl tā var ietekmēt lielas sabiedrības daļas privāto dzīvi, izraisīt pastāvīgas uztraudzības sajūtu un netieši atturēt no pulcēšanās brīvības un citu pamattiesību īstenošanas. Turklāt tūlītējā ietekme un ierobežotas iespējas veikt turpmākas pārbaudes vai labojumus attiecībā uz šādu reāllaikā darbojošos sistēmu izmantošanu rada pastiprinātu risku to personu tiesībām un brīvībām, pret kurām vērstas tiesībaizsardzības darbības.
- (19) Tāpēc minēto sistēmu izmantošana tiesībaizsardzības nolūkos būtu jāaizliedz, izņemot trīs precīzi uzskaitītas un šauri definētas situācijas, kurās sistēmu izmantošana ir absolūti nepieciešama tādu būtisku vispārības interešu īstenošanai, kuru nozīme atsver riskus. Minētās situācijas ietver noziegumos potenciāli cietušo, tostarp pazudušu bērnu, meklēšanu; nepārprotamu apdraudējumu fizisku personu dzīvībai vai fiziskajai drošībai vai teroristiska uzbrukuma draudus; un Padomes pamatlēmumā 2002/584/TI³⁸ minēto noziedzīgo nodarījumu izdarītāju vai aizdomās turamo atklāšanu, atrašanās vietas noteikšanu, identifikāciju vai saukšanu pie atbildības, ja minētie noziedzīgie nodarījumi attiecīgajā dalībvalstī ir sodāmi ar brīvības atņemšanas sodu vai ar brīvības atņemšanu saistītu drošības līdzekli vismaz uz trim gadiem, un kā noteikts attiecīgās

³⁸

Padomes pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

dalībvalsts tiesību aktos. Šāda robežvērtība brīvības atņemšanas sodam vai ar brīvības atņemšanu saistītam drošības līdzeklim saskaņā ar valstu tiesību aktiem palīdz nodrošināt, ka noziedzīgajam nodarījumam jābūt pietiekami smagam, lai potenciāli pamatotu reāllaika biometriskās tālidentifikācijas sistēmas izmantošanu. Turklāt no 32 noziedzīgajiem nodarījumiem, kas uzskaitīti Padomes pamatlēmumā 2002/584/TI, daži praksē, visticamāk, būs būtiskāki nekā citi, proti, paredzams, ka reāllaika biometriskās tālidentifikācijas sistēmas izmantošana būs nepieciešama un samērīga ļoti atšķirīgā pakāpē atkarā no praktiskajām darbībām dažādo uzskaitīto noziedzīgo nodarījumu izdarītāja vai aizdomās turamā atklāšanai, atrašanās vietas noteikšanai, identifikācijai vai saukšanai pie atbildības, ņemot vērā paredzamās atšķirības kaitējuma smaguma, iespējamības un apmēra vai iespējamo negatīvo seku ziņā.

- (20) Lai nodrošinātu, ka minētās sistēmas tiek izmantotas atbildīgi un samērīgi, ir svarīgi arī noteikt, ka katrā no trim precīzi uzskaitītajām un šauri definētajām situācijām jāņem vērā noteikti elementi, it īpaši situācijas raksturs, kurš pamato sistēmas izmantošanu, izmantošanas ietekme uz visu iesaistīto personu tiesībām un brīvībām, un izmantošanai nodrošinātie apstākļi un aizsardzības pasākumi. Turklāt reāllaika biometriskās tālidentifikācijas sistēmu izmantošanai sabiedriskās vietās tiesībaizsardzības nolūkos būtu jānosaka atbilstoši ierobežojumi laikā un telpā, galvenokārt ņemot vērā pierādījumus vai norādes par apdraudējumiem, cietušajiem vai noziedzīgo nodarījumu izdarītājiem. Personu atsauces datubāzei vajadzētu būt pielāgotai katram izmantošanas gadījumam katrā no trim iepriekš minētajām situācijām.
- (21) Katram reāllaika biometriskās tālidentifikācijas sistēmas izmantošanas gadījumam sabiedriskās vietās tiesībaizsardzības nolūkos vajadzētu saņemt skaidru un precīzu atļauju no tiesu iestādes vai dalībvalsts neatkarīgas administratīvās iestādes. Šādu atļauju būtībā vajadzētu saņemt pirms izmantošanas, izņemot pienācīgi pamatotas, steidzamas situācijas, proti, situācijas, kurās nepieciešamība izmantot attiecīgās sistēmas padara atļaujas iegūšanu pirms izmantošanas sākšanas faktiski un objektīvi neiespējamu. Šādās steidzamās situācijās izmantošanai būtu jāaprobežojas ar absolūti nepieciešamo minimumu un jānodrošina atbilstoši aizsardzības pasākumi un apstākļi, kā to nosaka valstu tiesību akti un precizē pati tiesībaizsardzības iestāde katra atsevišķa steidzamas izmantošanas gadījuma kontekstā. Papildus tam tiesībaizsardzības iestādei šādās situācijās būtu jācenšas saņemt atļauju pēc iespējas ātrāk, vienlaikus norādot iemeslus, kāpēc atļauju nebija iespējams pieprasīt agrāk.
- (22) Turklāt šīs regulas izveidotajā izsmēlošajā sistēmā ir lietderīgi noteikt, ka minētajai izmantošanai dalībvalsts teritorijā saskaņā ar šo regulu vajadzētu būt iespējamai tikai, ja un ciktāl attiecīgā dalībvalsts ir nolēmusi valsts tiesību aktu noteikumos skaidri paredzēt iespēju atļaut minēto izmantošanu. Tādējādi dalībvalstis saskaņā ar šo regulu var neparedzēt šādu iespēju nemaz vai paredzēt to attiecībā uz dažiem mērķiem, ar kuriem var pamatot šajā regulā noteikto atļauto izmantošanu.
- (23) AI sistēmu izmantošana fizisku personu reāllaika biometriskajai tālidentifikācijai sabiedriskās vietās tiesībaizsardzības nolūkos neizbēgami ietver biometrisku datu apstrādi. Šīs regulas noteikumi, kas aizliedz (ar dažiem izņēmumiem) minēto izmantošanu un pamatojas uz LESD 16. pantu, būtu jāpiemēro kā speciālās normas attiecībā uz Direktīvas (ES) 2016/680 10. panta noteikumiem par biometrisku datu apstrādi, tādā veidā izsmēloši regulējot minēto izmantošanu un ar to saistīto biometrisku datu apstrādi. Tāpēc minētajai izmantošanai un datu apstrādei vajadzētu būt iespējamai, tikai ciktāl tā ir saderīga ar šajā regulā noteikto sistēmu, bez darbības jomas ārpus minētās sistēmas, kurā kompetentās iestādes, rīkojoties tiesībaizsardzības

nolūkā, varētu izmantot šādas sistēmas un apstrādāt saistītos datus, pamatojoties uz Direktīvas (ES) 2016/680 10. pantā uzskaitītajiem iemesliem. Minētajā kontekstā šīs regulas mērķis nav nodrošināt juridisko pamatu persondatu apstrādei saskaņā ar Direktīvas (ES) 2016/680 8. pantu. Tomēr reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās nolūkos, kas nav saistīti ar tiesībaizsardzību, tostarp no kompetento iestāžu puses, nebūtu jāiekļauj šajā regulā noteiktajā attiecīgajā sistēmā, kas regulē minēto izmantošanu tiesībaizsardzības nolūkos. Tāpēc šajā regulā noteiktā prasība saņemt atļauju un piemērojamie valstu tiesību aktu noteikumi, kas varētu to ieviest, nebūtu jāattiecinā uz minēto izmantošanu nolūkos, kas nav saistīti ar tiesībaizsardzību.

- (24) Biometrisko datu un citu persondatu apstrādei saistībā ar AI sistēmu izmantošanu biometriskajai identifikācijai, kas nav saistīta ar reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos, kā to nosaka šī regula, ieskaitot gadījumus, kad kompetentās iestādes izmanto minētās sistēmas sabiedriskās vietās nolūkos, kas nav saistīti ar tiesībaizsardzību, būtu arī turpmāk jāatbilst visām piemērojamajām prasībām, kas izriet no Regulas (ES) 2016/679 9. panta 1. punkta, Regulas (ES) 2018/1725 10. panta 1. punkta un Direktīvas (ES) 2016/680 10. panta.
- (25) Saskaņā ar LES un LESD pievienotā Protokola (Nr. 21) par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu 6.a pantu Īrijai nav saistoši šīs regulas 5. panta 1. punkta d) apakšpunkta un 2. un 3. punkta noteikumi, kuri pieņemti, pamatojoties uz LESD 16. pantu, un ir saistīti ar persondatu apstrādi dalībvalstīs, veicot darbības, uz kurām attiecas LESD trešās daļas V sadaļas 4. un 5. nodaļa, kurās noteikts, ka uz Īriju neattiecas noteikumi, kas regulē tiesu iestāžu sadarbības krimināllietās formas vai policijas sadarbību, kam nepieciešama atbilstība noteikumiem, kuri noteikti, pamatojoties uz LESD 16. pantu.
- (26) Saskaņā ar LES un LESD pievienotā Protokola (Nr. 22) par Dānijas nostāju 2. un 2.a pantu Dānijai nav saistoši un nav jāpiemēro šīs regulas 5. panta 1. punkta d) apakšpunkta un 2. un 3. punkta noteikumi, kuri pieņemti, pamatojoties uz LESD 16. pantu, un ir saistīti ar persondatu apstrādi dalībvalstīs, veicot darbības, uz kurām attiecas LESD trešās daļas V sadaļas 4. un 5. nodaļa.
- (27) Augsta riska AI sistēmas būtu jālaiž Savienības tirgū vai jānodod ekspluatācijā tikai tad, ja tās atbilst noteiktām obligātām prasībām. Minētajām prasībām būtu jānodrošina, ka augsta riska AI sistēmas, kuras pieejamas Savienībā vai kuru iznākumus citādā veidā izmanto Savienībā, nerada nepieņemamus riskus svarīgām Savienības sabiedriskajām interesēm, kas ir atzītas un aizsargātas Savienības tiesību aktos. Kā augsta riska sistēmas būtu jāklasificē tikai tās AI sistēmas, kurām ir ievērojama kaitējoša ietekme uz personu veselību, drošību un pamattiesībām Savienībā, un šādai klasificēšanai būtu pēc iespējas jāsamazina iespējamu starptautiskās tirdzniecības ierobežojumu rašanās.
- (28) AI sistēmas var radīt personu veselībai un drošībai kaitīgu iznākumu, īpaši tad, ja šādas sistēmas darbojas kā produktu sastāvdaļas. Saskaņā ar Savienības saskaņošanas tiesību aktu mērķiem veicināt produktu brīvu apriti iekšējā tirgū un gādāt, ka tirgū nonāk tikai droši un cita veida prasībām atbilstoši produkti, ir svarīgi pienācīgi novērst un mazināt drošības riskus, kurus var radīt produkts kopumā tā digitālo sastāvdaļu, arī AI sistēmu, dēļ. Piemēram, arvien autonomākiem robotiem gan ražošanas, gan personīgās palīdzības un aprūpes kontekstā vajadzētu spēt droši darboties un veikt savas funkcijas sarežģītās vidēs. Tāpat veselība aprūpes nozarē, kur runa ir par

veselību un dzīvību, arvien sarežģītākām diagnostikas sistēmām un cilvēka lēmumus atbalstošām sistēmām vajadzētu būt ticamām un pareizām. AI sistēmas izraisītās kaitējošās ietekmes uz Pamattiesību hartā aizsargātajām pamattiesībām apmērs ir īpaši nozīmīgs, klasificējot AI sistēmu kā augsta riska sistēmu. Minētās tiesības ietver cilvēka cieņas aizsardzību, privātās un ģimenes dzīves neaizskaramību un persondatu aizsardzību, vārda un informācijas brīvību, pulcēšanās un biedrošanās brīvību, nediskriminēšanu, patērētāju aizsardzību, darba ņēmēju tiesības, invalīdu tiesības, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, nevainīguma prezumpciju un tiesības uz aizstāvību, tiesības uz labu pārvaldību. Papildus minētajām tiesībām ir svarīgi izcelt, ka bērniem ir īpašas tiesības, kas noteiktas ES Pamattiesību hartas 24. pantā un ANO Konvencijā par bērna tiesībām (sīkāk izstrādātas minētās ANO konvencijas Vispārējā komentārā Nr. 25 par digitālo vidi); abi dokumenti nosaka, ka ir jāņem vērā bērnu neaizsargātība un viņu labklājības labad nepieciešams nodrošināt aizsardzību un aprūpi. Novērtējot kaitējuma smagumu, ko AI sistēma var nodarīt, arī attiecībā uz personu veselību un drošību, būtu jāņem vērā arī Pamattiesības uz augstu vides aizsardzības līmeni, kuras ir nostiprinātas Pamattiesību hartā un iestrādātas Savienības politikā.

- (29) Attiecībā uz augsta riska AI sistēmām, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas, uz ko attiecas Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008³⁹, Eiropas Parlamenta un Padomes Regula (ES) Nr. 167/2013⁴⁰, Eiropas Parlamenta un Padomes Regula (ES) Nr. 168/2013⁴¹, Eiropas Parlamenta un Padomes Direktīva 2014/90/ES⁴², Eiropas Parlamenta un Padomes Direktīva (ES) 2016/797⁴³, Eiropas Parlamenta un Padomes Regula (ES) 2018/858⁴⁴, Eiropas Parlamenta un Padomes Regula (ES) 2018/1139⁴⁵, un Eiropas Parlamenta un Padomes Regula (ES) 2019/2144⁴⁶, ir lietderīgi grozīt minētos aktus, lai nodrošinātu,

³⁹ Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008 (2008. gada 11. marts) par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ Regulu (EK) Nr. 2320/2002 (OV L 97, 9.4.2008., 72. lpp.).

⁴⁰ Eiropas Parlamenta un Padomes Regula (ES) Nr. 167/2013 (2013. gada 5. februāris) par lauksaimniecības un mežsaimniecības transportlīdzekļu apstiprināšanu un tirgus uzraudzību (OV L 60, 2.3.2013., 1. lpp.).

⁴¹ Eiropas Parlamenta un Padomes Regula (ES) Nr. 168/2013 (2013. gada 15. janvāris) par divu riteņu vai trīs riteņu transportlīdzekļu un kvadriciklu apstiprināšanu un tirgus uzraudzību (OV L 60, 2.3.2013., 52. lpp.).

⁴² Eiropas Parlamenta un Padomes Direktīva 2014/90/ES (2014. gada 23. jūlijs) par kuģu aprīkojumu un ar ko atceļ Padomes Direktīvu 96/98/EK (OV L 257, 28.8.2014., 146. lpp.).

⁴³ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/797 (2016. gada 11. maijs) par dzelzceļa sistēmas savstarpēju izmantojamību Eiropas Savienībā (OV L 138, 26.5.2016., 44. lpp.).

⁴⁴ Eiropas Parlamenta un Padomes Regula (ES) 2018/858 (2018. gada 30. maijs) par mehānisko transportlīdzekļu un to piekabju, kā arī tādiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisku vienību apstiprināšanu un tirgus uzraudzību un ar ko groza Regulas (EK) Nr. 715/2007 un (EK) Nr. 595/2009 un atceļ Direktīvu 2007/46/EK (OV L 151, 14.6.2018., 1. lpp.).

⁴⁵ Eiropas Parlamenta un Padomes Regula (ES) 2018/1139 (2018. gada 4. jūlijs) par kopīgiem noteikumiem civilās aviācijas jomā un ar ko izveido Eiropas Savienības Aviācijas drošības aģentūru, un ar ko groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 2111/2005, (EK) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 un Direktīvas 2014/30/ES un 2014/53/ES un atceļ Eiropas Parlamenta un Padomes Regulas (EK) Nr. 552/2004 un (EK) Nr. 216/2008 un Padomes Regulu (EEK) Nr. 3922/91 (OV L 212, 22.8.2018., 1. lpp.).

⁴⁶ Eiropas Parlamenta un Padomes Regula (ES) 2019/2144 (2019. gada 27. novembris) par prasībām mehānisko transportlīdzekļu un to piekabju un šiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisko vienību tipa apstiprināšanai attiecībā uz to vispārīgo drošību un transportlīdzekļa braucēju un neaizsargāto ceļu satiksmes dalībnieku aizsardzību, ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2018/858 un atceļ Eiropas Parlamenta un Padomes Regulas (EK) Nr. 78/2009,

ka Komisija, pamatojoties uz katras nozares tehniskajām un regulatīvajām īpatnībām un neiejaucoties nozarēs pastāvošajos pārvaldes, atbilstības novērtēšanas un izpildes mehānismos un iestādēs, ņem vērā šajā regulā noteiktās obligātās prasības augsta riska AI sistēmām, kad tā pieņem turpmākus attiecīgus deleģētos vai īstenošanas aktus, pamatojoties uz minētajiem tiesību aktiem.

- (30) Attiecībā uz augsta riska AI sistēmām, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas, uz ko attiecas konkrēti Savienības saskaņošanas tiesību akti, ir lietderīgi tās klasificēt kā augsta riska sistēmas saskaņā ar šo regulu, ja attiecīgajam produktam piemēro atbilstības novērtēšanas struktūras, kas ir trešā persona, veiktu atbilstības novērtēšanas procedūru saskaņā ar attiecīgajiem Savienības saskaņošanas tiesību aktiem. Proti, tādi produkti ir mašīnas, rotaļlietas, lifti, iekārtas un aizsardzības sistēmas, kas paredzētas lietošanai sprādzienbīstamā vidē, radioiekārtas, spiediena iekārtas, atpūtas kuģu aprīkojums, trošu ceļu iekārtas, iekārtas, kurās izmanto gāzveida kurināmo, medicīniskās ierīces un *in vitro* diagnostikas medicīniskās ierīces.
- (31) Tam, ka AI sistēmu klasificē kā augsta riska sistēmu saskaņā ar šo regulu, nebūtu obligāti jānozīmē, ka produktu, kura drošības sastāvdaļa ir attiecīgā AI sistēma, vai pašu AI sistēmu kā produktu uzskata par augstu risku radošu saskaņā ar kritērijiem, kas noteikti attiecīgajos Savienības saskaņošanas tiesību aktos, kurus piemēro minētajam produktam. Tā tas ir īpaši ar Eiropas Parlamenta un Padomes Regulu (ES) 2017/745⁴⁷ un Eiropas Parlamenta un Padomes Regulu (ES) 2017/746⁴⁸, kurās paredzēta trešās personas veikta atbilstības novērtēšana vidēja riska augsta riska produktiem.
- (32) Savrupas AI sistēmas, proti, augsta riska AI sistēmas, kuras nav produktu drošības sastāvdaļas vai kuras pašas ir produkti, ir lietderīgi klasificēt kā augsta riska sistēmas, ja, pamatojoties uz to paredzēto nolūku, tās rada augstu kaitējuma risku personu veselībai, drošībai vai pamattiesībām, ņemot vērā gan iespējamā kaitējuma smagumu, gan iespējamību, un ja tās izmanto vairākās iepriekš īpaši noteiktās jomās, kā precizēts regulā. Minēto sistēmu identifikācija pamatojas uz tādu pašu metodiku un kritērijiem, kādus paredzēts izmantot jebkādos turpmākos augsta riska AI sistēmu saraksta grozījumos.
- (33) Fizisku personu biometriskajai tālidentifikācijai paredzētu AI sistēmu tehniskās neprecizitātes var radīt neobjektīvus rezultātus un diskriminējošu ietekmi. Īpaši tas var būt saistīts ar vecumu, tautību, dzimumu vai invaliditāti. Tāpēc reāllaika un vēlāklaika biometriskās tālidentifikācijas sistēmas būtu jāklasificē kā augsta riska sistēmas. Ņemot vērā to radītos riskus, abu veidu biometriskās tālidentifikācijas sistēmām būtu jāpiemēro zināmas prasības par reģistrēšanas iespējām un cilvēka virsvadību.

(EK) Nr. 79/2009 un (EK) Nr. 661/2009 un Komisijas Regulas (EK) Nr. 631/2009, (ES) Nr. 406/2010, (ES) Nr. 672/2010, (ES) Nr. 1003/2010, (ES) Nr. 1005/2010, (ES) Nr. 1008/2010, (ES) Nr. 1009/2010, (ES) Nr. 19/2011, (ES) Nr. 109/2011, (ES) Nr. 458/2011, (ES) Nr. 65/2012, (ES) Nr. 130/2012, (ES) Nr. 347/2012, (ES) Nr. 351/2012, (ES) Nr. 1230/2012 un (ES) 2015/166 (OV L 325, 16.12.2019., 1. lpp.).

⁴⁷ Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm, ar ko groza Direktīvu 2001/83/EK, Regulu (EK) Nr. 178/2002 un Regulu (EK) Nr. 1223/2009 un atceļ Padomes Direktīvas 90/385/EEK un 93/42/EEK (OV L 117, 5.5.2017., 1. lpp.).

⁴⁸ Eiropas Parlamenta un Padomes Regula (ES) 2017/746 (2017. gada 5. aprīlis) par *in vitro* diagnostikas medicīniskām ierīcēm un ar ko atceļ Direktīvu 98/79/EK un Komisijas Lēmumu 2010/227/ES (OV L 117, 5.5.2017., 176. lpp.).

- (34) Attiecībā uz kritiskās infrastruktūras apsaimniekošanu un darbību ir lietderīgi kā augsta riska sistēmas klasificēt tās AI sistēmas, kuras paredzēts izmantot kā drošības sastāvdaļas ceļu satiksmes pārvaldībā un darbībā, kā arī ūdens, gāzes un elektroenerģijas piegādē un apkures nodrošināšanā, jo sistēmu darbības atteice vai traucējumi var plašā mērogā apdraudēt cilvēku veselību un dzīvību un izraisīt ievērojamus traucējumus sociālo un saimniecisko darbību parastajā norisē.
- (35) Izglītībā un apmācībā izmantotās AI sistēmas, īpaši piekļuves noteikšanai vai personu uzņemšanai izglītības un arodmacību iestādēs, vai personu izvērtēšanai tādu pārbaudījumu ietvaros, kas ir daļa no izglītības procesa vai priekšnosacījums izglītības iegūšanai, būtu jāuzskata par augsta riska sistēmām, jo tās var noteikt izglītības vai profesionālo ievirzi personas dzīvē un tādējādi ietekmēt personas iespēju nopelnīt iztiku. Ja šādas sistēmas ir nepareizi projektētas un izmantotas, tās var pārkāpt tiesības uz izglītību un apmācību, kā arī tiesības uz nediskriminēšanu, un nostiprināt vēsturiskos diskriminācijas modeļus.
- (36) AI sistēmas, kuras izmanto nodarbinātībā, darba ņēmēju pārvaldībā un piekļuvē pašnodarbinātībai, īpaši personu darbā līgšanas un atlases nolūkos, lēmumu pieņemšanā par paaugstināšanu amatā vai atlaišanu no darba, uzdevumu sadalē un darba līgumattiecībās esošu personu pārraudzībā vai izvērtēšanā, arī būtu jāklasificē kā augsta riska sistēmas, jo tās var ievērojami ietekmēt karjeras iespējas nākotnē un attiecīgo personu labklājību. Attiecīgajām darba līgumattiecībām būtu jāietver darba ņēmēji un personas, kuras sniedz pakalpojumus caur platformām, kā norādīts Komisijas darba programmā 2021. gadam. Šādas personas faktiski nebūtu jāuzskata par lietotājiem šīs regulas nozīmē. Darbā līgšanas procesa un izvērtēšanas, paaugstināšanas amatā vai darba līgumattiecību uzturēšanas ietvaros minētās sistēmas var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, attiecībā uz sievietēm, noteiktām vecuma grupām, invalīdiem vai personām ar noteiktu etnisko vai rasisko piederību vai dzimumorientāciju. AI sistēmas, ko izmanto šo personu snieguma un uzvedības pārraudzībai, var arī ietekmēt viņu tiesības uz datu aizsardzību un privātumu.
- (37) Cita joma, kurā AI sistēmu izmantošanai ir jāpievērš īpaša uzmanība, ir piekļuve noteiktiem privātiem un sabiedriskiem pamatpakalpojumiem un pabalstiem, kas cilvēkiem nepieciešami, lai viņi varētu pilnvērtīgi piedalīties sabiedrības norisēs vai uzlabot savu dzīves līmeni, un šādu pakalpojumu un pabalstu izmantošana. Tā, AI sistēmas, ko izmanto fizisku personu kredītnovērtējuma vai kredītspējas izvērtēšanai, būtu jāklasificē kā augsta riska AI sistēmas, jo tās nosaka minēto personu piekļuvi finanšu resursiem vai tādiem būtiskiem pakalpojumiem kā mājoklis, elektroenerģija un telesakaru pakalpojumi. Šim nolūkam izmantotās AI sistēmas var izraisīt personu vai grupu diskrimināciju un atkārtot vēsturiskos diskriminācijas modeļus, piemēram, pamatojoties uz rasisko vai etnisko izcelsmi, invaliditāti, vecumu vai dzimumorientāciju, vai radīt jaunas diskriminējošas ietekmes formas. Ņemot vērā ietekmes ļoti ierobežoto apmēru un tirgū pieejamās alternatīvas, ir lietderīgi noteikt izņēmumu attiecībā uz tām kredītspējas novērtēšanai un kredītnovērtējuma noteikšanai paredzētajām AI sistēmām, kuras pašu vajadzībām ekspluatācijā nodevuši mazapjoma sagādātāji. Fiziskas personas, kuras piesakās sociālās palīdzības pabalstiem un pakalpojumiem vai saņem tos no publiskā sektora iestādēm, parasti ir atkarīgas no šiem pabalstiem un pakalpojumiem un atrodas neaizsargātā pozīcijā attiecībā pret atbildīgajām iestādēm. Ja AI sistēmas izmanto, lai noteiktu, vai šādi pabalsti un pakalpojumi būtu jāatsaka, jāsamazina, jāatsauc vai jāatgūst, tām var būt ievērojama ietekme uz personu labklājību un tās var pārkāpt tādas personu pamattiesības kā

tiesības uz sociālo aizsardzību, nediskriminēšanu, cilvēka cieņas neaizskaramību vai efektīvu tiesību aizsardzību. Tāpēc minētās sistēmas būtu jāklasificē kā augsta riska sistēmas. Tomēr šai regulai nevajadzētu kavēt inovatīvu pieeju izstrādi un izmantošanu valsts pārvaldē, kas gūtu labumu no prasībām atbilstošu un drošu AI sistēmu plašākas izmantošanas ar nosacījumu, ka minētās sistēmas nerada augstu risku fiziskām un juridiskām personām. Visbeidzot, AI sistēmas, ko izmanto ārkārtas pirmās reaģēšanas dienestu nosūtīšanai vai šo dienestu nosūtīšanas prioritāšu noteikšanai, arī būtu jāklasificē kā augsta riska sistēmas, jo tās pieņem lēmumus personu veselībai un dzīvībai un to īpašumam izšķirīgi svarīgās situācijās.

- (38) Tiesībaizsardzības iestāžu darbībām, kuras ietver noteiktus AI sistēmu izmantošanas veidus, ir raksturīga ievērojama varas nelīdzsvarotības pakāpe, un to rezultāts var būt novērošana, aizturēšana vai fiziskas personas brīvības atņemšana, kā arī cita veida nelabvēlīga ietekme uz Pamattiesību hartā nostiprinātajām pamattiesībām. Proti, ja AI sistēma nav apmācīta ar augstas kvalitātes datiem, neatbilst precizitātes vai noturības prasībām vai nav pienācīgi projektēta un testēta pirms laišanas tirgū vai citādas nodošanas ekspluatācijā, tā var norādīt uz cilvēkiem diskriminējošu vai kā citādi nekorektā vai netaisnīgā veidā. Bez tam var tikt traucēta būtisku procesuālo pamattiesību, piemēram, tiesību uz efektīvu tiesību aizsardzību un taisnīgu tiesu, kā arī tiesību uz aizstāvību un nevainīguma prezumpcijas, īstenošana, it īpaši, ja minētās AI sistēmas nav pietiekami pārredzamas, izskaidrojamas un dokumentētas. Tāpēc ir lietderīgi klasificēt kā augsta riska sistēmas vairākas AI sistēmas, kas paredzētas izmantošanai tiesībaizsardzības kontekstā, kurā precizitāte, uzticamība un pārredzamība ir īpaši svarīga, lai novērstu kaitējošu ietekmi, saglabātu sabiedrības uzticēšanos un nodrošinātu pārskatatbildību un efektīvu tiesisko aizsardzību. Ņemot vērā attiecīgo darbību raksturu un ar tām saistītos riskus, pie minētajām augsta riska AI sistēmām būtu galvenokārt jāpieskaita AI sistēmas, kas paredzētas izmantošanai tiesībaizsardzības iestādēs individuālam riska novērtējumam, melu detektoros un līdzīgos rīkos fiziskas personas emocionālā stāvokļa noteikšanai, “dziļviltojumu” konstatēšanai, pierādījumu uzticamības izvērtēšanai kriminālprocesa ietvaros, faktiska vai potenciāla noziedzīga nodarījuma izdarīšanas vai atkārtotas izdarīšanas prognozēšanai, pamatojoties uz fizisku personu profilēšanu vai novērtējot fizisku personu vai grupu personiskās īpašības un rakstura iezīmes vai iepriekšēju noziedzīgu rīcību, profilēšanai noziedzīgu nodarījumu atklāšanas, izmeklēšanas vai kriminālvajāšanas gaitā, kā arī noziegumu analīzei attiecībā uz fiziskām personām. AI sistēmas, kuras īpaši paredzētas izmantošanai administratīvajā procesā nodokļu un muitas iestādēs, nebūtu jāuzskata par augsta riska AI sistēmām, ko tiesībaizsardzības iestādes izmanto noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai un kriminālvajāšanai par tiem.

- (39) Migrācijas un patvēruma jomā un robežkontroles pārvaldībā izmantotās AI sistēmas ietekmē cilvēkus, kuri bieži ir īpaši neaizsargātā pozīcijā un ir atkarīgi no kompetento publiskā sektora iestāžu darbības rezultāta. Tāpēc minētajos kontekstos izmantoto AI sistēmu precizitāte, nediskriminējošais raksturs un pārredzamība ir īpaši svarīga skarto personu pamattiesību ievērošanas garantēšanai, proti, viņu tiesību brīvi pārvietoties, tiesību uz nediskrimināciju, privātuma un persondatu aizsardzību, starptautisko aizsardzību un labu pārvaldību īstenošanai. Tāpēc ir lietderīgi klasificēt kā augsta riska sistēmas tās AI sistēmas, ko kompetentajās publiskā sektora iestādēs, kurām uzticēti pienākumi migrācijas, patvēruma un robežkontroles pārvaldības jomā, paredzēts izmantot kā melu detektorus un līdzīgus rīkus vai nolūkā noteikt fiziskas personas emocionālo stāvokli; novērtēt noteiktus riskus, kurus rada fiziskas personas, kas ieceļo dalībvalsts teritorijā vai piesakās vīzai vai patvērumam; pārbaudīt fizisku personu

attiecīgo dokumentu autentiskumu; sniegt palīdzību kompetentām publiskā sektora iestādēm patvēruma, vīzu un uzturēšanās atļauju pieteikumu un saistīto sūdzību izskatīšanā ar mērķi noteikt fizisku personu, kuras iesniegušas pieteikumu noteikta statusa iegūšanai, atbilstību kritērijiem. AI sistēmām migrācijas, patvēruma un robežkontroles pārvaldības jomā, uz kurām attiecas šī regula, būtu jāatbilst attiecīgajām procesuālajām prasībām, kas noteiktas Eiropas Parlamenta un Padomes Direktīvā 2013/32/ES⁴⁹, Eiropas Parlamenta un Padomes Regulā (EK) Nr. 810/2009⁵⁰ un citos attiecīgajos tiesību aktos.

- (40) Dažas AI sistēmas, kas paredzētas izmantošanai tiesvedībā un demokrātiskajos procesos, būtu jāklasificē kā augsta riska sistēmas, ņemot vērā to potenciāli ievērojamo ietekmi uz demokrātiju, tiesiskumu, individuālajām brīvībām, kā arī tiesībām uz efektīvu tiesību aizsardzību un taisnīgu tiesu. Proti, lai mazinātu potenciālu neobjektivitātes, kļūdu un nepārredzamības risku, ir lietderīgi uzskatīt par augsta riska sistēmām tās AI sistēmas, kuru mērķis ir palīdzēt tiesu iestādēm faktu un tiesību normu izpētē un interpretēšanā un tiesību normu piemērošanā konkrētam faktu kopumam. Tomēr šāda klasifikācija nebūtu jāattiecinā uz AI sistēmām, kuras paredzētas tikai tādu administratīvu papilddarbību veikšanai, kam nav ietekmes uz faktisko tiesvedību atsevišķās lietās, piemēram, tiesas nolēmumu, dokumentu vai datu anonimizācijai vai pseidonimizācijai, saziņai starp darbiniekiem, administratīvu uzdevumu veikšanai vai resursu sadalei.
- (41) Fakts, ka AI sistēma saskaņā ar šo regulu ir klasificēta kā augsta riska sistēma, nebūtu jāinterpretē kā norāde, ka sistēmas izmantošana obligāti ir likumīga citu Savienības tiesību aktu vai ar tiem saderīgu valsts tiesību aktu ietvaros, piemēram, attiecībā uz persondatu aizsardzību, melu detektoru un tamlīdzīgu rīku vai citu sistēmu izmantošanu fizisku personu emocionālā stāvokļa noteikšanai. Tāda izmantošana būtu jāturpina tikai saskaņā ar piemērojamajām prasībām, kas izriet no Pamattiesību hartas un attiecīgajiem Savienības sekundārajiem tiesību aktiem un dalībvalstu tiesību aktiem. Nebūtu jāuzskata, ka šī regula nodrošina juridisko pamatu persondatu apstrādei, attiecīgā gadījumā ieskaitot īpašu kategoriju persondatus.
- (42) Lai mazinātu Savienības tirgū laisto vai citādi ekspluatācijā nodoto augsta riska AI sistēmu radītos riskus lietotājiem un skartajām personām, būtu jāpiemēro dažas obligātas prasības, ņemot vērā paredzēto sistēmas izmantošanas nolūku un saskaņā ar riska pārvaldības sistēmu, kura sagādātājam jāizveido.
- (43) Prasībām būtu jāattiecas uz augsta riska AI sistēmām saistībā ar izmantoto datu kopu kvalitāti, tehnisko dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu lietotājiem, cilvēka virsvadību un noturību, precizitāti un kiberdrošību. Minētās prasības ir nepieciešamas, lai efektīvi mazinātu riskus veselībai, drošībai un pamattiesībām, tās ir piemērojamas, ņemot vērā sistēmas paredzēto nolūku, un citi tirdzniecību mazāk ierobežojoši pasākumi nav pienācīgi pieejami, tādējādi netiek radīti nepamatoti tirdzniecības ierobežojumi.
- (44) Augsta datu kvalitāte ir nepieciešama daudzu AI sistēmu veikspējai, it īpaši, ja tiek izmantotas metodes, kas ietver modeļu apmācīšanu, ar mērķi nodrošināt, ka augsta

⁴⁹ Eiropas Parlamenta un Padomes Direktīva 2013/32/ES (2013. gada 26. jūnijs) par kopējām procedūrām starptautiskās aizsardzības statusa piešķiršanai un atņemšanai (OV L 180, 29.6.2013., 60. lpp.).

⁵⁰ Eiropas Parlamenta un Padomes Regula (EK) Nr. 810/2009 (2009. gada 13. jūlijs), ar ko izveido Kopienas Vīzu kodeksu (Vīzu kodekss) (OV L 243, 15.9.2009., 1. lpp.).

riska AI sistēma darbojas, kā paredzēts, un droši un tā neklūst par Savienības tiesību aktos aizliegtas diskriminācijas avotu. Augstas kvalitātes apmācības, validēšanas un testēšanas datu kopām ir svarīga atbilstošas datu pārvaldes un pārvaldības īstenošana. Apmācības, validēšanas un testēšanas datu kopām vajadzētu būt pietiekami atbilstošām, reprezentatīvām, bez kļūdām un pilnīgām, ņemot vērā sistēmas paredzēto nolūku. Tām vajadzētu piemist arī atbilstošiem statistiskajiem raksturlielumiem, arī attiecībā uz personām vai personu grupām, ar kurām paredzēts izmantot konkrēto augsta riska AI sistēmu. Proti, apmācības, validēšanas un testēšanas datu kopās apmērā, ko nosaka to paredzētais nolūks, vajadzētu ņemt vērā iezīmes, raksturlielumus vai elementus, kas raksturīgi konkrētajai ģeogrāfiskajai, uzvedības vai funkcionālajai videi vai kontekstam, kurā paredzēts izmantot AI sistēmu. Lai citu tiesības aizsargātu pret diskrimināciju, kas varētu izrietēt no AI sistēmu neobjektivitātes, sagādātājiem būtu jāvar apstrādāt arī īpašu kategoriju persondatus svarīgās vispārības interesēs ar mērķi nodrošināt neobjektivitātes uzraudzību, atklāšanu un korekciju augsta riska AI sistēmās.

- (45) Augsta riska AI sistēmu izstrādes nolūkā noteiktiem dalībniekiem, piemēram, sagādātājiem, pieteiktajām struktūrām un citām attiecīgajām struktūrām, piemēram, digitālās inovācijas centriem, testēšanas un eksperimentēšanas struktūrām un pētniekiem, jāvar piekļūt augstas kvalitātes datu kopām un izmantot tās savās attiecīgajās darbības jomās, kas ir saistītas ar šo regulu. Komisijas izveidotās Eiropas vienotās datu telpas un datu kopīgošanas atvieglošana uzņēmumu starpā un ar valdības iestādēm vispārības interešu labā būs ļoti būtiska, lai nodrošinātu uzticēšanos raisošu, pārskatāmu un nediskriminējošu piekļuvi augstas kvalitātes datiem AI sistēmu apmācībai, validēšanai un testēšanai. Piemēram, veselības jomā Eiropas veselības datu telpa veicinās nediskriminējošu piekļuvi veselības jomas datiem un mākslīgā intelekta algoritmu apmācībai šajās datu kopās privātumu saglabājošā, drošā, laicīgā, pārredzamā un uzticamā veidā ar pienācīgu iestāžu pārvaldi. Arī attiecīgās kompetentās iestādes, ieskaitot nozaru iestādes, nodrošinot vai atbalstot piekļuvi datiem, var atbalstīt augstas kvalitātes datu piegādāšanu AI sistēmu apmācībai, validēšanai un testēšanai.
- (46) Informācija par to, kā izstrādātas augsta riska AI sistēmas un kā tās darbojas to darbmūžā, ir ļoti būtiska, lai pārbaudītu atbilstību šajā regulā noteiktajām prasībām. Tam nepieciešama uzskaitē un tādas tehniskās dokumentācijas pieejamība, kura satur informāciju, kas nepieciešama, lai novērtētu AI sistēmas atbilstību attiecīgajām prasībām. Šādai informācijai būtu jāietver ziņas par sistēmas vispārīgajiem raksturlielumiem, spējām un ierobežojumiem, algoritmiem, datiem, apmācību, izmantotajiem testēšanas un validēšanas procesiem, kā arī attiecīgās riska pārvaldības sistēmas dokumentācija. Tehniskā dokumentācija būtu pastāvīgi jāaktualizē.
- (47) Lai mazinātu nepārredzamību, kas dažas AI sistēmas padara fiziskām personām nesaprotamas vai pārāk sarežģītas, augsta riska AI sistēmām būtu jānosaka noteikta pārredzamības pakāpe. Lietotājiem būtu jāspēj interpretēt sistēmas iznākumus un tos atbilstoši izmantot. Tāpēc augsta riska AI sistēmām būtu jāpievieno attiecīgā dokumentācija un lietošanas instrukcijas, kā arī īsa un skaidra informācija, tostarp attiecīgā gadījumā par iespējamajiem pamattiesību riskiem un diskrimināciju.
- (48) Augsta riska AI sistēmas būtu jāprojektē un jāizstrādā tā, lai fiziskas personas varētu pārraudzīt to funkcionēšanu. Šajā nolūkā sistēmas sagādātājam pirms sistēmas laišanas tirgu vai nodošanas ekspluatācijā būtu jānosaka piemēroti cilvēka virsvadības pasākumi. Tā, attiecīgā gadījumā šādiem pasākumiem jāgarantē, ka sistēmai ir iebūvēti ierobežojumi, kurus pati sistēma nevar neievērot, un ka tā reaģē uz cilvēka virsvadību

un ka fiziskām personām, kurām uzticēta šī virsvadība, ir uzdevuma veikšanai nepieciešamā kompetence, apmācība un pilnvaras.

- (49) Augsta riska AI sistēmām jādarbojas konsekventi visā to darbībā un jānodrošina atbilstošs precizitātes, noturības un kiberdrošības līmenis saskaņā ar vispāratzīto tehnoloģiju attīstības līmeni. Precizitātes līmenis un tā rādītāji jā dara zināmi lietotājiem.
- (50) Tehniskā noturība ir viena no galvenajām prasībām augsta riska AI sistēmām. Minētajām sistēmām jābūt noturīgām pret riskiem, kas ir saistīti ar sistēmas ierobežojumiem (piemēram, kļūdas, nepilnības, neatbilstības, negaidītas situācijas), kā arī pret ļaunprātīgām darbībām, kuras var apdraudēt AI sistēmas drošību un izraisīt kaitējošu vai citādi nevēlamu sistēmas darbību. Nespēja aizsargāt pret šiem riskiem varētu ietekmēt drošību vai negatīvi ietekmēt pamattiesības, piemēram, AI sistēmas radītu kļūdainu lēmumu vai nepareizu vai neobjektīvu iznākumu dēļ.
- (51) Kiberdrošībai ir būtiska loma, nodrošinot, ka AI sistēmas ir noturīgas pret mēģinājumiem mainīt to lietojumu, uzvedību vai veikspēju vai apdraudēt to drošības iezīmes, ļaunprātīgām trešām personām ekspluatējot sistēmas vājās vietas. Kiberuzbrukumi AI sistēmām var izmantot AI raksturīgos aktīvus, piemēram, apmācībā izmantotās datu kopas (piemēram, datu saindēšana) vai apmācītos modeļus (piemēram, adversatīvie uzbrukumi) vai ekspluatēt AI sistēmas digitālo aktīvu vai pamatā esošās IKT infrastruktūras vājās vietas. Lai nodrošinātu riskiem atbilstošu kiberdrošības līmeni, augsta riska AI sistēmu sagādātājiem būtu jāveic piemēroti pasākumi, attiecīgi ņemot vērā arī pamatā esošo IKT infrastruktūru.
- (52) Kā daļa no Savienības saskaņošanas tiesību aktiem augsta riska AI sistēmu laišanai tirdzniecībā, nodošanai ekspluatācijā un izmantošanai piemērojamie noteikumi būtu jānosaka saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008⁵¹, ar ko nosaka akreditācijas un tirgus uzraudzības prasības produktiem, Eiropas Parlamenta un Padomes Lēmumu Nr. 768/2008/EK⁵² par produktu tirdzniecības vienotu sistēmu un Eiropas Parlamenta un Padomes Regulu (ES) 2019/1020⁵³ par tirgus uzraudzību un produktu atbilstību ("produktu tirdzniecības Jaunais tiesiskais regulējums").
- (53) Ir lietderīgi, ka konkrēta fiziska vai juridiska persona, kas definēta kā sagādātājs, uzņemas atbildību par augsta riska AI sistēmas laišanu tirgū vai nodošanu ekspluatācijā neatkarīgi no tā, vai attiecīgā fiziskā vai juridiskā persona pati ir šīs sistēmas projektētājs vai izstrādātājs.
- (54) Sagādātājam jāizveido stabila kvalitātes vadības sistēma, jānodrošina nepieciešamās atbilstības novērtēšanas procedūras pabeigšana, jāizstrādā attiecīgā dokumentācija un jāizveido spēcīga pēctirgus uzraudzības sistēma. Publiskā sektora iestādes, kuras nodod ekspluatācijā augsta riska AI sistēmu pašu izmantošanai, var pieņemt un īstenot kvalitātes vadības sistēmas noteikumus valsts vai reģionālā līmenī pieņemtas

⁵¹ Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

⁵² Eiropas Parlamenta un Padomes Lēmums Nr. 768/2008/EK (2008. gada 9. jūlijs) par produktu tirdzniecības vienotu sistēmu un ar ko atceļ Padomes Lēmumu 93/465/EEK (OV L 218, 13.8.2008., 82. lpp.).

⁵³ Eiropas Parlamenta un Padomes Regula (ES) 2019/1020 (2019. gada 20. jūnijs) par tirgus uzraudzību un produktu atbilstību un ar ko groza Direktīvu 2004/42/EK un Regulas (EK) Nr. 765/2008 un (ES) Nr. 305/2011 (Dokuments attiecas uz EEZ) (OV L 169, 25.6.2019., 1.–44. lpp.).

kvalitātes vadības sistēmas ietvaros, attiecīgi ņemot vērā nozares īpatnības un attiecīgās publiskā sektora iestādes kompetences un struktūru.

- (55) Ja augsta riska AI sistēma, kas ir drošības sastāvdaļa produktā, kuru skar attiecīgi Jaunā tiesiskā regulējuma nozaru tiesību akti, nav laista tirgū vai nodota ekspluatācijā neatkarīgi no produkta, attiecīgajā Jaunā tiesiskā regulējuma tiesību aktā definētajam gatavā produkta ražotājam būtu jāizpilda šajā regulā noteiktie sagādātāja pienākumi un, galvenais, jānodrošina, ka gatavajā produktā iegultā AI sistēma atbilst šīs regulas prasībām.
- (56) Lai nodrošinātu šīs regulas izpildi un radītu vienlīdzīgus konkurences apstākļus ekonomikas dalībniekiem, un ņemot vērā dažādās formas, kā digitālos produktus var darīt pieejamus, ir svarīgi nodrošināt, ka Savienībā iedibināta persona jebkuros apstākļos var iestādēm sniegt visu nepieciešamo informāciju par AI sistēmas atbilstību. Tāpēc, pirms darīt savas AI sistēmas pieejamas Savienībā, ja importētāju nevar identificēt, ārpus Savienības iedibinātiem sagādātājiem ar rakstisku pilnvaru jāieceļ Savienībā iedibināts pilnvarots pārstāvis.
- (57) Saskaņā ar Jaunā tiesiskā regulējuma principiem attiecīgajiem ekonomikas dalībniekiem (piemēram, importētājiem un izplatītājiem) būtu jānosaka zināmi pienākumi ar mērķi nodrošināt juridisko noteiktību un veicināt minēto ekonomikas dalībnieku normatīvo atbilstību.
- (58) Ņemot vērā AI sistēmu raksturu un iespējamos riskus drošībai un pamattiesībām, kas saistīti ar to izmantošanu, tostarp attiecībā uz nepieciešamību nodrošināt AI sistēmas veiktspējas reālos apstākļos pienācīgu uzraudzību, ir lietderīgi noteikt zināmus pienākumus lietotājiem. Lietotājiem būtu jāizmanto augsta riska AI sistēmas saskaņā ar lietošanas instrukcijām, un būtu jānosaka daži citi pienākumi attiecībā uz AI sistēmu funkcionēšanas uzraudzību un uzskaiti vajadzības gadījumā.
- (59) Ir lietderīgi paredzēt, ka AI lietotājam vajadzētu būt fiziskai vai juridiskai personai, publiskā sektora iestādei, aģentūrai vai citai struktūrai, kuras pārziņā darbojas AI sistēma, izņemot, ja izmantošana notiek personīgas, neprofesionālas darbības ietvaros.
- (60) Ņemot vērā mākslīgā intelekta vērtības ķēdes sarežģītību, attiecīgajām trešām personām, proti, tām, kuras ir iesaistītas programmatūras, programmatūras rīku un sastāvdaļu, iepriekš apmācītu modeļu un datu tirdzniecībā un piegādē, vai tīkla pakalpojumu sniedzējiem vajadzības gadījumā būtu jāsadarbojas ar sagādātājiem un lietotājiem, lai ļautu tiem nodrošināt atbilstību šajā regulā noteiktajiem pienākumiem, kā arī tiem būtu jāsadarbojas ar šajā regulā noteiktajām kompetentajām iestādēm.
- (61) Standartizācijai vajadzētu būt ļoti būtiskai tādu tehnisko risinājumu nodrošināšanā, kas sistēmu sagādātājiem ļautu nodrošināt atbilstību šīs regulas noteikumiem. Atbilstībai Eiropas Parlamenta un Padomes Regulā (ES) Nr. 1025/2012⁵⁴ noteiktajiem saskaņotajiem standartiem vajadzētu būt veidam, kā sagādātāji var demonstrēt atbilstību šīs regulas prasībām. Tomēr Komisija varētu pieņemt kopīgas tehniskās specifikācijas jomās, kurās nav saskaņotu standartu vai tie nav pietiekami.

⁵⁴

Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

- (62) Lai nodrošinātu augsta riska AI sistēmu augstu uzticamības līmeni, būtu jāveic šo sistēmu atbilstības novērtēšana pirms to laišanas tirgū vai nodošanas ekspluatācijā.
- (63) Lai mazinātu slogu uz ekonomikas dalībniekiem un novērstu iespējamo dublēšanos, attiecībā uz augsta riska AI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas esošie Savienības saskaņošanas tiesību akti saskaņā ar Jaunā tiesiskā regulējuma pieeju, ir lietderīgi, ka minēto sistēmu atbilstību šīs regulas prasībām vajadzētu novērtēt minētajos tiesību aktos jau paredzētās atbilstības novērtēšanas ietvaros. Tādējādi šīs regulas prasību piemērojamībai nevajadzētu ietekmēt attiecīgajā Jaunā tiesiskā regulējuma tiesību aktā paredzētās atbilstības novērtēšanas īpašo loģiku, metodiku vai vispārīgo struktūru. Minētajai pieejai pilnīgi atbilst mijiedarbība starp šo regulu un [Mašīnu regulu]. Lai gan drošības riski, kas saistīti ar AI sistēmām, kuras veic drošības funkcijas mašīnās, ir risināti šīs regulas prasībās, dažas specifiskas [Mašīnu regulas] prasības nodrošinās drošu AI sistēmas integrēšanu kopējā mašīnā ar mērķi negatīvi neietekmēt mašīnas drošību kopumā. [Mašīnu regulā] izmantota tāda pati AI sistēmas definīcija, kā šajā regulā.
- (64) Ņemot vērā, ka profesionāliem sertificētajiem, kuri darbojas pirmstirdzniecības posmā, ir plašāka pieredze produktu drošuma jomā, kā arī saistīto risku atšķirīgo raksturu, vismaz sākotnējā šīs regulas piemērošanas posmā ir lietderīgi ierobežot trešās personas veiktas atbilstības novērtēšanas piemērošanas jomu tādām augsta riska AI sistēmām, kuras nav saistītas ar produktiem. Tāpēc minēto sistēmu atbilstības novērtēšanu parasti būtu jāveic sagādātājam uz savu atbildību, izņemot vienīgi AI sistēmas, kuras paredzēts izmantot personu biometriskajai tālidentifikācijai; šādā gadījumā būtu jāparedz pieteiktās struktūras iesaiste atbilstības novērtēšanā, ciktāl minētās sistēmas nav aizliegtas.
- (65) Lai īstenotu fizisku personu biometriskajai tālidentifikācijai paredzētu AI sistēmu trešās personas veiktu atbilstības novērtēšanu, valstu kompetentajām iestādēm saskaņā ar šo regulu būtu jānorīko pieteiktās struktūras ar nosacījumu, ka tās atbilst prasību kopumam, it īpaši neatkarības, kompetences un interešu konflikta neesības ziņā.
- (66) Saskaņā ar vispārārstīto būtisku modifikāciju jēdzienu, ko attiecina uz Savienības saskaņošanas tiesību aktu regulētajiem produktiem, ir lietderīgi, ka AI sistēmai veic jaunu atbilstības novērtēšanu ikreiz, kad notikušas izmaiņas, kas var ietekmēt sistēmas atbilstību šīs regulas noteikumiem, vai mainījies sistēmas paredzētais nolūks. Turklāt to AI sistēmu gadījumā, kuras pēc laišanas tirgū vai nodošanas ekspluatācijā turpina “mācīties” (t. i., tās automātiski pielāgo veidu, kādā tās veic funkcijas), ir nepieciešams pieņemt noteikumus, kas nosaka, ka tādas izmaiņas algoritmā un tā sniegunā, kuras sagādātājs ir iepriekš noteicis un novērtējis atbilstības novērtēšanas procesā, nav uzskatāmas par būtiskām modifikācijām.
- (67) Augsta riska AI sistēmām jābūt marķētām ar zīmi *CE*, atspoguļojot to atbilstību šīs regulas noteikumiem, kas ļautu tām būt brīvā apritē iekšējā tirgū. Dalībvalstīm nevajadzētu radīt nepamatotus šķēršļus tādu augsta riska AI sistēmu laišanai tirgū vai nodošanai ekspluatācijā, kuras atbilst šajā regulā noteiktajām prasībām un ir marķētas ar *CE* zīmi.
- (68) Noteiktos apstākļos ātra inovatīvu tehnoloģiju pieejamība var būt ļoti svarīga personu veselībai un drošībai, kā arī sabiedrībai kopumā. Līdz ar to ir lietderīgi, ka ar sabiedrisko drošību vai fizisku personu veselības un drošības aizsardzību un rūpnieciskā un komerciālā īpašuma aizsardzību saistītos ārkārtas apstākļos dalībvalstis varētu atļaut laist tirgū vai nodot ekspluatācijā AI sistēmas, kurām nav veikta atbilstības novērtēšana.

- (69) Lai veicinātu Komisijas un dalībvalstu darbu mākslīgā intelekta jomā, kā arī vairotu pārredzamību sabiedrībai, būtu jānosaka prasība tādu augsta riska AI sistēmu, kuras nav saistītas ar produktiem, uz kuriem attiecas esošie Savienības saskaņošanas tiesību akti, sagādātājiem reģistrēt savas augsta riska AI sistēmas ES datubāzē, ko izveidos un pārvaldīs Komisija. Komisijai vajadzētu būt minētās datubāzes pārzinei saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725⁵⁵. Lai nodrošinātu datubāzes pilnīgu funkcionalitāti pēc tās darbības sākšanas, datubāzes izveides procedūrā būtu jāietver Komisijas veikta funkcionālo specifikāciju izstrāde un neatkarīgs revīzijas ziņojums.
- (70) Dažas AI sistēmas, kas paredzētas saskarsmei ar fiziskām personām vai satura radīšanai, var radīt īpašu uzdošanās par citu personu vai apmānīšanas risku neatkarīgi no tā, vai tās ir pieskaitāmas augsta riska sistēmām vai nav. Tāpēc noteiktos apstākļos šādu sistēmu izmantošanai būtu jānosaka īpaši pārredzamības pienākumi, neskarot augsta riska AI sistēmām noteiktās prasības un pienākumus. Īpaši – fiziskas personas būtu jāinformē, ka tās ir saskarsmē ar AI sistēmu, ja vien tas nav pats par sevi saprotams attiecīgajos apstākļos un izmantošanas kontekstā. Turklāt fiziskām personām būtu jāpaziņo, ja tās ir pakļautas emociju uztveršanas sistēmas vai biometriskās kategorizācijas sistēmas darbībai. Šāda informācija un paziņojumi būtu jāsniedz invalīdiem izmantojamā formātā. Turklāt lietotājiem, kuri izmanto AI sistēmu tāda attēla, audio vai video satura radīšanai vai manipulēšanai, kas ievērojami atgādina reālas personas, vietas vai notikumus un cilvēkam maldinoši šķistu autentisks, būtu jāizpauž tas, ka saturs ir mākslīgi radīts vai manipulēts, attiecīgi marķējot mākslīgā intelekta radīto iznākumu un atklājot tā mākslīgo izcelsmi.
- (71) Mākslīgais intelekts ir strauji attīstošos tehnoloģiju kopums, kam nepieciešamas nebijušas regulatīvās uzraudzības formas un droša vide eksperimentēšanai, vienlaikus nodrošinot atbildīgu inovāciju un atbilstošu aizsardzības un riska mazināšanas pasākumu integrēšanu. Lai nodrošinātu inovācijai labvēlīgu, nākotnes prasībām atbilstošu un pret traucējumiem noturīgu tiesisko regulējumu, vienas vai vairāku dalībvalstu kompetentās iestādes būtu jā mudina veidot mākslīgā intelekta “regulatīvās smilškastēs” ar mērķi veicināt inovatīvu AI sistēmu izstrādi un testēšanu stingrā regulatīvajā uzraudzībā, pirms šīs sistēmas laiž tirgū vai citādi nodod ekspluatācijā.
- (72) “Regulatīvo smilškastu” mērķiem jābūt veicināt AI inovāciju, radot vadītu eksperimentēšanas un testēšanas vidi izstrādes un pirmstirdzniecības posmā ar nolūku nodrošināt inovatīvu AI sistēmu atbilstību šīs regulas noteikumiem un citiem attiecīgajiem Savienības un dalībvalstu tiesību aktiem; uzlabot juridisko noteiktību novatoriem un kompetento iestāžu uzraudzību un izpratni par iespējām, jauniem riskiem un AI izmantošanas ietekmi un paātrināt piekļuvi tirgum, tostarp novēršot šķēršļus maziem un vidējiem uzņēmumiem (MVU) un jaunuzņēmumiem. Lai nodrošinātu vienotu īstenošanu visā Savienībā un apjomradītus ietaupījumus, ir lietderīgi noteikt kopīgus noteikumus “regulatīvo smilškastu” īstenošanai un sistēmu sadarbībai starp attiecīgajām iestādēm, kuras iesaistītas “smilškastu” uzraudzībā. Šai regulai jānodrošina juridiskais pamats persondatu, kas savākti citiem nolūkiem, izmantošanai noteiktu AI sistēmu izstrādē vispārības interesēs AI “regulatīvās smilškastēs” ietvaros saskaņā ar Regulas (ES) 2016/679 6. panta 4. punktu un Regulas (ES) 2018/1725 6. pantu un neskarot Direktīvas (ES) 2016/680 4. panta 2. punktu.

⁵⁵

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

“Smilškastēs” dalībniekiem būtu jānodrošina atbilstoši aizsardzības pasākumi un jāsadarbojas ar kompetentajām iestādēm, tostarp sekojot to norādēm un rīkojoties efektīvi un labticīgi, lai mazinātu jebkādus augstus riskus drošībai un pamattiesībām, kas varētu rasties “smilškastē” veiktās izstrādes un eksperimentēšanas gaitā. Kompetentajām iestādēm būtu jāņem vērā dalībnieku rīcība “smilškastē”, lemjot, vai uzlikt administratīvu naudas sodu saskaņā ar Regulas (ES) 2016/679 83. panta 2. punktu un Direktīvas (ES) 2016/680 57. pantu.

- (73) Inovācijas veicināšanas un aizsardzības nolūkā ir svarīgi īpaši ņemt vērā AI sistēmu mazapjoma sagādātāju un lietotāju intereses. Šā mērķa sasniegšanai dalībvalstīm būtu jāizstrādā iniciatīvas, kas ir vērstas uz šiem operatoriem, arī saistībā ar izpratnes veicināšanu un informēšanu. Turklāt mazapjoma sagādātāju intereses un vajadzības pieteiktajām struktūrām būtu jāņem vērā, nosakot maksu par atbilstības novērtēšanu. Ar obligāto dokumentāciju un saziņu ar iestādēm saistītie tulkošanas izdevumi var radīt ievērojamas izmaksas sagādātājiem un citiem ekonomikas dalībniekiem, īpaši mazākiem. Iespējams, ka dalībvalstīm vajadzētu nodrošināt, ka viena no valodām, ko tās nosaka un pieņem kā valodu attiecīgās sagādātāju dokumentācijas sagatavošanai un saziņai ar operatoriem, ir valoda, kuru plaši saprot pēc iespējas lielāks pārrobežu lietotāju skaits.
- (74) Lai minimalizētu ar īstenošanu saistītos riskus, kas izriet no zināšanu un zinātības trūkuma tirgū, kā arī veicinātu sagādātāju un pieteikto struktūru pienākumu izpildi saskaņā ar šo regulu, platformai “MI pēc pieprasījuma”, Eiropas digitālās inovācijas centriem un testēšanas un eksperimentēšanas struktūrām, kuras Komisija un dalībvalstis izveidojušas valstu vai Savienības līmenī, iespējams, būtu jāpalīdz šīs regulas īstenošanā. Minētās iestādes savu attiecīgo uzdevumu un kompetences ietvaros varētu nodrošināt tehnisko un zinātnisko atbalstu sagādātājiem un pieteiktajām struktūrām.
- (75) Ir lietderīgi, ka Komisija struktūrām, grupām vai laboratorijām, kuras izveidotas vai akreditētas saskaņā ar attiecīgajiem Savienības saskaņošanas tiesību aktiem un izpilda uzdevumus to produktu vai ierīču, uz kuriem attiecas minētie Savienības saskaņošanas tiesību akti, atbilstības novērtēšanas kontekstā, cik vien iespējams atvieglo piekļuvi testēšanas un eksperimentēšanas struktūrām. Tas īpaši attiecas uz ekspertu grupām, ekspertu laboratorijām un references laboratorijām medicīnisko ierīču jomā saskaņā ar Regulu (ES) 2017/745 un Regulu (ES) 2017/746.
- (76) Lai sekmētu netraucētu, efektīvu un saskaņotu šīs regulas īstenošanu, būtu jāizveido Eiropas Mākslīgā intelekta padome (“AI padome”). AI padome atbildētu par vairākiem padomdošanas uzdevumiem, ieskaitot atzinumu, ieteikumu, padomu vai pamatnostādņu izdošanu jautājumos, kas saistīti ar šīs regulas īstenošanu, tostarp par tehniskajām specifikācijām vai pašreizējiem standartiem attiecībā uz šajā regulā noteiktajām prasībām, kā arī par Komisijas konsultēšanu un palīdzību tai specifiskos mākslīgā intelekta jautājumos.
- (77) Dalībvalstīm ir būtiska loma šīs regulas piemērošanā un izpildē. Šajā ziņā katrai dalībvalstij būtu jānorīko viena vai vairākas valsts kompetentās iestādes šīs regulas piemērošanas un īstenošanas uzraudzībai. Lai vairotu dalībvalstu organizatorisku efektivitāti un izveidotu oficiālu kontaktpunktu saziņai ar sabiedrību un citiem partneriem dalībvalstu un Savienības līmenī, viena valsts iestāde katrā dalībvalstī būtu jāieceļ par valsts uzraudzības iestādi.
- (78) Lai nodrošinātu, ka augsta riska AI sistēmu sagādātāji pieredzi minēto sistēmu izmantošanā var ņemt vērā, uzlabojot savas sistēmas un projektēšanas un izstrādes

procesu, vai savlaicīgi veikt iespējamus korektīvos pasākumus, visiem sagādātājiem būtu jāizveido pēctirgus uzraudzības sistēma. Minētā sistēma ir svarīga arī, lai varētu efektīvi un savlaicīgi novērst iespējamus riskus, kas rodas, AI sistēmām turpinot “mācīties” pēc to laišanas tirgū vai nodošanas ekspluatācijā. Šajā kontekstā būtu jānosaka, ka sagādātājiem ir jāizveido sistēma ar mērķi paziņot attiecīgajām iestādēm par to AI sistēmu izmantošanas izraisītiem nopietniem incidentiem vai pārkāpumiem attiecībā uz valsts un Savienības tiesību aktiem, kuri aizsargā pamattiesības.

- (79) Lai nodrošinātu šajā regulā, kas ir Savienības saskaņošanas tiesību akts, noteikto prasību un pienākumu pienācīgu un iedarbīgu izpildi, ar Regulu (ES) 2019/1020 izveidotā tirgus uzraudzības un produktu atbilstības sistēma būtu jāpiemēro pilnā mērā. Kad tas nepieciešams to pilnvaru īstenošanai, valstu publiskā sektora iestādēm vai struktūrām, tostarp līdztiesības iestādēm, kuras uzrauga Savienības tiesību aktu, kuri aizsargā pamattiesības, piemērošanu, vajadzētu būt piekļuvei jebkādi dokumentācijai, kas radīta saskaņā ar šo regulu.
- (80) Savienības tiesību akti finansiālo pakalpojumu jomā ietver iekšējās pārvaldes un riska pārvaldības noteikumus un prasības, kuras attiecas uz regulētām finanšu iestādēm minēto pakalpojumu sniegšanas gaitā, arī tad, kad tās izmanto AI sistēmas. Lai nodrošinātu šajā regulā noteikto pienākumu un Savienības finanšu pakalpojumu tiesību aktu attiecīgo noteikumu un prasību saskaņotu piemērošanu un izpildi, par finanšu pakalpojumu tiesību aktu uzraudzību un izpildi atbildīgās iestādes, tostarp attiecīgos gadījumos Eiropas Centrālā Banka, būtu jāieceļ par kompetentajām iestādēm šīs regulas īstenošanas uzraudzībai, ieskaitot tirgus uzraudzības pasākumus, attiecībā uz AI sistēmām, kuras sagādā vai izmanto regulētas un uzraudzītas finanšu iestādes. Lai vēl vairāk uzlabotu saskaņotību starp šo regulu un noteikumiem, kuri attiecas uz kredītiestādēm, kas regulētas saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2013/36/ES⁵⁶, ir lietderīgi atbilstības novērtēšanas procedūru un dažus sagādātāju procesuālos pienākumus saistībā ar riska pārvaldību, pēctirgus uzraudzību un dokumentāciju integrēt arī pašreizējos pienākumos un procedūrās, kas noteiktas Direktīvā 2013/36/ES. Lai novērstu pārklāšanos, būtu jāparedz arī ierobežotas atkāpes attiecībā uz sagādātāju kvalitātes vadības sistēmām un uzraudzības pienākumiem, kas noteikti augsta riska AI sistēmu lietotājiem, ciktāl tie attiecas uz Direktīvas 2013/36/ES regulētajām kredītiestādēm.
- (81) Tādu AI sistēmu, kas nav augsta riska AI sistēmas, izstrāde saskaņā ar šīs regulas prasībām varētu izraisīt uzticama mākslīgā intelekta plašāku ieviešanu Savienībā. Tādu AI sistēmu sagādātāji, kas nav augsta riska sistēmas, būtu jāmudina izstrādāt rīcības kodeksus, kuru mērķis būtu veicināt augsta riska AI sistēmām piemērojamo obligāto prasību brīvprātīgu piemērošanu. Tāpat sagādātāji jāmudina brīvprātīgi piemērot papildu prasības, kas ir saistītas, piemēram, ar vides ilgtspēju, pieejamību invalīdiem, ieinteresēto personu līdzdalību AI sistēmu projektēšanā un izstrādē un daudzveidību izstrādes grupās. Komisija var izstrādāt iniciatīvas, ieskaitot nozaru iniciatīvas, ar mērķi veicināt tādu tehnisko šķēršļu mazināšanu, kuri kavē pārrobežu datu apmaiņu AI izstrādei, tostarp par datu piekļuves infrastruktūru un dažādu veidu datu semantisko un tehnisko savietojamību.

⁵⁶

Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).

- (82) Ir svarīgi, lai ar produktiem saistītas AI sistēmas, kuras nav augsta riska sistēmas saskaņā ar šo regulu un kurām līdz ar to nav jāatbilst šajā regulā noteiktajām prasībām, tomēr būtu drošas, kad tās tiek laistas tirgū vai nodotas ekspluatācijā. Minētā mērķa sekmēšanas nolūkā Eiropas Parlamenta un Padomes Direktīva 2001/95/EK⁵⁷ tiktu piemērota kā drošības tīkls.
- (83) Lai nodrošinātu uzticēšanās pilnu un konstruktīvu sadarbību starp kompetentajām iestādēm Savienības un valstu līmenī, visām šīs regulas piemērošanā iesaistītajām personām būtu jāievēro savu uzdevumu veikšanas gaitā iegūtās informācijas un datu konfidencialitāte.
- (84) Dalībvalstīm jāveic šīs regulas noteikumu īstenošanas nodrošināšanai nepieciešamie pasākumi, tostarp jānosaka iedarbīgi, samērīgi un atturoši sodi par noteikumu pārkāpumiem. Dažu specifisku pārkāpumu gadījumā dalībvalstīm jāņem vērā šajā regulā noteiktās robežas un kritēriji. Eiropas Datu aizsardzības uzraudzītājam jābūt pilnvarotam uzlikt naudas sodus Savienības iestādēm, aģentūrām un struktūrām, uz kurām attiecas šī regula.
- (85) Lai nodrošinātu, ka tiesisko regulējumu vajadzības gadījumā iespējams pielāgot, būtu jāpiešķir Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu ar mērķi grozīt I pielikumā minētās metodes un pieejas AI sistēmu definēšanai, II pielikumā uzskaitītos Savienības saskaņošanas tiesību aktus, augsta riska AI sistēmu sarakstu III pielikumā, noteikumus par IV pielikumā uzskaitīto tehnisko dokumentāciju, V pielikumā iekļautās ES atbilstības deklarācijas saturu, noteikumus par VI un VII pielikumā minētajām atbilstības novērtēšanas procedūrām un noteikumus, ar ko nosaka augsta riska AI sistēmas, kurām būtu jāpiemēro atbilstības novērtēšanas procedūra, pamatojoties uz kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtēšanu. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu attiecīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu⁵⁸. Proti, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.
- (86) Lai nodrošinātu vienotus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir Komisijai īstenošanas pilnvaras. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011⁵⁹.
- (87) Ņemot vērā to, ka šīs regulas mērķus nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet tās mēroga un iedarbības dēļ tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar LES 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai.
- (88) Šī regula jāpiemēro no ... [OP – norādīt 85. pantā noteikto datumu]. Tomēr ar pārvaldi un atbilstības novērtēšanu saistītajai infrastruktūrai jādarbojas pirms minētā

⁵⁷ Eiropas Parlamenta un Padomes Direktīva 2001/95/EK (2001. gada 3. decembris) par produktu vispārēju drošību (OV L 11, 15.1.2002., 4. lpp.).

⁵⁸ OV L 123, 12.5.2016., 1. lpp.

⁵⁹ Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

datuma, tāpēc noteikumi par pieteiktajām struktūrām un pārvaldes struktūru būtu jāpieņem no ... [OP – norādīt datumu – trīs mēneši pēc šīs regulas stāšanās spēkā]. Turklāt dalībvalstīm jānosaka noteikumi par sodiem, ieskaitot administratīvos naudas sodus, un tie jā dara zināmi Komisijai, un jānodrošina to pienācīga un efektīva īstenošana līdz šīs regulas piemērošanas sākuma dienai. Tāpēc noteikumi par sodiem jāpieņem no [OP – norādīt datumu – divpadsmit mēneši pēc šīs regulas stāšanās spēkā].

- (89) Saskaņā ar Regulas (ES) 2018/1725 42. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju un Eiropas Datu aizsardzības kolēģiju, kuri [...] sniedza atzinumu,

IR PIENĒMUŠI ŠO REGULU.

I SADAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Priekšmets

Šī regula nosaka:

- (a) saskaņotus noteikumus par mākslīgā intelekta sistēmu ("AI sistēmas") laišanu tirgū, nodošanu ekspluatācijā un izmantošanu Savienībā;
- (a) noteiktas mākslīgā intelekta prakses aizliegumus;
- (b) īpašas prasības augsta riska AI sistēmām un pienākumus tādu sistēmu operatoriem;
- (c) saskaņotus pārredzamības noteikumus par AI sistēmām, kas paredzētas saskarsmei ar fiziskām personām, emociju uztveršanas sistēmām un biometriskās kategorizācijas sistēmām, kā arī AI sistēmām, ko izmanto, lai radītu vai manipulētu ar attēlu, audio vai video saturu;
- (d) tirgus kontroles un uzraudzības noteikumus.

2. pants

Darbības joma

1. Šī regula attiecas uz:

- (a) sagādātājiem, kas Savienībā laiž tirgū vai nodod ekspluatācijā AI sistēmas, neatkarīgi no tā, vai šie sagādātāji ir iedibināti Savienībā vai trešā valstī;
- (b) Savienībā esošu AI sistēmu lietotājiem;
- (c) tādu AI sistēmu sagādātājiem un lietotājiem, kas atrodas trešā valstī, ja sistēmas radītos iznākumus izmanto Savienībā.

2. Tikai šīs regulas 84. pantu piemēro augsta riska AI sistēmām, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas un uz kurām attiecas tālāk norādītie tiesību akti:

- (a) Regula (EK) Nr. 300/2008;
- (b) Regula (ES) Nr. 167/2013;

- (c) Regula (ES) Nr. 168/2013;
 - (d) Direktīva 2014/90/ES;
 - (e) Direktīva (ES) 2016/797;
 - (f) Regula (ES) 2018/858;
 - (g) Regula (ES) 2018/1139;
 - (h) Regula (ES) 2019/2144.
3. Šī regula neattiecas uz AI sistēmām, kas izstrādātas vai tiek izmantotas vienīgi militāriem mērķiem.
 4. Šī regula neattiecas uz publiskā sektora iestādēm trešā valstī un starptautiskām organizācijām, kas ir šīs regulas piemērošanas jomā saskaņā ar 1. punktu, ja šīs iestādes vai organizācijas izmanto AI sistēmas saskaņā ar starptautiskiem nolīgumiem par tiesībaizsardzības un tiesu iestāžu sadarbību ar Savienību vai ar vienu vai vairākām dalībvalstīm.
 5. Šī regula neietekmē to noteikumu piemērošanu, kuri attiecas uz starpnieku pakalpojumu sniedzēju atbildību un ir izklāstīti Eiropas Parlamenta un Padomes Direktīvas 2000/31/EK⁶⁰ II nodaļas IV iedaļā [*ko aizstās ar attiecīgiem noteikumiem Digitālo pakalpojumu aktā*].

3. pants *Definīcijas*

Šajā regulā piemēro šādas definīcijas:

- (1) “mākslīgā intelekta sistēma” (AI sistēma) ir programmatūra, kas izstrādāta, izmantojot vienu vai vairākas I pielikumā uzskaitītās metodes un pieejas, un attiecībā uz cilvēka noteiktu konkrētu mērķu kopumu var radīt tādu iznākumu kā saturs, prognozes, ieteikumi vai lēmumi, kuri ietekmē vidi, ar ko tie mijiedarbojas;
- (2) “sagādātājs” ir fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura par samaksu vai par brīvu izstrādā vai liek izstrādāt AI sistēmu laišanai tirgū vai nodošanai ekspluatācijā ar savu vārdu vai preču zīmi;
- (3) “mazapjoma sagādātājs” ir sagādātājs, kas ir mikrouzņēmums vai mazais uzņēmums Komisijas Ieteikuma 2003/361/EK nozīmē⁶¹;
- (4) “lietotājs” ir fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura izmanto AI sistēmu, kas ir tās pārziņā, izņemot gadījumus, kad AI sistēmu izmanto personiskas neprofesionālas darbības veikšanai;
- (5) “pilnvarots pārstāvis” ir fiziska vai juridiska persona, kas iedibināta Savienībā un saņēmusi rakstisku pilnvarojumu no AI sistēmas sagādātāja, lai tā vārdā attiecīgi veiktu un pildītu šajā regulā noteiktos pienākumus un procedūras;

⁶⁰ Eiropas Parlamenta un Padomes Direktīva 2000/31/EK (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) (OV L 178, 17.7.2000., 1. lpp.).

⁶¹ Komisijas 2003. gada 6. maija Ieteikums par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

- (6) “importētājs” ir fiziska vai juridiska persona, kas iedibināta Savienībā un laiž tirgū vai nodod ekspluatācijā AI sistēmu ar ārpus Savienības iedibinātas fiziskas vai juridiskas personas nosaukumu vai preču zīmi;
- (7) “izplatītājs” piegādes ķēdē ir fiziska vai juridiska persona, kas nav sagādātājs vai importētājs un kas AI sistēmu dara pieejamu Savienības tirgū, neietekmējot tās īpašības;
- (8) “operators” ir sagādātājs, lietotājs, pilnvarotais pārstāvis, importētājs vai izplatītājs;
- (9) “laist tirgū” ir pirmo reizi AI sistēmu darīt pieejamu Savienības tirgū;
- (10) “darīt pieejamu tirgū” ir par samaksu vai par brīvu piegādāt AI sistēmu izplatīšanai vai izmantošanai Savienības tirgū, veicot komercdarbību;
- (11) “nodošana ekspluatācijā” ir AI sistēmas piegāde pirmajai lietošanai tieši lietotājam vai pašu lietošanai Savienības tirgū tai paredzētajam nolūkam;
- (12) “paredzētais nolūks” ir lietojums, kam sagādātājs ir paredzējis AI sistēmu, arī īpašais konteksts un lietošanas nosacījumi, kas noteikti sagādātāja sniegtajā informācijā, kas iekļauta lietošanas instrukcijā, reklāmas vai pārdošanas materiālos un paziņojumos, kā arī tehniskajā dokumentācijā;
- (13) “pamatoti paredzama nepareiza lietošana” ir AI sistēmas lietošana tādā veidā, kas neatbilst tai paredzētajam nolūkam, bet var rasties no pamatoti paredzamas cilvēku rīcības vai sistēmas mijiedarbības ar citām sistēmām;
- (14) “produkta vai sistēmas drošības sastāvdaļa” ir produkta vai sistēmas sastāvdaļa, kura pilda šā produkta vai sistēmas drošības funkciju vai kuras atteice vai darbības traucējumi apdraud cilvēku veselību un drošību vai mantas drošību;
- (15) “lietošanas instrukcija” ir informācija, ko sniedzis sagādātājs, lai lietotāju informētu galvenokārt par AI sistēmai paredzēto nolūku un pareizu lietošanu, ietverot īpašo ģeogrāfisko, uzvedības vai funkcionālo vidi, kurā paredzēts lietot attiecīgo augsta riska AI sistēmu;
- (16) “AI sistēmas atsauksana” ir katrs pasākums, kura mērķis ir panākt lietotājiem pieejamās AI sistēmas atpakaļnodošanu sagādātājam;
- (17) “AI sistēmas izņemšana” ir katrs pasākums, kura mērķis ir novērst AI sistēmas izplatīšanu, demonstrēšanu un piedāvāšanu;
- (18) “AI sistēmas veikspēja” ir AI sistēmas spēja sasniegt paredzēto nolūku;
- (19) “pieteicējiestāde” ir valsts iestāde, kas atbild par vajadzīgo procedūru izveidi un izpildi atbilstības novērtēšanas struktūru novērtēšanai, norīkošanai un pieteikšanai, kā arī to uzraudzībai;
- (20) “atbilstības novērtēšana” ir process, kurā pārbauda, vai ir izpildītas šīs regulas III sadaļas 2. nodaļā noteiktās prasības, kas attiecas uz AI sistēmu;
- (21) “atbilstības novērtēšanas struktūra” ir struktūra, kas kā trešā persona veic atbilstības novērtēšanas darbības, ieskaitot testēšanu, sertifikēšanu un pārbaudi;
- (22) “pieteiktā struktūra” ir atbilstības novērtēšanas struktūra, kas norīkota saskaņā ar šo regulu un citiem attiecīgajiem Savienības saskaņošanas tiesību aktiem;
- (23) “būtiska modifikācija” ir izmaiņas AI sistēmā pēc tās laišanas tirgū vai nodošanas ekspluatācijā, kuras ietekmē AI sistēmas atbilstību šīs regulas III sadaļas 2. nodaļā

izklāstītajām prasībām vai kuru rezultātā tiek mainīts paredzētais nolūks, attiecībā pret kuru šī AI sistēma ir novērtēta;

- (24) “atbilstības zīme “CE”” (zīme “CE”) ir marķējums, ar kuru sagādātājs norāda, ka AI sistēma atbilst šīs regulas III sadaļas 2. nodaļas prasībām un citu tādu piemērojamo Savienības tiesību aktu prasībām, kas saskaņo produktu tirdzniecības nosacījumus (“Savienības saskaņošanas tiesību akti”) un kas paredz tās uzlikšanu;
- (25) “pēctirgus uzraudzība” ir visas darbības, ko AI sistēmu sagādātāji veic, lai proaktīvi apkopotu un pārskatītu pieredzi, kura iegūta, lietojot AI sistēmas, ko tie laiž tirgū vai nodod ekspluatācijā, ar mērķi identificēt vajadzību nekavējoties piemērot nepieciešamos korektīvos vai preventīvos pasākumus;
- (26) “tirgus uzraudzības iestāde” ir valsts iestāde, kas veic darbības un pasākumus saskaņā ar Regulu (ES) 2019/1020;
- (27) “saskaņots standarts” ir Eiropas standarts kas atbilst Regulas (ES) Nr. 1025/2012 2. panta 1. punkta c) apakšpunkta definīcijai;
- (28) “kopīgas specifikācijas” ir dokuments, kas nav standarts, bet satur tehniskus risinājumus, kuri nodrošina līdzekļus kādu šajā regulā noteiktu prasību un pienākumu izpildei;
- (29) “apmācības dati” ir dati, ko izmanto AI sistēmas apmācībai, pielāgojot tās apgūstamos parametrus, tostarp neironu tīkla svērumus;
- (30) “validēšanas dati” ir dati, ko izmanto apmācītās AI sistēmas izvērtēšanai un tās neapgūstamo parametru un mācību procesa pielāgošanai, lai cita starpā novērstu pārmērīgu pielāgošanu; validēšanas datu kopa var būt atsevišķa datu kopa vai apmācības datu kopas daļa, kā vai nu fiksēts, vai mainīgs tās sadalījums;
- (31) “testēšanas dati” ir dati, ko izmanto, lai nodrošinātu apmācītās un validētas AI sistēmas neatkarīgu izvērtēšanu nolūkā apstiprināt šīs sistēmas sagaidāmo veikspēju pirms tās laišanas tirgū vai nodošanas ekspluatācijā;
- (32) “ievaddati” ir AI sistēmā ievadītie vai tās tieši iegūtie dati, pamatojoties uz kuriem, šī sistēma rada iznākumu;
- (33) “biometriskie dati” ir persondati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprināt minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopiskie dati;
- (34) “emociju uztveršanas sistēma” ir AI sistēma, kuras mērķis ir identificēt vai izsecināt fizisku personu emocijas vai nodomus, pamatojoties uz viņu biometriskajiem datiem;
- (35) “biometriskās kategorizācijas sistēma” ir AI sistēma, kuras mērķis ir noteikt fizisku personu piederību noteiktām kategorijām, piemēram, tādām kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, etniskā izcelsme vai seksuālā vai politiskā orientācija, pamatojoties uz viņu biometriskajiem datiem;
- (36) “biometriskās tālidentifikācijas sistēma” ir AI sistēma, kuras mērķis ir identificēt fiziskas personas no attāluma, salīdzinot personas biometriskos datus ar atsaucēs datubāzē esošiem biometriskajiem datiem, AI sistēmas lietotājam iepriekš nezinot, vai attiecīgā persona būs klāt un varēs tikt identificēta;
- (37) “reāllaika biometriskās tālidentifikācijas sistēma” ir biometriskās tālidentifikācijas sistēma, kurā biometrisko datu uztveršana, salīdzināšana un identificēšana notiek bez

būtiskas aiztures. Lai novērstu apiešanu –tas ietver ne tikai tūlītēju identifikāciju, bet arī ierobežotu īslaicīgu aizturi;

- (38) “vēlāklaika biometriskās tālidentifikācijas sistēma” ir biometriskās tālidentifikācijas sistēma, kas nav reāllaika biometriskās tālidentifikācijas sistēma;
- (39) “sabiedriska vieta” ir jebkura fiziska vieta, kas pieejama sabiedrībai, neatkarīgi no tā, ka šim nolūkam var būt piemēroti noteikti piekļuves nosacījumi;
- (40) “tiesībaizsardzības iestāde” ir
 - (a) publiskā sektora iestāde, kuras kompetencē ir noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai saukšana pie atbildības par tiem, vai kriminālsodu izpilde, arī aizsardzība pret sabiedriskās drošības apdraudējumiem un to novēršana; vai
 - (b) cita struktūra vai vienība, kurai saskaņā ar dalībvalsts tiesību aktiem ir uzticēts īstenot publisku varu un publiskas pilnvaras, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai aizsargātu no draudiem sabiedriskajai drošībai un tos novērstu;
- (41) “tiesībaizsardzība” ir darbības, ko veic tiesībaizsardzības iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai aizsargātu no draudiem sabiedriskajai drošībai un tos novērstu;
- (42) “valsts uzraudzības iestāde” ir iestāde, kurai dalībvalsts uzliek atbildību par šīs regulas īstenošanu un piemērošanu, par šai dalībvalstij uzticēto darbību koordinēšanu, par tās kā vienotā kontaktpunkta ar Komisiju lomu un attiecīgās dalībvalsts pārstāvēšanu Eiropas Mākslīgā intelekta padomē;
- (43) “valsts kompetentā iestāde” ir valsts uzraudzības iestāde, pieteicējierstāde un tirgus uzraudzības iestāde;
- (44) “nopietns incidents” ir jebkurš incidents, kas tieši vai netieši izraisa, būtu varējis izraisīt vai varētu izraisīt kādas no šīm sekām:
 - (a) personas nāve vai nopietns kaitējums personas veselībai, īpašumam vai videi;
 - (b) nopietni un neatgriezeniski kritiskās infrastruktūras pārvaldības un darbības traucējumi.

4. pants

Grozījumi I pielikumā

Komisijai piešķir pilnvaras pieņemt deleģētos aktus saskaņā ar 73. pantu, lai veiktu grozījumus I pielikumā ietvertajā metožu un pieeju sarakstā ar mērķi atjaunināt šo sarakstu atbilstoši tirgus un tehnoloģiju attīstībai, pamatojoties uz īpašībām, kas ir līdzīgas tām metodēm un pieejām, kas tajā uzskaitītas.

II SADAĻA

AIZLIEGTA MĀKSLĪGĀ INTELEKTA PRAKSE

5. pants

1. Ir aizliegta šāda mākslīgā intelekta prakse:

- (a) tādas AI sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kura izmanto subliminālus paņēmienus, lai būtiski iespaidotu personas uzvedību tādā veidā, kas šai vai citai personai rada vai var radīt fizisku vai psiholoģisku kaitējumu;
- (b) tādas AI sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kura izmanto kādu no specifiskas personu grupas neaizsargātības iezīmēm ar viņu vecuma vai fiziskās vai garīgās invaliditātes dēļ, lai būtiski iespaidotu šai grupai piederīgas personas uzvedību tā, ka šai vai citai personai tiek vai var tikt radīts fizisks vai psiholoģisks kaitējums;
- (c) AI sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana, ko veic publiskā sektora iestādes vai to vārdā fiziskas personas, lai izvērtētu vai klasificētu fizisku personu uzticamību noteiktā laikposmā, pamatojoties uz viņu sociālo uzvedību vai zināmām vai prognozētām personas vai personības īpašībām, ja sociālais novērtējums ved pie viena vai abiem šādiem iznākumiem:
 - i) kaitīga vai nelabvēlīga apiešanās ar noteiktām fiziskām personām vai veselām to grupām sabiedriskajā vidē, kas nav saistīta ar vidi, kurā dati sākotnēji radīti vai savākti;
 - ii) kaitīga vai nelabvēlīga apiešanās ar noteiktām fiziskām personām vai veselām to grupām, kas nav pamatota vai nav samērīga ar viņu sociālo uzvedību vai tās smagumu;
- (d) reāllaika biometriskās tālidentifikācijas sistēmu izmantošana sabiedriskās vietās tiesībsargāšanas nolūkos, ja tāda izmantošana nav stingri nepieciešama kādam no šiem mērķiem:
 - i) mērķtiecīga konkrētu noziegumos potenciāli cietušo, arī pazudušu bērnu meklēšana;
 - ii) īpaša, būtiska un nenovēršama apdraudējuma fizisku personu dzīvībai vai fiziskai drošībai vai teroristu uzbrukuma nepieļaušana;
 - iii) vainīgā vai aizdomās turētā atklāšana, vietas noteikšana, identificēšana vai saukšana pie atbildības par noziedzīgu nodarījumu, kas minēts Padomes Pamatlēmuma 2002/584/TI⁶² 2. panta 2. punktā un par ko attiecīgajā dalībvalstī var sodīt ar brīvības atņemšanu vai piemērot ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz trīs gadi, kā noteikts attiecīgās dalībvalsts tiesību aktos.

⁶²

Padomes Pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

2. Izmantojot reāllaika biometriskās tālidentifikācijas sistēmas sabiedriskās vietās tiesībaizsardzības nolūkos ar kādu no 1. punkta d) apakšpunktā minētajiem mērķiem, ņem vērā šādus elementus:

- (a) tās situācijas raksturs, kuras dēļ var būt nepieciešama tāda lietošana, it īpaši kaitējuma smagums, iespējamība un apmērs, kas rastos, sistēmu nelietojot;
- (b) sistēmas izmantošanas sekas attiecībā uz visu iesaistīto personu tiesībām un brīvībām, it īpaši šo seku smagums, iespējamība un apmērs.

Turklāt reāllaika biometriskās tālidentifikācijas sistēmu lietošanā sabiedriskās vietās tiesībaizsardzības nolūkos 1. punkta d) apakšpunktā minētajiem mērķiem jāatbilst nepieciešamiem un samērīgiem aizsardzības pasākumiem un lietošanas nosacījumiem, it īpaši laika, ģeogrāfisku un personu ierobežojumu ziņā.

3. Attiecībā uz 1. punkta d) apakšpunktu un 2. punktu katrai reāllaika biometriskās tālidentifikācijas sistēmas lietošanai tiesībaizsardzības nolūkos sabiedriskās vietās ir nepieciešama iepriekšēja atļauja, ko izsniegusi tiesu iestāde vai tās dalībvalsts neatkarīga administratīva iestāde, kurā šo sistēmu paredzēts izmantot, un kas izsniegta pēc pamatota pieprasījuma un saskaņā ar sīki izstrādātiem valsts tiesību aktu noteikumiem, kā minēts 4. punktā. Pienācīgi pamatotā steidzamā gadījumā sistēmas lietošanu var sākt bez atļaujas un atļauju pieprasīt tikai lietošanas laikā vai pēc tās.

Kompetentā tiesas vai pārvaldes iestāde piešķir atļauju tikai tad, ja pēc tai iesniegtiem objektīviem pierādījumiem vai skaidrām norādēm pārliecinās, ka attiecīgās reāllaika biometriskās tālidentifikācijas sistēmas izmantošana ir nepieciešama un samērīga, lai sasniegtu vienu no 1. punkta d) apakšpunktā norādītajiem mērķiem, kas norādīts pieteikumā. Lemjot par pieteikumu, kompetentā tiesas vai pārvaldes iestāde ņem vērā 2. punktā minētos elementus.

4. Dalībvalsts var nolemt noteikt iespēju pilnīgi vai daļēji atļaut reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu sabiedriskās vietās tiesībaizsardzības vajadzībām, ievērojot ierobežojumus un nosacījumus, kas uzskaitīti 1. punkta d) apakšpunktā un 2. un 3. punktā. Minētā dalībvalsts savos tiesību aktos nosaka vajadzīgos sīki izstrādātos noteikumus par 3. punktā minēto atļauju pieteikšanu, izdošanu un izmantošanu, kā arī to attiecīgo uzraudzību. Minētajos noteikumos arī norāda, attiecībā uz kuriem no 1. punkta d) apakšpunktā uzskaitītajiem mērķiem – tai skaitā kuru minētā apakšpunkta iii) punktā norādīto noziedzīgo nodarījumu gadījumā – kompetentajām iestādēm var atļaut šīs sistēmas izmantot tiesībaizsardzības vajadzībām.

III SADAĻA

AUGSTA RISKĀ AI SISTĒMAS

1. NODAĻA

AI SISTĒMU KLASIFICĒŠANA PAR AUGSTA RISKĀ AI SISTĒMĀM

6. pants

Noteikumi klasifikācijai par augsta riska AI sistēmām

1. Neatkarīgi no tā, vai AI sistēmu laiž tirgū vai nodod ekspluatācijā neatkarīgi no a) un b) apakšpunktā minētajiem produktiem, šo AI sistēmu uzskata par augsta riska sistēmu, ja ir izpildīti abi šie nosacījumi:
 - (a) AI sistēmu paredzēts izmantot kā produkta drošības sastāvdaļu, vai tā pati par sevi ir produkts, uz kuru attiecas Savienības saskaņošanas tiesību akti, kas uzskaitīti II pielikumā;
 - (b) produktam, kura drošības sastāvdaļa ir AI sistēma, vai arī pašai AI sistēmai kā produktam ir jāveic trešās personas veikts atbilstības novērtējums, lai to varētu laist tirgū vai nodot ekspluatācijā saskaņā ar Savienības saskaņošanas tiesību aktiem, kas uzskaitīti II pielikumā.
2. Papildus 1. punktā minētajām augsta riska AI sistēmām arī III pielikumā minētās AI sistēmas uzskata par augsta riska sistēmām.

7. pants

Grozījumi III pielikumā

1. Komisijai piešķir pilnvaras pieņemt deleģētos aktus saskaņā ar 73. pantu, lai atjauninātu III pielikumā ietvertu sarakstu, pievienojot augsta riska AI sistēmas, ja izpildīti abi šie nosacījumi:
 - (a) AI sistēmas ir paredzētas lietošanai jebkurā no III pielikuma 1.–8. punktā uzskaitītajām jomām;
 - (b) AI sistēmas rada kaitējuma risku attiecībā uz veselību un drošību vai nelabvēlīgu ietekmi uz pamattiesībām, t. i., tāda kaitējuma risku, kura smagums un iestāšanās iespējamība ir līdzvērtīga vai lielāka par kaitējuma vai nelabvēlīgas ietekmes risku, ko rada augsta riska AI sistēmas, kuras jau minētas III pielikumā.
2. Atbilstoši 1. punktam vērtējot, vai AI sistēma izraisa risku, ka radīsies kaitējums veselībai un drošībai vai nelabvēlīga ietekme uz pamattiesībām, kas ir vienāds vai lielāks par kaitējuma risku, kuru rada augsta riska AI sistēmas, kas jau minētas III pielikumā, Komisija ņem vērā šādus kritērijus:
 - (a) AI sistēmas paredzētais nolūks;
 - (b) kādā mērā AI sistēma ir lietota vai ir domājams, ka tiks lietota;
 - (c) kādā mērā AI sistēmas lietošana jau ir nodarījusi kaitējumu veselībai un drošībai vai izraisījusi nelabvēlīgu ietekmi uz pamattiesībām, vai raisījusi nopietnas bažas par šāda kaitējuma vai nelabvēlīgas ietekmes iestāšanos, kā

liecina ziņojumi vai dokumentēti apgalvojumi, kas iesniegti valsts kompetentajām iestādēm;

- (d) šāda kaitējuma vai šādas nelabvēlīgas ietekmes iespējamais apmērs, it īpaši attiecībā uz to intensitāti un spēju skart daudzus cilvēkus;
- (e) kādā mērā potenciāli cietušās vai nelabvēlīgi ietekmētās personas ir atkarīgas no AI sistēmas radītā iznākuma, sevišķi tāpēc, ka praktisku vai juridisku iemeslu dēļ nav pamatoti iespējams atteikties no tāda iznākuma izmantošanas;
- (f) kādā mērā potenciāli cietušās vai nelabvēlīgi ietekmētās personas ir neaizsargātā stāvoklī attiecībā pret AI sistēmas lietotāju, it īpaši varas, zināšanu, ekonomisko vai sociālo apstākļu vai vecuma izraisītas nelīdzsvarotības dēļ;
- (g) kādā mērā ar AI sistēmu iegūtais iznākums ir viegli izlabojams; turklāt iznākumus, kas ietekmē cilvēku veselību vai drošību, neuzskata par viegli izlabojamiem;
- (h) kādā mērā spēkā pašreizējie Savienības tiesību akti nosaka:
 - i) efektīvus tiesiskās aizsardzības pasākumus saistībā ar AI sistēmas radītajiem riskiem, izņemot prasības par zaudējumu atlīdzību;
 - ii) efektīvus pasākumus minēto risku novēršanai vai būtiskai samazināšanai.

2. NODAĻA

PRASĪBAS AUGSTA RISKĀ AI SISTĒMĀM

8. pants

Atbilstība prasībām

1. Augsta riska AI sistēmas atbilst šajā nodaļā noteiktajām prasībām.
2. Nodrošinot atbilstību šīm prasībām, ņem vērā paredzēto augsta riska AI sistēmas nolūku un 9. pantā minēto riska pārvaldības sistēmu.

9. pants

Riska pārvaldības sistēma

1. Saistībā ar augsta riska AI sistēmām izveido, ievieš, dokumentē un uztur riska pārvaldības sistēmu.
2. Riska pārvaldības sistēmu veido nepārtraukts iteratīvs process visā augsta riska AI sistēmas darbībā, un tam nepieciešama regulāra sistemātiska atjaunināšana. Tajā ietilpst šādi posmi:
 - (a) ar katru augsta riska AI sistēmu saistīto zināmo un paredzamo risku identificēšana un analīze;
 - (b) to risku aprēķināšana un izvērtēšana, kas var rasties, ja augsta riska AI sistēmu lieto atbilstoši paredzētajam nolūkam un pamatoti paredzamas nepareizas lietošanas apstākļos;
 - (c) citu iespējamo risku izvērtēšana, pamatojoties uz to datu analīzi, kas iegūti no 61. pantā minētās pēctirgus uzraudzības sistēmas;

- (d) piemērotu riska pārvaldības pasākumu pieņemšana saskaņā ar turpmāko punktu noteikumiem.
3. Riska pārvaldības pasākumos, kas minēti 2. punkta d) apakšpunktā, pienācīgi ņem vērā sekas un iespējamo mijiedarbību, ko rada šajā 2. nodaļā izklāstīto prasību kombinēta piemērošana. Tajos ņem vērā vispāratzīto tehnoloģiju attīstības līmeni, ieskaitot to, kas atspoguļots attiecīgajos saskaņotos standartos vai kopīgās specifikācijās.
4. Riska pārvaldības pasākumi, kas minēti 2. punkta d) apakšpunktā, ir tādi, ka visi ar katru apdraudējumu saistītie atlikušie riski, kā arī augsta riska AI sistēmu kopējais atlikušais risks tiek uzskatīti par pieņemamiem, ar nosacījumu, ka augsta riska AI sistēmu lieto atbilstoši paredzētajam nolūkam vai pamatoti paredzamas nepareizas lietošanas apstākļos. Par šiem atlikušajiem riskiem paziņo lietotājam.
- Nosakot vispiemērotākos riska pārvaldības pasākumus, nodrošina:
- (a) risku novēršanu vai samazināšanu, ciktāl iespējams, ar atbilstošu projektēšanu un izstrādi;
- (b) attiecīgā gadījumā atbilstīgu riska mazināšanas un kontroles pasākumu īstenošanu attiecībā uz riskiem, kurus nevar novērst;
- (c) atbilstošas informācijas sniegšanu saskaņā ar 13. pantu, it īpaši attiecībā uz riskiem, kas minēti šā panta 2. punkta b) apakšpunktā, un attiecīgā gadījumā lietotāju apmācību.
- Novēršot vai samazinot riskus, kas saistīti ar augsta riska AI sistēmas lietošanu, pienācīgi ņem vērā tehniskās zināšanas, pieredzi, izglītību, apmācību, kas tiek gaidīta attiecībā uz lietotāju, un vidi, kurā sistēmu paredzēts izmantot.
5. Augsta riska AI sistēmas testē, lai noteiktu vispiemērotākos riska pārvaldības pasākumus. Testēšana nodrošina, ka augsta riska AI sistēmas darbojas konsekventi paredzētajam nolūkam un atbilst šajā nodaļā noteiktajām prasībām.
6. Testēšanas procedūras ir piemērotas, lai sasniegtu AI sistēmas paredzēto nolūku, un tajās nav jāpārsniedz tas, kas nepieciešams šā mērķa sasniegšanai.
7. Augsta riska AI sistēmu testēšanu pēc vajadzības veic jebkurā brīdī visā izstrādes procesā un jebkurā gadījumā pirms laišanas tirgū vai nodošanas ekspluatācijā. Testēšanu veic, izmantojot iepriekš noteiktus rādītājus un varbūtības sliekšņus, kas atbilst augsta riska AI sistēmai paredzētajam nolūkam.
8. Ieviešot 1.–7. punktā aprakstīto riska pārvaldības sistēmu, īpašu uzmanību pievērš tam, vai augsta riska AI sistēmai nepieklūs bērni un tā neietekmēs bērnus.
9. Attiecībā uz kredītiestādēm, kuru darbību reglamentē Direktīva 2013/36/ES, 1.–8. punktā aprakstītie aspekti ir daļa no riska pārvaldības procedūrām, ko šīs iestādes izveidojušas saskaņā ar minētās direktīvas 74. pantu.

10. pants

Dati un datu pārvalde

1. Augsta riska AI sistēmas, kurās izmanto metodes, kas saistītas ar modeļu apmācību ar datiem, izstrādā, pamatojoties uz apmācības, validēšanas un testēšanas datu kopām, kas atbilst 2.–5. punktā minētajiem kvalitātes kritērijiem.

2. Apmācības, validēšanas un testēšanas datu kopām piemēro atbilstošu datu pārvaldes un pārvaldības praksi. Šī prakse īpaši attiecas uz:
 - (a) attiecīgām izstrādes izvēlēm;
 - (b) datu vākšanu;
 - (c) attiecīgām datu sagatavošanas darbībām, piemēram, anotēšanu, marķēšanu, tīrīšanu, bagātināšanu un apkopošanu;
 - (d) attiecīgu pieņēmumu formulēšanu, it īpaši attiecībā uz informāciju, kuru šiem datiem vajadzētu izmērīt un attēlot;
 - (e) nepieciešamo datu kopu pieejamības, daudzuma un piemērotības iepriekšēju novērtējumu;
 - (f) iespējamās neobjektivitātes pārbaudi;
 - (g) visu iespējamo datu trūkumu vai nepilnību noteikšanu un to, kā šos trūkumus un nepilnības var novērst.
3. Apmācības, validēšanas un testēšanas datu kopas ir atbilstošas, reprezentatīvas, bez kļūdām un pilnīgas. Tām ir atbilstoši statistiskie raksturlielumi, tostarp vajadzības gadījumā attiecībā uz personām vai personu grupām, saistībā ar kurām paredzēts izmantot konkrēto augsta riska AI sistēmu. Šos datu kopu raksturlielumus var izpildīt atsevišķu datu kopu vai to kombinācijas līmenī.
4. Apmācības, validēšanas un testēšanas datu kopās, ciktāl to nosaka paredzētais nolūks, ņem vērā raksturlielumus vai elementus, kas raksturīgi specifiskajai ģeogrāfiskajai, uzvedības vai funkcionālajai videi, kurā paredzēts lietot augsta riska AI sistēmu.
5. Ciktāl tas ir absolūti nepieciešams, lai nodrošinātu neobjektivitātes uzraudzību, atklāšanu un izlabošanu augsta riska AI sistēmās, šādu sistēmu sagādātāji var apstrādāt īpašu kategoriju persondatus, kas minēti Regulas (ES) 2016/679 9. panta 1. punktā, Direktīvas (ES) 2016/680 10. pantā un Regulas (ES) 2018/1725 10. panta 1. punktā, ievērojot atbilstošus fizisko personu pamattiesību un brīvību aizsardzības pasākumus, tostarp tehniskos ierobežojumus modernāko drošības un privātuma saglabāšanas pasākumu izmantošanā un atkalizmantošanā, piemēram, tādu kā pseidonimizācija vai šifrēšana, ja anonimizācija var būtiski ietekmēt sasniedzamo mērķi.
6. Atbilstošu datu pārvaldes un pārvaldības praksi piemēro augsta riska AI sistēmu izstrādei, izņemot tās sistēmas, kurās tiek izmantotas metodes, kas paredz modeļu apmācību, lai nodrošinātu, ka šīs augsta riska AI sistēmas atbilst 2. punktam.

11. pants

Tehniskā dokumentācija

1. Pirms augsta riska AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā sagatavo šīs sistēmas tehnisko dokumentāciju, un to regulāri atjaunina.

Tehnisko dokumentāciju sagatavo tā, lai parādītu, ka attiecīgā augsta riska AI sistēma atbilst šajā nodaļā noteiktajām prasībām, un valstu kompetentajām iestādēm un pieteiktajām struktūrām sniedz visu nepieciešamo informāciju, lai novērtētu AI sistēmas atbilstību šīm prasībām. Tajā ir vismaz IV pielikumā izklāstītie elementi.

2. Ja tiek laista tirgū vai nodota ekspluatācijā augsta riska AI sistēma, kas saistīta ar produktu, uz kuru attiecas II pielikuma A iedaļā uzskaitītie tiesību akti, sagatavo vienu vienotu tehnisko dokumentāciju, kurā ir visa informācija, kas izklāstīta IV pielikumā, kā arī informācija, kas paredzēta saskaņā ar minētajiem tiesību aktiem.
3. Komisijai piešķir pilnvaras pieņemt deleģētos aktus saskaņā ar 73. pantu, lai veiktu grozījumus IV pielikumā, vajadzības gadījumā nodrošinot, ka, ņemot vērā tehnikas attīstību, tehniskajā dokumentācijā tiek sniegta visa nepieciešamā informācija, kas vajadzīga, lai novērtētu sistēmas atbilstību šajā nodaļā noteiktajām prasībām.

12. pants

Uzskaitē

1. Augsta riska AI sistēmas projektē un izstrādā, paredzot iespējas, kas ļauj automātiski reģistrēt notikumus ("žurnāldatnes") laikā, kad šīs augsta riska AI sistēmas darbojas. Šīs reģistrēšanas iespējas atbilst atzītiem standartiem vai kopīgām specifikācijām.
2. Reģistrēšanas iespējas nodrošina tādu AI sistēmas darbības izsekojamības līmeni visā tās darbībā, kas atbilst sistēmai paredzētajam nolūkam.
3. Proti, reģistrēšanas iespējas ļauj uzraudzīt augsta riska AI sistēmas darbību saistībā ar tādu situāciju rašanos, kurās AI sistēma var radīt risku 65. panta 1. punkta nozīmē vai kurās var notikt būtiska modifikācija, un atvieglo 61. pantā minēto pēctirgus uzraudzību.
4. Augsta riska AI sistēmām, kas minētas III pielikuma 1. punkta a) apakšpunktā, reģistrēšanas iespējas nodrošina vismaz:
 - (a) katras sistēmas lietošanas perioda (katras lietošanas sākuma datums un laiks un beigu datums un laiks) reģistrāciju;
 - (b) informāciju par atsauces datubāzi, salīdzinot ar kuru sistēma pārbaudījusi ievaddatus;
 - (c) ievaddatus, kuru meklēšanas rezultātā ir iegūta atbilstība;
 - (d) rezultātu pārbaudē iesaistīto fizisko personu identifikāciju, kā minēts 14. panta 5. punktā.

13. pants

Pārredzamība un informācijas sniegšana lietotājiem

1. Augsta riska AI sistēmas projektē un izstrādā tā, lai nodrošinātu, ka to darbība ir pietiekami pārredzama, lai lietotāji varētu interpretēt sistēmas iznākumus un tos pienācīgi izmantot. Ir jānodrošina atbilstošs pārredzamības veids un pakāpe, lai panāktu atbilstību attiecīgajiem lietotāja un sagādātāja pienākumiem, kas noteikti šīs sadaļas 3. nodaļā.
2. Augsta riska AI sistēmām pievieno lietošanas instrukciju piemērotā digitālā formātā vai citādi, un tajā ietver kodolīgu, pilnīgu, pareizu un skaidru informāciju, kas ir būtiska, pieejama un saprotama lietotājiem.
3. Šā panta 2. punktā minētā informācija ietver šādas ziņas:
 - (a) sagādātāja un attiecīgā gadījumā tā pilnvarotā pārstāvja identitāte un kontaktinformācija;

- (b) augsta riska AI sistēmas raksturlielumi, iespējas un veikspējas ierobežojumi, tostarp:
 - i) tai paredzētais nolūks;
 - ii) 15. pantā minētais precizitātes, noturības un kiberdrošības līmenis, par kuru ir testēta un validēta attiecīgā augsta riska AI sistēma un kurš var būt gaidāms, un visi zināmie un paredzamie apstākļi, kas var ietekmēt sagaidāmo precizitātes, noturības un kiberdrošības līmeni;
 - iii) zināmie vai paredzamie apstākļi, kas saistīti ar augsta riska AI sistēmas lietošanu atbilstoši tās paredzētajam nolūkam vai pamatoti paredzamas nepareizas lietošanas apstākļos un kas var radīt risku veselībai un drošībai vai pamattiesībām;
 - iv) tās veikspēja attiecībā uz personām vai personu grupām, ar kurām sistēmu paredzēts izmantot;
 - v) attiecīgā gadījumā – ievaddatu specifikācijas vai cita būtiska informācija attiecībā uz izmantotajām apmācības, validēšanas un testēšanas datu kopām, ņemot vērā AI sistēmai paredzēto nolūku;
- (c) izmaiņas augsta riska AI sistēmā un tās veikspējā, kuras sākotnējās atbilstības novērtēšanas brīdī ir noteicis sagādātājs, ja tādas ir;
- (d) cilvēka virsvadības pasākumi, kas minēti 14. pantā, tostarp tehniskie pasākumi, kuri ieviesti, lai palīdzētu lietotājiem interpretēt AI sistēmu iznākumus;
- (e) paredzamais augsta riska AI sistēmas darbmužs un visi uzturēšanas un apkopes pasākumi, kas nepieciešami, lai nodrošinātu šīs AI sistēmas pareizu darbību, arī saistībā ar programmatūras atjauninājumiem.

14. pants

Cilvēka virsvadība

1. Augsta riska AI sistēmas projektē un izstrādā, izmantojot arī atbilstošus cilvēka un mašīnas saskarnes rīkus, tā, lai AI sistēmas lietošanas laikā fiziskas personas to varētu efektīvi pārraudzīt.
2. Cilvēka virsvadības mērķis ir novērst vai mazināt riskus attiecībā uz veselību, drošību vai pamattiesībām, kuri var rasties, ja augsta riska AI sistēmu izmanto atbilstoši paredzētajam nolūkam vai pamatoti paredzamas nepareizas lietošanas apstākļos, it īpaši, ja šādi riski arvien pastāv, neraugoties uz citu šajā nodaļā noteikto prasību piemērošanu.
3. Cilvēka virsvadību nodrošina, izmantojot vienu vai visus šos pasākumus:
 - (a) sagādātājs to identificē un integrē augsta riska AI sistēmā, ja tas ir tehniski iespējams, pirms tās laišanas tirgū vai nodošanas ekspluatācijā;
 - (b) sagādātājs to identificē pirms augsta riska AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā, un lietotājam tā ir pienācīgi īstenojama.
4. Šā panta 3. punktā minētie pasākumi personām, kurām virsvadība uzticēta, atbilstoši apstākļiem nodrošina šādas iespējas:
 - (a) pilnībā izprast augsta riska AI sistēmas iespējas un ierobežojumus un spēt pienācīgi uzraudzīt tās darbību, lai pēc iespējas ātrāk varētu atklāt un novērst novirzu, disfunkciju un neparedzētas darbības pazīmes;

- (b) apzināties iespējamo tendenci automātiski paļauties vai pārāk paļauties uz augsta riska AI sistēmas radītajiem iznākumiem (“automatizācijas neobjektivitāte”), īpaši attiecībā uz augsta riska AI sistēmām, kuras lieto, lai sniegtu informāciju vai ieteikumus lēmumiem, kas jāpieņem fiziskām personām;
 - (c) spēt pareizi interpretēt augsta riska AI sistēmas radīto iznākumu, galvenokārt ņemot vērā sistēmas īpašības un pieejamos interpretācijas rīkus un metodes;
 - (d) spēt katrā atsevišķā situācijā izlemt nelietot augsta riska AI sistēmu vai citādi neievērot, pārņemt vai anulēt augsta riska AI sistēmas darbības iznākumu;
 - (e) spēt iejaukties augsta riska AI sistēmas darbībā vai pārtraukt to, izmantojot pogu “stop” vai līdzīgu procedūru.
5. Attiecībā uz augsta riska AI sistēmām, kas minētas III pielikuma 1. punkta a) apakšpunktā, šā panta 3. punktā minētajiem pasākumiem jābūt tādiem, kas nodrošina, ka lietotājs turklāt neveic nekādas darbības vai nepieņem nekādu lēmumu, pamatojoties uz identifikāciju, kas izriet no attiecīgās sistēmas, ja to nav pārbaudījušas un apstiprinājušas vismaz divas fiziskas personas.

15. pants

Precizitāte, noturība un kiberdrošība

1. Augsta riska AI sistēmas projektē un izstrādā tā, lai tās, ņemot vērā tām paredzēto nolūku, sasniegtu atbilstošu precizitātes, noturības un kiberdrošības līmeni un šajos aspektos konsekvēnti darbotos visu darbību.
2. Augsta riska AI sistēmu precizitātes līmeni un attiecīgos precizitātes rādītājus norāda tām pievienotajā lietošanas instrukcijā.
3. Augsta riska AI sistēmas ir noturīgas pret kļūdām, defektiem vai neatbilstībām, kas var rasties pašā sistēmā vai vidē, kurā attiecīgā sistēma darbojas, it īpaši sistēmas mijiedarbībā ar fiziskām personām vai citām sistēmām.
4. Augsta riska AI sistēmu noturību var panākt ar tehniskiem rezerves risinājumiem, kuru vidū var būt dublēšanas vai atteikdrošības plāni.
5. Augsta riska AI sistēmas, kas turpina mācīties pēc to laišanas tirgū vai nodošanas ekspluatācijā, jāizstrādā tā, lai nodrošinātu, ka jautājums par iespējami neobjektīviem iznākumiem, ko rada izvaddati, kurus izmanto par ievaddatiem nākamās operācijās (“atgriezeniskās saites cilpas”), tiek pienācīgi risināts ar atbilstošiem mazināšanas pasākumiem.
6. Augsta riska AI sistēmām jābūt noturīgām pret nepiederīgu trešo personu mēģinājumiem mainīt to lietojumu vai veikspēju, izmantojot sistēmas ietekmējamību.

Tehniskajiem risinājumiem, kuru mērķis ir nodrošināt augsta riska AI sistēmu kiberdrošību, jāatbilst attiecīgajiem apstākļiem un riskiem.

Tehniskie risinājumi, kas paredzēti, lai novērstu AI specifisko ietekmējamību, attiecīgā gadījumā ietver pasākumus, kuru mērķis ir novērst un kontrolēt uzbrukumus, kuros tiek mēģināts manipulēt ar apmācības datu kopu (“datu saindēšana”), ievaddatiem, kas paredzēti modeļa kļūdas izraisīšanai (“pretrunīgi piemēri”), vai modeļa nepilnībām.

3. NODAĻA

AUGSTA RISKA AI SISTĒMU SAGĀDĀTĀJU UN LIETOTĀJU UN CITU PERSONU PIENĀKUMI

16. pants

Augsta riska AI sistēmu sagādātāju pienākumi

Augsta riska AI sistēmu sagādātāji:

- (a) nodrošina, ka to augsta riska AI sistēmas atbilst šīs sadaļas 2. nodaļā noteiktajām prasībām;
- (b) ievieš kvalitātes vadības sistēmu, kas atbilst 17. pantam;
- (c) sagatavo augsta riska AI sistēmas tehnisko dokumentāciju;
- (d) glabā žurnāldatnes, kuras automātiski ģenerējušas to augsta riska AI sistēmas, ja žurnāldatnes ir viņu pārziņā;
- (e) nodrošina, ka attiecībā uz augsta riska AI sistēmu pirms tās laišanas tirgū vai nodošanas ekspluatācijā tiek veikta atbilstības novērtēšanas procedūra;
- (f) pilda 51. pantā minētos reģistrēšanas pienākumus;
- (g) veic nepieciešamos korektīvos pasākumus, ja augsta riska AI sistēma neatbilst šīs sadaļas 2. nodaļā noteiktajām prasībām;
- (h) par neatbilstību un visiem veiktajiem korektīvajiem pasākumiem informē to dalībvalstu kompetentās iestādes, kurās tie ir darījuši AI sistēmu pieejamu vai nodevuši to ekspluatācijā, un – attiecīgā gadījumā – pieteikto struktūru;
- (i) saskaņā ar 49. pantu uzliek zīmi "CE" savām augsta riska AI sistēmām, lai norādītu uz atbilstību šai regulai;
- (j) pēc valsts kompetentās iestādes pieprasījuma pierāda augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām.

17. pants

Kvalitātes vadības sistēma

1. Augsta riska AI sistēmu sagādātāji izveido kvalitātes vadības sistēmu, kas nodrošina atbilstību šai regulai. Šo sistēmu sistemātiski un pienācīgi dokumentē rakstisku nostādņu, procedūru un instrukciju veidā, un tajā iekļauj vismaz šādus aspektus:
 - (a) normatīvās atbilstības stratēģija, tostarp atbilstības novērtēšanas procedūru un augsta riska AI sistēmas modifikāciju pārvaldības procedūru ievērošana;
 - (b) metodes, procedūras un sistemātiskas darbības, kas jāizmanto augsta riska AI sistēmas projektēšanai, projekta kontrolei un projekta verificēšanai;
 - (c) metodes, procedūras un sistemātiskas darbības, kas jāizmanto augsta riska AI sistēmas izstrādei, kvalitātes kontrolei un kvalitātes nodrošināšanai;
 - (d) pārbaudes, testēšanas un validēšanas procedūras, kas jāveic pirms augsta riska AI sistēmas izstrādes, tās laikā un pēc tās, un to biežums;
 - (e) tehniskās specifikācijas, ieskaitot standartus, kas jāpiemēro, un, ja attiecīgie saskaņotie standarti netiek piemēroti pilnībā, līdzekļi, kas jāizmanto, lai

nodrošinātu, ka augsta riska AI sistēma atbilst šīs sadaļas 2. nodaļā noteiktajām prasībām;

- (f) datu pārvaldības sistēmas un procedūras, arī datu vākšana, datu analīze, datu marķēšana, datu glabāšana, datu filtrēšana, datu izrace, datu apkopošana, datu saglabāšana un jebkura cita darbība ar datiem, kas tiek veikta pirms augsta riska AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā un to nolūkā;
 - (g) riska pārvaldības sistēma, kas minēta 9. pantā;
 - (h) pēctirgus uzraudzības sistēmas izveidošana, ieviešana un uzturēšana saskaņā ar 61. pantu;
 - (i) procedūras, kas saistītas ar ziņošanu par nopietniem incidentiem un darbības traucējumiem saskaņā ar 62. pantu;
 - (j) komunikācijas organizēšana ar valstu kompetentajām iestādēm, kompetentajām iestādēm, ieskaitot nozaru iestādes, dodot vai atbalstot piekļuvi datiem, pieteiktajām struktūrām, citiem operatoriem, klientiem vai citām ieinteresētajām personām;
 - (k) sistēmas un procedūras visas attiecīgās dokumentācijas un informācijas uzskaitē;
 - (l) resursu pārvaldība, ieskaitot ar piegādes drošību saistītus pasākumus;
 - (m) pārskatatbildības sistēma, kurā noteikti vadības un cita personāla pienākumi, kas attiecas uz visiem šajā punktā uzskaitītajiem aspektiem.
2. Šā panta 1. punktā minēto aspektu īstenošana ir proporcionāla sagādātāja organizācijas lielumam.
3. Attiecībā uz sagādātājiem, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, tiek uzskatīts, ka to pienākums ieviest kvalitātes vadības sistēmu ir izpildīts, ja ir izpildīti noteikumi par iekšējās pārvaldes kārtību, procesiem un mehānismiem saskaņā ar minētās direktīvas 74. pantu. Šajā sakarā ņem vērā visus šīs regulas 40. pantā minētos saskaņotos standartus.

18. pants

Pienākums sastādīt tehnisko dokumentāciju

1. Augsta riska AI sistēmu sagādātāji saskaņā ar IV pielikumu sastāda 11. pantā minēto tehnisko dokumentāciju.
2. Sagādātāji, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, tehnisko dokumentāciju uztur kā daļu no iekšējās pārvaldes, procedūru, procesu un mehānismu dokumentācijas saskaņā ar minētās direktīvas 74. pantu.

19. pants

Atbilstības novērtēšana

1. Augsta riska AI sistēmu sagādātāji gādā, lai pirms laišanas tirgū vai nodošanas ekspluatācijā to sistēmām tiktu veikta atbilstības novērtēšanas procedūra saskaņā ar 43. pantu. Ja pēc atbilstības novērtēšanas ir pierādīta AI sistēmu atbilstība šīs sadaļas 2. nodaļā noteiktajām prasībām, sagādātāji sagatavo ES atbilstības deklarāciju saskaņā ar 48. pantu un uzliek atbilstības zīmi "CE" saskaņā ar 49. pantu.

2. III pielikuma 5. punkta b) apakšpunktā minētajām augsta riska AI sistēmām, kuras laiž tirgū vai nodod ekspluatācijā sagādātāji, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, atbilstības novērtēšanu veic kā minētās direktīvas 97.–101. pantā minētās procedūras daļu.

20. pants

Automātiski ģenerētas žurnāldatnes

1. Augsta riska AI sistēmu sagādātāji glabā žurnāldatnes, ko automātiski ģenerē to augsta riska AI sistēmas, ciktāl šādas žurnāldatnes ir viņu pārziņā saskaņā ar līgumu, kas noslēgts ar lietotāju, vai citādi – saskaņā ar tiesību aktiem. Žurnāldatnes glabā tādu laiku, cik pienākas, ņemot vērā augsta riska AI sistēmas paredzēto nolūku un piemērojamās juridiskās saistības, kas noteiktas saskaņā ar Savienības vai valsts tiesību aktiem.
2. Sagādātāji, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, žurnāldatnes, ko automātiski ģenerē to augsta riska AI sistēmas, uztur kā daļu no dokumentācijas saskaņā ar minētās direktīvas 74. pantu.

21. pants

Korektīvie pasākumi

Augsta riska AI sistēmu sagādātāji, kas uzskata vai kam ir iemesls uzskatīt, ka augsta riska AI sistēma, kuru tie ir laiduši tirgū vai nodevuši ekspluatācijā, neatbilst šai regulai, nekavējoties veic nepieciešamos korektīvos pasākumus, kas vajadzīgi, lai panāktu sistēmas atbilstību vai, ja vajadzīgs, to izņemtu vai atsauktu no tirgus. Par to viņi informē attiecīgās augsta riska AI sistēmas izplatītājus un attiecīgā gadījumā pilnvaroto pārstāvi un importētājus.

22. pants

Pienākums informēt

Ja augsta riska AI sistēma rada risku 65. panta 1. punkta nozīmē un šis risks ir zināms sistēmas sagādātājam, šis sagādātājs nekavējoties informē to dalībvalstu kompetentās iestādes, kurās tas sistēmu darījis pieejamu, un, ja vajadzīgs, pieteikto struktūru, kas izdevusi sertifikātu augsta riska AI sistēmai, it īpaši par neatbilstību un visiem veiktajiem korektīvajiem pasākumiem.

23. pants

Sadarbība ar kompetentajām iestādēm

Augsta riska AI sistēmu sagādātāji pēc valsts kompetentās iestādes pieprasījuma sniedz šai iestādei visu informāciju un dokumentāciju, kas vajadzīga, lai pierādītu augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām, noformējot to vienā no oficiālajām Savienības valodām, ko noteikusi attiecīgā dalībvalsts. Pēc pamatota valsts kompetentās iestādes pieprasījuma sagādātāji šai iestādei nodrošina arī piekļuvi žurnāldatnēm, kuras automātiski ģenerē augsta riska AI sistēma, ciktāl šādas žurnāldatnes ir viņu pārziņā saskaņā ar līgumu, kas noslēgts ar lietotāju, vai citādi – saskaņā ar tiesību aktiem.

24. pants
Produktu ražotāju pienākumi

Ja augsta riska AI sistēma, kas saistīta ar produktiem, uz kuriem attiecas II pielikuma A iedaļā uzskaitītie tiesību akti, tiek laista tirgū vai nodota ekspluatācijā kopā ar produktu, kas saražots saskaņā ar minētajiem tiesību aktiem un ar produkta ražotāja vārdu, produkta ražotājs uzņemas atbildību par AI sistēmas atbilstību šai regulai un, ciktāl tiek skarta AI sistēma, tam ir tādi paši pienākumi, kādus šī regula uzliek sagādātājam.

25. pants
Pilnvarotie pārstāvji

1. Ja nav iespējams identificēt importētāju, sagādātāji, kas iedibināti ārpus Savienības, pirms savu sistēmu dara pieejamu Savienības tirgū, ar rakstisku pilnvaru iecel pilnvarotu pārstāvi, kurš iedibināts Savienībā.
2. Pilnvarotais pārstāvis veic uzdevumus, kas noteikti no sagādātāja saņemtajā pilnvarojumā. Šis pilnvarojums pilnvarotajam pārstāvim dod tiesības veikt šādus uzdevumus:
 - (a) glabāt ES atbilstības deklarācijas un tehniskās dokumentācijas kopiju, lai tā būtu pieejama valsts kompetentajām iestādēm un 63. panta 7. punktā minētajām valsts iestādēm;
 - (b) pēc pamatota pieprasījuma sniegt valsts kompetentajai iestādei visu informāciju un dokumentāciju, kas vajadzīga, lai pierādītu augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām, tostarp piekļuvi augsta riska AI sistēmas automātiski ģenerētajām žurnāldatnēm, ciktāl šādas žurnāldatnes ir sagādātāja pārziņā saskaņā ar līgumu, kas noslēgts ar lietotāju, vai citādi – saskaņā ar tiesību aktiem;
 - (c) pēc pamatota pieprasījuma sadarboties ar kompetentajām valsts iestādēm visās darbībās, ko tās veic saistībā ar augsta riska AI sistēmu.

26. pants
Importētāju pienākumi

1. Pirms augsta riska AI sistēmas laišanas tirgū šādas sistēmas importētāji pārliecinās, ka:
 - (a) šīs AI sistēmas sagādātājs ir veicis pienācīgu atbilstības novērtēšanas procedūru;
 - (b) sagādātājs ir sagatavojis tehnisko dokumentāciju saskaņā ar IV pielikumu;
 - (c) sistēmai ir noteiktais atbilstības marķējums, un tai ir pievienota nepieciešamā dokumentācija un lietošanas instrukcija.
2. Ja importētājs uzskata vai tam ir pamats uzskatīt, ka augsta riska AI sistēma neatbilst šai regulai, tas šo sistēmu nelaiž tirgū, kamēr nav panākts, ka šī AI sistēma ir atbilstoša. Ja augsta riska AI sistēma rada risku 65. panta 1. punkta nozīmē, importētājs par to informē AI sistēmas sagādātāju un tirgus uzraudzības iestādes.
3. Uz augsta riska AI sistēmas iepakojuma vai, ja tas nav iespējams, vajadzības gadījumā tai pievienotajā dokumentācijā importētāji norāda savu vārdu/nosaukumu, reģistrēto tirdzniecības nosaukumu vai reģistrēto preču zīmi un kontaktadresi.

4. Importētāji vajadzības gadījumā nodrošina, ka laikā, kad tie atbild par augsta riska AI sistēmu, tās glabāšanas vai pārvadāšanas apstākļi negatīvi neietekmē tās atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām.
5. Importētāji pēc pamatota pieprasījuma visu nepieciešamo informāciju un dokumentāciju, kas vajadzīga, lai pierādītu augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām valsts kompetentajām iestādēm sniedz valodā, kas ir viegli saprotama valsts kompetentajai iestādei, kā arī nodrošina piekļuvi augsta riska AI sistēmas automātiski ģenerētajām žurnāldatnēm, ciktāl šādas žurnāldatnes ir sagādātāja pārziņā saskaņā ar līgumu, kas noslēgts ar lietotāju, vai citādi – saskaņā ar tiesību aktiem. Tie arī sadarbojas ar šīm iestādēm visās darbībās, ko valsts kompetentā iestāde veic saistībā ar šo sistēmu.

27. pants

Izplatītāju pienākumi

1. Pirms augsta riska AI sistēmu dara pieejamu tirgū, izplatītāji pārbauda, vai augsta riska AI sistēmai ir paredzētā CE atbilstības zīme, vai tai ir pievienota nepieciešamā dokumentācija un lietošanas instrukcija un vai sagādātājs un importētājs attiecīgā gadījumā ir izpildījuši šajā regulā noteiktos pienākumus.
2. Ja izplatītājs uzskata vai tam ir iemesls uzskatīt, ka augsta riska AI sistēma neatbilst šīs sadaļas 2. nodaļā norādītajām prasībām, tas augsta riska AI sistēmu nedara pieejamu tirgū, kamēr nav panākta šīs sistēmas atbilstība minētajām prasībām. Turklāt, ja sistēma rada risku 65. panta 1. punkta nozīmē, izplatītājs par to attiecīgi informē sistēmas sagādātāju vai importētāju.
3. Izplatītāji vajadzības gadījumā nodrošina, ka laikā, kad tie atbild par augsta riska AI sistēmu, tās glabāšanas vai pārvadāšanas apstākļi negatīvi neietekmē tās atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām.
4. Izplatītājs, kas uzskata vai kam ir pamats uzskatīt, ka augsta riska AI sistēma, kuru tas darījis pieejamu tirgū, neatbilst šīs sadaļas 2. nodaļā noteiktajām prasībām, veic korektīvus sākusmus, kas vajadzīgi, lai panāktu šīs sistēmas atbilstību šīm prasībām, izņem vai atsauc to no tirgus vai nodrošina, ka šos korektīvos pasākumus veic sagādātājs, importētājs vai attiecīgā gadījumā attiecīgais operators. Ja augsta riska AI sistēma rada risku 65. panta 1. punkta nozīmē, izplatītājs nekavējoties par to informē to dalībvalstu kompetentās iestādes, kurās tas produktu darījis pieejamu tirgū, norādot sīku informāciju, it īpaši par neatbilstību un veiktajiem korektīvajiem pasākumiem.
5. Pēc pamatota valsts kompetentās iestādes pieprasījuma augsta riska AI sistēmu izplatītāji šai iestādei sniedz visu informāciju un dokumentāciju, kas vajadzīga, lai pierādītu augsta riska sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām. Izplatītāji arī sadarbojas ar šo valsts kompetento iestādi visās šīs iestādes veiktajās darbībās.

28. pants

Izplatītāju, importētāju, lietotāju vai citu trešo personu pienākumi

1. Katru izplatītāju, importētāju, lietotāju vai citu trešo personu šajā regulā uzskata par sagādātāju, un uz to attiecas sagādātāja pienākumi saskaņā ar 16. pantu, kādos no šiem apstākļiem:

- (a) tie laiž tirgū vai nodod ekspluatācijā augsta riska AI sistēmu ar savu vārdu vai preču zīmi;
 - (b) tie pārveido augsta riska AI sistēmai, kura jau laista tirgū vai nodota ekspluatācijā, paredzēto nolūku;
 - (c) tie izdara būtisku augsta riska AI sistēmas modifikāciju.
2. Ja ir 1. punkta b) vai c) apakšpunktā minētie apstākļi, sagādātājs, kas sākotnēji laidis tirgū vai nodevis ekspluatācijā augsta riska AI sistēmu, vairs netiek uzskatīts par sagādātāju šīs regulas nozīmē.

29. pants

Augsta riska AI sistēmu lietotāju pienākumi

1. Augsta riska AI sistēmu lietotāji šādas sistēmas izmanto saskaņā ar sistēmām pievienotajām lietošanas instrukcijām, izpildot 2. un 5. punktu.
2. Šā panta 1. punktā minētie pienākumi neskar citus lietotāju pienākumus, kas noteikti Savienības vai valsts tiesību aktos, un lietotāja rīcības brīvību organizēt savus resursus un darbības, lai īstenotu sagādātāja norādītos cilvēka virsvadības pasākumus.
3. Neskarot 1. punktu, ciktāl lietotājs īsteno kontroli pār ievaddatiem, lietotājs nodrošina, lai ievaddati būtu atbilstoši, ņemot vērā augsta riska AI sistēmai paredzēto nolūku.
4. Lietotāji uzrauga augsta riska AI sistēmas darbību, pamatojoties uz lietošanas instrukciju. Ja viņiem ir iemesls uzskatīt, ka sistēmas lietošana saskaņā ar lietošanas instrukciju var izraisīt AI sistēmas radītu risku 65. panta 1. punkta nozīmē, viņi informē sagādātāju vai izplatītāju un aptur sistēmas izmantošanu. Viņi arī informē sagādātāju vai izplatītāju, ja ir konstatējuši nopietnus incidentus vai darbības traucējumus 62. panta nozīmē, un šādā gadījumā pārtrauc AI sistēmas izmantošanu. Ja lietotājs nevar sazināties ar sagādātāju, pēc analogijas piemēro 62. pantu.
5. Attiecībā uz lietotājiem, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, pirmajā daļā noteikto uzraudzības pienākumu uzskata par izpildītu, ja ir izpildīti noteikumi par iekšējās pārvaldes kārtību, procesiem un mehānismiem saskaņā ar minētās direktīvas 74. pantu.
6. Augsta riska AI sistēmu lietotāji glabā žurnāldatnes, ko automātiski ģenerē šī augsta riska AI sistēma, ciktāl žurnāldatnes ir viņu pārziņā. Žurnāldatnes glabā pienācīgu laiku, ņemot vērā augsta riska AI sistēmai paredzēto nolūku un piemērojamās juridiskās saistības, kas noteiktas saskaņā ar Savienības vai valsts tiesību aktiem.

Lietotāji, kas ir kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, žurnāldatnes uztur kā daļu no iekšējās pārvaldes, procedūru, procesu un mehānismu dokumentācijas saskaņā ar minētās direktīvas 74. pantu.
7. Augsta riska AI sistēmu lietotāji vajadzības gadījumā izmanto saskaņā ar 13. pantu sniegto informāciju, lai izpildītu pienākumu veikt datu aizsardzības ietekmes novērtēšanu saskaņā ar Regulas (ES) 2016/679 35. pantu vai Direktīvas (ES) 2016/680 27. pantu.

4. NODAĻA

PIETEICĒJESTĀDES UN PIETEIKTĀS STRUKTŪRAS

30. pants

Pieteicējiestādes

1. Katra dalībvalsts norīko vai izveido pieteicējiestādi, kas atbild par vajadzīgo procedūru izveidi un izpildi atbilstības novērtēšanas struktūru novērtēšanai, norīkošanai un pieteikšanai, kā arī to uzraudzībai.
2. Par pieteicējiestādi dalībvalstis var izraudzīt Regulā (EK) Nr. 765/2008 minēto valsts akreditācijas struktūru.
3. Pieteicējiestādes tiek izveidotas, organizētas un darbojas tā, lai nerastos interešu konflikts ar atbilstības novērtēšanas struktūrām un tiktu aizsargāta to darba objektivitāte un neitralitāte.
4. Pieteicējiestādes tiek organizētas tā, lai lēmumus par atbilstības novērtēšanas struktūru pieteikšanu pieņemtu kompetentās personas, kas nav tās pašas, kuras veikušas minēto struktūru novērtēšanu.
5. Pieteicējiestādes nepiedāvā un neveic darbības, ko veic atbilstības novērtēšanas struktūras, un nekādus komerciālus un konkurējošus konsultāciju pakalpojumus.
6. Pieteicējiestādes nodrošina iegūtās informācijas konfidencialitāti.
7. Savu uzdevumu pienācīgai izpildei pieteicējiestādes pietiekamā skaitā nodarbina kompetentus darbiniekus.
8. Pieteicējiestādes gādā, ka atbilstības novērtēšana tiek veikta samērīgi, neradot nevajadzīgu slogu sagādātājiem, un ka pieteiktās struktūras veic savas darbības, pienācīgi ņemot vērā uzņēmuma lielumu, nozari, kurā tas darbojas, tā struktūru un attiecīgās AI sistēmas sarežģītības pakāpi.

31. pants

Atbilstības novērtēšanas struktūras pieteikšanas iesniegums

1. Atbilstības novērtēšanas struktūras iesniedz pieteikšanas iesniegumu pieteicējiestādei tajā dalībvalstī, kurā tās nodibinātas.
2. Pieteikšanas iesniegumam pievieno aprakstu par atbilstības novērtēšanas darbībām, atbilstības novērtēšanas moduli vai moduļiem un mākslīgā intelekta tehnoloģijām, par kurām atbilstības novērtēšanas struktūra apliecina savu kompetenci, kā arī valsts akreditācijas struktūras izsniegtu akreditācijas sertifikātu, ja tāds ir, kas apliecina, ka atbilstības novērtēšanas struktūra atbilst 33. pantā noteiktajām prasībām. Pievieno derīgus dokumentus, kas saistīti ar iesniedzējas pieteiktās struktūras pastāvošajiem norīkojumiem saskaņā ar citiem Savienības saskaņošanas tiesību aktiem.
3. Ja attiecīgā atbilstības novērtēšanas struktūra nevar iesniegt akreditācijas sertifikātu, tā iesniedz pieteicējiestādei dokumentus, kas vajadzīgi, lai pārbaudītu, atzītu un regulāri uzraudzītu tās atbilstību 33. pantā noteiktajām prasībām. Attiecībā uz pieteiktām struktūrām, kuras ir norīkotas saskaņā ar citiem Savienības saskaņošanas tiesību aktiem, visus dokumentus un sertifikātus, kas saistīti ar šiem norīkojumiem, var izmantot, lai vajadzības gadījumā atbalstītu to norīkošanas procedūru, kura paredzēta šajā regulā.

32. pants *Pieteikšanas kārtība*

1. Pieteicējstādes var pieteikt tikai tādas atbilstības novērtēšanas struktūras, kas atbilst 33. pantā norādītajām prasībām.
2. Paziņošanai Komisijai un pārējām dalībvalstīm pieteicējstādes izmanto Komisijas izstrādāto un pārvaldīto elektronisko paziņošanas sistēmu.
3. Pieteikumā iekļauj sīkas ziņas par atbilstības novērtēšanas darbībām, atbilstības novērtēšanas moduli vai moduļiem un attiecīgajām mākslīgā intelekta tehnoloģijām.
4. Attiecīgā atbilstības novērtēšanas struktūra var veikt pieteiktas struktūras darbības tikai tad, ja Komisija un pārējās dalībvalstis viena mēneša laikā no pieteikšanas nav cēlušas iebildumus.
5. Pēcākas pieteikuma izmaiņas pieteicējstāde dara zināmas Komisijai un pārējām dalībvalstīm.

33. pants *Pieteiktās struktūras*

1. Pieteiktās struktūras pārbauda augsta riska AI sistēmas atbilstību saskaņā ar 43. pantā minētajām atbilstības novērtēšanas procedūrām.
2. Pieteiktās struktūras atbilst organizatoriskajām, kvalitātes vadības, resursu un procesa prasībām, kas nepieciešamas to uzdevumu veikšanai.
3. Pieteikto struktūru uzbūvei, pienākumu sadalījumam, pārskatu sniegšanas kārtībai un darbībai jābūt tādai, kas nodrošina uzticēšanos pieteikto struktūru veikto atbilstības novērtēšanas darbību veikšanai un rezultātiem.
4. Pieteiktās struktūras ir neatkarīgas no augsta riska AI sistēmas sagādātāja, kuram tās veic atbilstības novērtēšanas darbības. Pieteiktās struktūras ir neatkarīgas arī no citiem operatoriem, kuriem ir materiāla interese par novērtējamo augsta riska AI sistēmu, kā arī no visiem sagādātāja konkurentiem.
5. Pieteiktās struktūras ir organizētas un darbojas tā, lai nodrošinātu savu darbību neatkarību, objektivitāti un neitralitāti. Pieteiktās struktūras dokumentē un ievieš struktūru un procedūras, kas vajadzīgas, lai aizsargātu objektivitāti un veicinātu un piemērotu objektivitātes principus attiecībā uz visu to organizāciju, personālu un novērtēšanas darbībām.
6. Pieteiktās struktūras ievieš dokumentētas procedūras, lai nodrošinātu, ka to personāls, komitejas, meitasuzņēmumi, apakšuzņēmēji un jebkura saistītā struktūra vai ārējo struktūru darbinieki ievēro informācijas konfidencialitāti, kas ir to pārziņā, veicot atbilstības novērtēšanas darbības, izņemot gadījumus, kad izpaušana paredzēta tiesību aktos. Pieteikto struktūru personālam ir pienākums ievērot dienesta noslēpumu attiecībā uz visu informāciju, kas iegūta, veicot uzdevumus saskaņā ar šo regulu, izņemot attiecībā uz tās dalībvalsts pieteicējstādēm, kurā tiek veiktas viņu darbības.
7. Pieteiktajām struktūrām ir procedūras tādu darbību veikšanai, kurās pienācīgi ņem vērā uzņēmuma lielumu, nozari, kurā tas darbojas, struktūru, attiecīgās AI sistēmas sarežģītības pakāpi.
8. Pieteiktajām struktūrām ir pienācīgi apdrošināta civiltiesiskā atbildība attiecībā uz savām atbilstības novērtēšanas darbībām, ja vien atbildību neuzņemas attiecīgā

dalībvalsts saskaņā ar šīs valsts tiesību aktiem vai ja dalībvalsts pati tieši neatbild par atbilstības novērtēšanu.

9. Pieteiktās struktūras spēj veikt visus uzdevumus, kas tām noteikti saskaņā ar šo regulu, ar visaugstāko profesionālo godaprātu un nepieciešamo kompetenci konkrētajā jomā, neatkarīgi no tā, vai šos uzdevumus veic pieteiktās struktūras pašas vai cita persona to uzdevumā un saskaņā ar savām pilnvarām.
10. Pieteiktajām struktūrām ir pietiekamas iekšējās spējas, lai tās varētu efektīvi izvērtēt uzdevumus, ko to uzdevumā veic ārējās personas. Šajā nolūkā vienmēr katrai atbilstības novērtēšanas procedūrai un katram augsta riska AI sistēmas tipam, attiecībā uz kuru norīkota pieteiktā struktūra, tās rīcībā jābūt pastāvīgi pieejamam pietiekamam administratīvajam, tehniskajam un zinātniskajam personālam, kam ir pieredze un zināšanas par attiecīgajām mākslīgā intelekta tehnoloģijām, datiem un datošanu, kā arī par šīs sadaļas 2. nodaļā noteiktajām prasībām.
11. Pieteiktās struktūras piedalās 38. pantā minētajās koordinācijas darbībās. Tās arī tiešā veidā piedalās vai ir pārstāvētas Eiropas standartizācijas organizācijās, vai nodrošina, ka ir informētas un pastāvīgi atjaunina zināšanas par attiecīgajiem standartiem.
12. Pieteiktās struktūras dara pieejamu un pēc pieprasījuma iesniedz visu attiecīgo dokumentāciju, ieskaitot sagādātāju dokumentāciju, pieteicējistādei, kas minēta 30. pantā, lai tā varētu veikt novērtēšanas, norīkošanas, pieteikšanas, uzraudzības un pārraudzības darbības un atvieglotu šajā nodaļā izklāstīto novērtēšanu.

34. pants

Pieteikto struktūru meitasuzņēmumi un apakšuzņēmuma līgumu slēgšana

1. Ja pieteiktā struktūra par noteiktu ar atbilstības novērtēšanu saistītu uzdevumu veikšanu slēdz apakšuzņēmuma līgumus vai to veikšanai izmanto meitasuzņēmumu, tā pārliecinās, ka apakšuzņēmējs vai meitasuzņēmums atbilst 33. panta prasībām, un attiecīgi informē pieteicējistādi.
2. Pieteiktās struktūras uzņemas pilnu atbildību par apakšuzņēmēju vai meitasuzņēmumu veiktajiem uzdevumiem neatkarīgi no tā, kur tie iedibināti.
3. Par darbībām var slēgt apakšuzņēmuma līgumu vai tās var veikt meitasuzņēmums tikai tad, ja sagādātājs tam piekrīt.
4. Pieteiktās struktūras glabā attiecīgos dokumentus par apakšuzņēmēja vai meitasuzņēmuma kvalifikācijas novērtēšanu un darbu, ko tie veikuši atbilstīgi šai regulai, lai tie būtu pieejami pieteicējistādēm.

35. pants

Saskaņā ar šo regulu norīkoto pieteikto struktūru identifikācijas numuri un saraksti

1. Komisija pieteiktajām struktūrām piešķir identifikācijas numuru. Tā piešķir atsevišķu numuru arī tad, ja struktūra ir pieteikta saskaņā ar vairākiem Savienības tiesību aktiem.
2. Komisija dara publiski pieejamu to struktūru sarakstu, kas pieteiktas saskaņā ar šo regulu, ieskaitot tām piešķirtos identifikācijas numurus un darbības, kurām tās ir pieteiktas. Komisija nodrošina saraksta atjaunināšanu.

*36. pants
Izmaiņas pieteikumos*

1. Ja pieteicējīestādei rodas aizdomas vai tā ir informēta, ka pieteiktā struktūra vairs neatbilst 33. pantā noteiktajām prasībām vai nepilda pienākumus, šī iestāde nekavējoties ar vislielāko rūpību izskata šo jautājumu. Šajā sakarā tā informē attiecīgo pieteikto struktūru par attiecīgajiem iebildumiem un dod tai iespēju darīt zināmu savu viedokli. Ja pieteicējīestāde secina, ka pieteiktā struktūra vairs neatbilst 33. pantā noteiktajām prasībām vai nespēj pildīt savus pienākumus, pieteicējīestāde attiecīgi ierobežo, aptur vai atsauc pieteikumu, ņemot vērā to, kādā mērā attiecīgā struktūra neatbilst prasībām vai nespēj pildīt savus pienākumus. Tā arī nekavējoties attiecīgi informē Komisiju un pārējās dalībvalstis.
2. Ja pieteikums tiek ierobežots, apturēts vai atsaukts vai pieteiktā struktūra ir beigusi darboties, pieteicējīestāde veic attiecīgos pasākumus, kas nodrošina, ka minētās pieteiktās struktūras dokumentus pārņem cita pieteiktā struktūra vai tie tiek glabāti, lai pēc pieprasījuma būtu pieejami atbildīgajām pieteicējīestādēm.

*37. pants
Pieteikto struktūru kompetences apstrīdēšana*

1. Vajadzības gadījumā Komisija izmeklē visus gadījumus, kur ir pamats šaubīties, vai pieteiktā struktūra atbilst 33. pantā noteiktajām prasībām.
2. Pieteicējīestāde pēc pieprasījuma sniedz Komisijai visu attiecīgo informāciju, kas saistīta ar attiecīgās pieteiktās struktūras pieteikšanu.
3. Komisija nodrošina, ka visa izmeklēšanas gaitā saskaņā ar šo pantu saņemtā konfidenciālā informācija tiek apstrādāta konfidenciāli.
4. Ja Komisija noskaidro, ka pieteiktā struktūra neatbilst vai vairs neatbilst 33. pantā noteiktajām prasībām, tā pieņem pamatotu lēmumu, kurā lūdz pieteikušo dalībvalsti veikt nepieciešamos korektīvos pasākumus, ieskaitot pieteikuma atsaukšanu, ja tā nepieciešama. Minēto īstenošanas aktu pieņem saskaņā ar 74. panta 2. punktā minēto pārbaudes procedūru.

*38. pants
Pieteikto struktūru koordinācija*

1. Komisija nodrošina, ka jomās, uz kurām attiecas šī regula, tiek izveidota atbilstoša koordinācija un sadarbība starp pieteiktajām struktūrām, kas saskaņā ar šo regulu darbojas AI sistēmu atbilstības novērtēšanas procedūrās un ir izveidotas un pienācīgi darbojas pieteikto struktūru nozares grupā.
2. Dalībvalstis nodrošina, ka to pieteiktās struktūras tieši vai ar ieceltu pārstāvju palīdzību piedalās nozares pieteikto struktūru grupas darbā.

*39. pants
Trešo valstu atbilstības novērtēšanas struktūras*

Atbilstības novērtēšanas struktūras, kas izveidotas saskaņā ar tādas trešās valsts tiesību aktiem, ar kuru Savienība ir noslēgusi nolīgumu, var tikt pilnvarotas veikt pieteikto struktūru darbības saskaņā ar šo regulu.

5. NODAĻA

STANDARTI, ATBILSTĪBAS NOVĒRTĒŠANA, SERTIFIKĀTI, REĢISTRĀCIJA

40. pants

Saskaņotie standarti

Augsta riska AI sistēmas, kas atbilst saskaņotiem standartiem vai to daļām, kuru atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, tiek uzskatītas par atbilstošām šīs sadaļas 2. nodaļā izklāstītajām prasībām, ciktāl minētie standarti aptver minētās prasības.

41. pants

Kopīgās specifikācijas

1. Ja nav saskaņotu standartu, kas minēti 40. pantā, vai ja Komisija uzskata, ka attiecīgie saskaņotie standarti nav pietiekami vai ir jāklīdzina specifiska nedrošība par drošību vai pamattiesībām, Komisija, izmantojot īstenošanas aktus, var pieņemt kopīgas specifikācijas par šīs sadaļas 2. nodaļā noteiktajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.
2. Sagatavojot 1. punktā minētās kopīgās specifikācijas, Komisija apkopo attiecīgo struktūru vai ekspertu grupu viedokļus, kas izveidotas saskaņā ar attiecīgajiem Savienības nozaru tiesību aktiem.
3. Tiek uzskatīts, ka augsta riska AI sistēmas, kas atbilst 1. punktā minētajām kopīgajām specifikācijām, atbilst šīs sadaļas 2. nodaļā noteiktajām prasībām, ciktāl uz šīm prasībām attiecas šīs kopīgās specifikācijas.
4. Ja sagādātāji neatbilst 1. punktā minētajām kopīgajām specifikācijām, tiem ir pienācīgi jāpamato, ka viņi ir pieņēmuši vismaz tām līdzvērtīgus tehniskos risinājumus.

42. pants

Prezumpcija par atbilstību noteiktām prasībām

1. Ņemot vērā paredzēto nolūku, tiek uzskatīts, ka augsta riska AI sistēmas, kas ir apmācītas un pārbaudītas ar datiem par konkrēto ģeogrāfisko, uzvedības un funkcionālo vidi, kurā tās paredzēts lietot, atbilst prasībām, kas noteiktas 10. panta 4. punktā.
2. Tiek uzskatīts, ka augsta riska AI sistēmas, kuras ir sertificētas vai kurām saskaņā ar kiberdrošības shēmu ir izsniegta atbilstības deklarācija saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881⁶³ un kuru atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, atbilst šīs regulas 15. pantā noteiktajām kiberdrošības prasībām, ciktāl uz šīm prasībām attiecas kiberdrošības sertifikāts vai atbilstības paziņojums vai tā daļas.

⁶³

Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts), OV L 151, 7.6.2019., 1. lpp.

43. pants
Atbilstības novērtēšana

1. Attiecībā uz augsta riska AI sistēmām, kas uzskaitītas III pielikuma 1. punktā, ja sagādātājs, pierādot augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām, ir piemērojis 40. pantā minētos saskaņotos standartus vai attiecīgā gadījumā 41. pantā minētās kopīgās specifikācijas, sagādātājs ievēro vienu no šīm procedūrām:
 - (a) VI pielikumā minētā atbilstības novērtēšanas procedūra uz iekšējās kontroles pamata;
 - (b) VII pielikumā minētā atbilstības novērtēšanas procedūra, kuras pamatā ir kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtēšana, iesaistot pieteikto struktūru.

Ja, pierādot augsta riska AI sistēmas atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām, sagādātājs nav piemērojis vai ir daļēji piemērojis 40. pantā minētos saskaņotos standartus, vai ja šādi saskaņotie standarti nepastāv un 41. pantā minētās kopīgās specifikācijas nav pieejamas, sagādātājs ievēro VII pielikumā noteikto atbilstības novērtēšanas procedūru.

VII pielikumā minētās atbilstības novērtēšanas procedūras vajadzībām sagādātājs var izvēlēties jebkuru no pieteiktajām struktūrām. Tomēr, ja sistēmu paredzēts nodot ekspluatācijā tiesībaizsardzības, imigrācijas vai patvēruma iestādēm, kā arī ES iestādēm, struktūrām vai aģentūrām, attiecīgi 63. panta 5. vai 6. punktā minētā tirgus uzraudzības iestāde, darbojas kā pieteiktā struktūra.

2. Attiecībā uz augsta riska AI sistēmām, kas minētas III pielikuma 2.–8. punktā, sagādātāji ievēro VI pielikumā minēto atbilstības novērtēšanas procedūru uz iekšējās kontroles pamata, kas neparedz pieteiktās struktūras iesaistīšanos. III pielikuma 5. punkta b) apakšpunktā minētajām augsta riska AI sistēmām, kuras tirgū laiž vai nodod ekspluatācijā kredītiestādes, uz kurām attiecas Direktīva 2013/36/ES, atbilstības novērtēšanu veic kā daļu no procedūras, kas minēta šīs direktīvas 97.–101. pantā.
3. Attiecībā uz augsta riska AI sistēmām, uz kurām attiecas II pielikuma A iedaļā uzskaitītie tiesību akti, sagādātājs veic attiecīgu atbilstības novērtēšanu, kā paredzēts minētajos tiesību aktos. Šīs sadaļas 2. nodaļā noteiktās prasības attiecas uz šīm augsta riska AI sistēmām, un tās ir daļa no šā novērtējuma. Piemēro arī VII pielikuma 4.3., 4.4., 4.5. punktu un 4.6. punkta piekto daļu.

Pieteiktajām struktūrām, kuras pieteiktas saskaņā ar minētajiem tiesību aktiem, minētajā novērtēšanā ir tiesības kontrolēt augsta riska AI sistēmu atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām, ar nosacījumu, ka pieteikto struktūru atbilstība prasībām, kas noteiktas 33. panta 4., 9. un 10. punktā, ir novērtēta saistībā ar pieteikšanas procedūru saskaņā ar minētajiem tiesību aktiem.

Ja tiesību akti, kas uzskaitīti II pielikuma A iedaļā, ļauj produkta ražotājam atteikties no trešās personas veiktas atbilstības novērtēšanas, ar nosacījumu, ka šis ražotājs ir piemērojis visus saskaņotos standartus, kas aptver visas attiecīgās prasības, šis ražotājs var izmantot šo iespēju tikai tad, ja ir piemērojis arī saskaņotos standartus vai attiecīgā gadījumā – 41. pantā minētās kopīgās specifikācijas, kas attiecas uz šīs sadaļas 2. nodaļā noteiktajām prasībām.

4. Augsta riska AI sistēmas pakļauj jaunai atbilstības novērtēšanas procedūrai ikreiz, kad tās tiek būtiski pārveidotas, neatkarīgi no tā, vai pārveidoto sistēmu paredzēts izplatīt tālāk jeb vai to turpinās lietot pašreizējais lietotājs.
Attiecībā uz augsta riska AI sistēmām, kuras pēc laišanas tirgū vai nodošanas ekspluatācijā turpina mācīties, tādas izmaiņas augsta riska AI sistēmā un tās veikspējā, ko iepriekš sākotnējās atbilstības novērtēšanas brīdī ir noteicis sagādātājs un kas ir norādītas informācijā, kura ietverta tehniskajā dokumentācijā, kas minēta IV pielikuma 2. punkta f) apakšpunktā, nav būtiskas modifikācijas.
5. Komisijai piešķir pilnvaras pieņemt deleģētos aktus saskaņā ar 73. pantu, lai atjauninātu VI un VII pielikumu ar mērķi ieviest atbilstības novērtēšanas procedūru elementus, kas ir nepieciešami, ņemot vērā tehnikas attīstību.
6. Komisijai piešķir pilnvaras pieņemt deleģētos aktus, lai grozītu 1. un 2. punktu nolūkā uz III pielikuma 2.–8. punktā minētajā augsta riska AI sistēmām attiecināt VII pielikumā vai tā daļās minēto atbilstības novērtēšanas procedūru. Komisija pieņem šādus deleģētos aktus, ņemot vērā tādas atbilstības novērtēšanas procedūras efektivitāti, kuras pamatā ir VI pielikumā minētā iekšējā kontrole, lai novērstu vai samazinātu šādu sistēmu radītos riskus attiecībā uz veselību un drošību, un pamattiesību aizsardzību, kā arī pienācīgu spēju un resursu pieejamība pieteikto struktūru starpā.

44. pants Sertifikāti

1. Sertifikātus, ko saskaņā ar VII pielikumu izdevušas pieteiktās struktūras, sagatavo kādā no Savienības oficiālajām valodām, ko nosaka dalībvalsts, kurā ir izveidota pieteiktā struktūra, vai oficiālajā Savienības valodā, kas pieteiktajai struktūrai ir citādā ziņā pieņemama.
2. Sertifikāti ir derīgi tajos norādītajā laikposmā, kas nepārsniedz piecus gadus. Pēc sagādātāja pieteikuma sertifikāta derīgumu var pagarināt uz turpmākiem laikposmiem, kas katrs nepārsniedz piecus gadus, pamatojoties uz atkārtotu novērtēšanu saskaņā ar piemērojamām atbilstības novērtēšanas procedūrām.
3. Ja pieteiktā struktūra konstatē, ka AI sistēma vairs neatbilst šīs sadaļas 2. nodaļā noteiktajām prasībām, tā, ņemot vērā proporcionalitātes principu, aptur vai atsauc izdoto sertifikātu vai uzliek tam jebkādu ierobežojumu, ja vien atbilstība šīm prasībām nav nodrošināta ar attiecīgiem korektīviem pasākumiem, ko sistēmas sagādātājs veic pieteiktās struktūras noteiktajā termiņā. Pieteiktā struktūra savu lēmumu pamato.

45. pants Pieteikto struktūru lēmumu pārsūdzēšana

Dalībvalstis nodrošina, ka pieteikto struktūru lēmumu pārsūdzēšanas procedūra ir pieejama personām, kam ir legītīma interese par šo lēmumu.

46. pants Pieteikto struktūru pienākums informēt

1. Pieteiktās struktūras informē pieteicējiestādi par:

- (a) katru Savienības tehniskās dokumentācijas novērtējuma sertifikātu, sertifikātu papildinājumiem, kvalitātes vadības sistēmas apstiprinājumiem, kas izsniegti saskaņā ar VII pielikuma prasībām;
 - (b) katru atteikumu, ierobežojumu, apturēšanu vai anulēšanu, kas attiecas uz Savienības tehniskās dokumentācijas novērtējuma sertifikātu vai kvalitātes vadības sistēmas apstiprinājumu, kas izdots saskaņā ar VII pielikuma prasībām;
 - (c) apstākļiem, kas ietekmē pieteikuma darbības jomu vai nosacījumus;
 - (d) no tirgus uzraudzības iestādēm saņemtiem pieprasījumiem pēc informācijas par atbilstības novērtēšanas darbībām;
 - (e) atbilstības novērtēšanas darbībām, ko tās veikušas darbības jomā, kurai tās pieteiktas, un visām citām darbībām, tostarp pārrobežu darbībām un apakšuzņēmuma līgumu slēgšanu (pēc pieprasījuma).
2. Katra pieteiktā struktūra informē pārējās pieteiktās struktūras par:
- (a) kvalitātes vadības sistēmas apstiprinājumiem, kurus tā ir atteikusi, apturējusi vai anulējusi, un pēc pieprasījuma arī par kvalitātes sistēmas apstiprinājumiem, kurus tā ir izdevusi;
 - (b) ES tehniskās dokumentācijas novērtējuma sertifikātiem vai to papildinājumiem, kurus tā ir noraidījusi, atsaukusi, apturējusi vai kā citādi ierobežojusi, un pēc pieprasījuma arī par tās izsniegtiem sertifikātiem un/vai to papildinājumiem.
3. Katra pieteiktā struktūra sniedz pārējām pieteiktajām struktūrām, kas veic līdzīgas atbilstības novērtēšanas darbības, kas attiecas uz tām pašām mākslīgā intelekta tehnoloģijām, attiecīgu informāciju par jautājumiem, kas saistīti ar negatīviem un pēc pieprasījuma – pozitīviem atbilstības novērtēšanas rezultātiem.

47. pants

Atkāpe no atbilstības novērtēšanas procedūras

1. Atkāpjoties no 43. panta, tirgus uzraudzības iestāde var atļaut noteiktu augsta riska AI sistēmu laišanu tirgū vai nodošanu ekspluatācijā attiecīgās dalībvalsts teritorijā ārkārtēju sabiedriskās drošības iemeslu dēļ vai cilvēku veselības un dzīvības aizsardzības, vides aizsardzības un svarīgu rūpniecības un infrastruktūras aktīvu aizsardzībai. Šī atļauja ir ierobežota laikposmā, kurā tiek veiktas nepieciešamās atbilstības novērtēšanas procedūras, un beidzas, tiklīdz šīs procedūras ir pabeigtas. Šīs procedūras pabeidz bez liekas kavēšanās.
2. 1. punktā minēto atļauju izsniedz tikai tad, ja tirgus uzraudzības iestāde secina, ka augsta riska AI sistēma atbilst šīs sadaļas 2. nodaļas prasībām. Par visām atļaujām, kas izsniegtas saskaņā ar 1. punktu, tirgus uzraudzības iestāde nekavējoties informē Komisiju un pārējās dalībvalstis.
3. Ja 15 kalendāro dienu laikā pēc 2. punktā minētās informācijas saņemšanas neviena dalībvalsts vai Komisija nav cēlusi iebildumus par atļauju, ko saskaņā ar 1. punktu izdevusi dalībvalstu tirgus uzraudzības iestāde, minēto atļauju uzskata par pamatotu.
4. Ja 15 kalendāro dienu laikā pēc 2. punktā minētā paziņojuma saņemšanas dalībvalsts ceļ iebildumus pret citu dalībvalstu tirgus uzraudzības iestāžu izdotajām atļaujām vai Komisija uzskata, ka atļauja ir pretrunā Savienības tiesību aktiem vai 2. punktā minētais dalībvalstu secinājums par attiecīgās sistēmas atbilstību nav pamatots,

Komisija nekavējoties sāk apspriešanos ar attiecīgo dalībvalsti; notiek apspriešanās ar attiecīgo(-ajiem) operatoru(-iem), un viņam(-iem) ir nodrošināta iespēja izklāstīt savu viedokli. To ņemot vērā, Komisija izlemj, vai atļauja ir pamatota vai nav. Komisija savu lēmumu adresē attiecīgajai dalībvalstij un attiecīgajam operatoram vai operatoriem.

5. Ja atļauju uzskata par nepamatotu, attiecīgās dalībvalsts tirgus uzraudzības iestāde to atsauc.
6. Atkāpjoties no 1.–5. punkta, augsta riska AI sistēmām, kuras paredzēts lietot kā ierīču drošības sastāvdaļas, vai kuras pašas ir ierīces, uz kurām attiecas Regula (ES) 2017/745 un Regula (ES) 2017/746, Regulas (ES) 2017/745 59. pantu un Regulas (ES) 2017/746 54. pantu piemēro arī saistībā ar atkāpi no atbilstības novērtēšanas attiecībā uz atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām.

48. pants

ES atbilstības deklarācija

1. Sagādātājs rakstiski sagatavo ES atbilstības deklarāciju katrai AI sistēmai un glabā to valsts kompetentajām iestādēm pieejamu 10 gadus pēc AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā. ES atbilstības deklarācijā norāda tās AI sistēmas identitāti, kurai deklarācija ir sagatavota. ES atbilstības deklarācijas kopiju pēc pieprasījuma nodod attiecīgajām valsts kompetentajām iestādēm.
2. ES atbilstības deklarācijā norāda, ka attiecīgā augsta riska AI sistēma atbilst šīs sadaļas 2. nodaļā noteiktajām prasībām. ES atbilstības deklarācijā iekļauj V pielikumā noteikto informāciju, un to tulko kādā no oficiālajām Savienības valodām vai valodās, ko pieprasa dalībvalsts(-is), kurā(-ās) ir pieejama attiecīgā augsta riska AI sistēma.
3. Ja uz augsta riska AI sistēmām attiecas citi Savienības saskaņošanas tiesību akti, kuriem arī vajadzīga ES atbilstības deklarācija, par visiem Savienības tiesību aktiem, kas piemērojami augsta riska AI sistēmai, sagatavo vienotu ES atbilstības deklarāciju. Deklarācijā iekļauj visu informāciju, kas vajadzīga, lai identificētu Savienības saskaņošanas tiesību aktus, uz kuriem attiecas šī deklarācija.
4. Sagatavojot ES atbilstības deklarāciju, sagādātājs uzņemas atbildību par ražojuma atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām. Vajadzības gadījumā sagādātājs ES atbilstības deklarāciju atjaunina.
5. Komisijai piešķir pilnvaras pieņemt deleģētos aktus saskaņā ar 73. pantu, lai atjauninātu V pielikumā noteiktās ES atbilstības deklarācijas saturu ar mērķi ieviest elementus, kas nepieciešami, ņemot vērā tehnikas attīstību.

49. pants

Atbilstības zīme “CE”

1. Zīmi “CE” augsta riska AI sistēmām uzliek tā, lai tā būtu redzama, salasāma un neizdzēšama. Ja augsta riska AI sistēmas specifikas dēļ tas nav iespējams vai netiek prasīts, zīmi liek uz iepakojuma vai attiecīgā gadījumā uz pievienotās dokumentācijas.
2. Uz zīmi “CE”, kas minēta šā panta 1. punktā, attiecas vispārīgie principi, kas izklāstīti Regulas (EK) Nr. 765/2008 30. pantā.

3. Zīmei “CE” seko pieteiktās struktūras identifikācijas numurs, ja tiek piemērota pielikuma 43. daļā norādītā atbilstības novērtēšanas procedūra. Identifikācijas numuru norāda arī visos reklāmas materiālos, kuros minēts, ka augsta riska AI sistēma atbilst zīmes “CE” prasībām.

50. pants

Dokumentu saglabāšana

Sagādātājs 10 gadus pēc augsta riska AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā glabā valsts kompetentajām iestādēm pieejamu šādu dokumentāciju:

- (a) 11. pantā minēto tehnisko dokumentāciju;
- (b) dokumentāciju par kvalitātes vadības sistēmu, kas minēta 17. pantā;
- (c) vajadzības gadījumā – dokumentāciju par izmaiņām, ko apstiprinājušas pieteiktās struktūras;
- (d) attiecīgā gadījumā – pieteikto struktūru izdotos lēmumus un citus dokumentus;
- (e) ES atbilstības deklarāciju, kas minēta 48. pantā.

51. pants

Reģistrēšana

Pirms 6. panta 2. punktā minētās augsta riska AI sistēmas laišanas tirgū vai nodošanas ekspluatācijā sagādātājs vai attiecīgā gadījumā pilnvarotais pārstāvis reģistrē šo sistēmu 60. pantā minētajā ES datubāzē.

IV SADAĻA

PIENĀKUMS NODROŠINĀT PĀRREDZAMĪBU NOTEIKTĀM AI SISTĒMĀM

52. pants

Pienākums nodrošināt pārredzamību noteiktām AI sistēmām

1. Sagādātāji nodrošina, ka AI sistēmas, kas paredzētas saskarsmei ar fiziskām personām, projektē un izstrādā tā, lai fiziskās personas tiktu informētas par to, ka tās ir saskarsmē ar AI sistēmu, ja vien tas nav pats par sevi saprotams attiecīgajos apstākļos un izmantošanas kontekstā. Šis pienākums neattiecas uz AI sistēmām, kuras ir likumiski atļautas noziedzīgu nodarījumu atklāšanai, novēršanai, izmeklēšanai un vainīgo saukšanai pie atbildības, ja šīs sistēmas nav pieejamas sabiedrībai ziņošanai par noziedzīgu nodarījumu.
2. Emociju uztveršanas sistēmas vai biometriskās kategorizācijas sistēmas lietotāji informē fiziskās personas par sistēmas darbību, kurai tās pakļautas. Šis pienākums neattiecas uz AI sistēmām, kuras izmanto biometriskai kategorizācijai un ar kurām ir likumiski atļauts atklāt, novērst un izmeklēt noziedzīgus nodarījumus.
3. Tādas AI sistēmas lietotāji, kura rada vai manipulē ar attēlu, audio vai video saturu, kas ievērojami atgādina reālas personas, objektus, vietas vai citas vienības vai notikumus un cilvēkam maldinoši šķistu autentisks vai patiess (“dziļviltojums”), atklāj, ka saturs ir mākslīgi radīts vai manipulēts.

Pirmo daļu tomēr nepiemēro, ja lietošana ir likumīgi atļauta noziedzīgu nodarījumu atklāšanai, novēršanai, izmeklēšanai un vainīgo saukšanai pie atbildības vai ja tas ir nepieciešams, lai izmantotu tiesības uz vārda brīvību un tiesības uz mākslas un zinātnes brīvību, kas garantētas ES Pamattiesību hartā, un ievērojot atbilstošus trešo personu tiesību un brīvību aizsardzības pasākumus.

4. Panta 1., 2. un 3. punkts neietekmē prasības un pienākumus, kas noteikti šīs regulas III sadaļā.

V SADAĻA

INOVĀCIJAS ATBALSTA PASĀKUMI

53. pants

AI “regulatīvās smilškastēs”

1. AI “regulatīvās smilškastēs”, ko izveidojusi viena vai vairākas dalībvalstu kompetentā(-ās) iestāde(-es) vai Eiropas Datu aizsardzības uzraudzītājs, nodrošina kontrolētu vidi, kas ierobežotu laiku atvieglo inovatīvu AI sistēmu izstrādi, testēšanu un validēšanu pirms laišanas tirgū vai nodošanas ekspluatācijā pēc īpaša plāna. Tas notiek tiešā kompetento iestāžu uzraudzībā un vadībā, lai nodrošinātu atbilstību šīs regulas prasībām un attiecīgā gadījumā citiem Savienības un dalībvalstu tiesību aktiem, kas tiek uzraudzīti “smilškastē”.
2. Dalībvalstis nodrošina, ka tādā mērā, kādā inovatīvās AI sistēmas ietver persondatu apstrādi vai citādi atrodas tādu citu valsts iestāžu vai kompetento iestāžu pārraudzībā, kas dod vai atbalsta piekļuvi datiem, valsts datu aizsardzības iestādes un šīs citas valsts iestādes ir saistītas ar AI “regulatīvās smilškastēs” darbību.
3. AI “regulatīvās smilškastēs” neietekmē kompetento iestāžu uzraudzības un korekcijas pilnvaras. Būtiski riski veselībai, drošībai un pamattiesībām, kas konstatēti šādu sistēmu izstrādes un testēšanas laikā, tiek nekavējoties mazināti un, ja tas nav iespējams, izstrādes un testēšanas procesu uz šādu risku mazināšanas laiku aptur.
4. AI “regulatīvās smilškastēs” dalībnieki saskaņā ar piemērojamajiem Savienības un dalībvalstu tiesību aktiem par atbildību atbild par kaitējumu, kas nodarīts trešām personām “smilškastē” notiekošo eksperimentu rezultātā.
5. Dalībvalstu kompetentās iestādes, kas ir izveidojušas AI “regulatīvās smilškastēs”, koordinē savas darbības un sadarbojas Eiropas Mākslīgā intelekta padomes satvarā. Tās iesniedz AI padomei un Komisijai ikgadējus ziņojumus par šo shēmu īstenošanas rezultātiem, ieskaitot paraugpraksi, gūto pieredzi un ieteikumus par to struktūru un – attiecīgā gadījumā – par šīs regulas un citu tādu Savienības tiesību aktu piemērošanu, ko tās uzrauga “smilškastē”.
6. AI “regulatīvās smilškastēs” darbības kārtību un nosacījumus, tostarp atbilstības kritērijus un procedūru, kas nosaka pieteikšanos tajā, atlasī, dalību un iziešanas no “smilškastēs”, kā arī dalībnieku tiesības un pienākumus nosaka īstenošanas aktos. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

54. pants

Persondatu turpmāka apstrāde noteiktu AI sistēmu izstrādei vispārības interesēs AI “regulatīvajā smilškastē”

1. Persondatus, kas likumīgi savākti citiem mērķiem, AI “regulatīvajā smilškastē” apstrādā, lai izstrādātu un testētu atsevišķas inovatīvas AI sistēmas, ar šādiem nosacījumiem:
 - (a) inovatīvās AI sistēmas izstrādā, lai aizsargātu būtiskas vispārības intereses vienā vai vairākās no šīm jomām:
 - i) noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai vainīgo saukšana pie atbildības, vai kriminālsodu izpilde, arī aizsardzība pret sabiedriskās drošības apdraudējumiem un to novēršana, ko veic kompetento iestāžu kontrolē un atbildībā. Apstrādes pamatā ir dalībvalstu vai Savienības tiesību akti;
 - ii) sabiedrības drošība un sabiedrības veselība, arī slimību profilakse, kontrole un ārstniecība;
 - iii) augsta līmeņa aizsardzība un vides kvalitātes uzlabošana;
 - (b) apstrādātie dati ir nepieciešami, lai izpildītu vienu vai vairākas III sadaļas 2. nodaļā minētās prasības, ja šīs prasības nevar efektīvi izpildīt, apstrādājot anonimizētus, sintētiskus vai citādus nepersondatus;
 - (c) ir efektīvi uzraudzības mehānismi, lai varētu noteikt, vai “smilškastēs” eksperimentēšanas laikā var rasties augsts risks datu subjektu pamattiesībām, kā arī reaģēšanas mehānisms, lai šos riskus ātri mazinātu un vajadzības gadījumā apturētu datu apstrādi;
 - (d) persondati, kas jāapstrādā “smilškastēs” vidē, atrodas funkcionāli nodalītā, izolētā un aizsargātā datu apstrādes vidē dalībnieku kontrolē, un piekļuve šiem datiem ir tikai pilnvarotām personām;
 - (e) apstrādātie persondati netiek pārsūtīti, nodoti vai citādi darīti pieejami citām personām;
 - (f) persondatu apstrāde “smilškastēs” vidē neraisa pasākumus vai lēmumus, kas ietekmē datu subjektus;
 - (g) persondati, kas apstrādāti “smilškastēs” vidē, tiek dzēsti, tiklīdz dalība “smilškastē” ir beigusies vai pienākušas persondatu glabāšanas perioda beigas;
 - (h) žurnāldatnes par persondatu apstrādi “smilškastēs” vidē tiek glabātas visu dalības “smilškastē” laiku un vienu gadu pēc tās izbeigšanas, tikai tam un vienīgi tik ilgi, kā nepieciešams pārskatatbildības un dokumentēšanas pienākumu izpildei saskaņā ar šo pantu vai citiem piemērojamiem Savienības vai dalībvalstu tiesību aktiem;
 - (i) pilnīgu un detalizētu procesa aprakstu un pamatojumu AI sistēmas apmācībai, testēšanai un validēšanai glabā kopā ar testēšanas rezultātiem kā daļu no tehniskās dokumentācijas, kas minēta IV pielikumā;
 - (j) īss kopsavilkums par “smilškastē” izstrādāto AI projektu, tā mērķi un gaidāmiem rezultātiem, kas publicēts kompetento iestāžu tīmekļa vietnē.
2. 1. punkts neskar Savienības un dalībvalstu tiesību aktus, kas neparedz apstrādi mērķiem, kuri nav skaidri minēti minētajos tiesību aktos.

55. pants
Pasākumi mazapjoma sagādātājiem un lietotājiem

1. Dalībvalstis veic šādas darbības:
 - (a) dod mazapjoma sagādātājiem un jaunuzņēmumiem prioritāru piekļuvi AI “regulatīvajām smilškastēm”, ciktāl tie atbilst atbilstības nosacījumiem;
 - (b) organizē īpašas izpratnes veicināšanas darbības par šīs regulas piemērošanu, kas pielāgotas mazapjoma sagādātāju un lietotāju vajadzībām;
 - (c) vajadzības gadījumā izveido īpašu kanālu saziņai ar mazapjoma sagādātājiem, lietotājiem un citiem novatoriem, lai sniegtu norādījumus un atbildētu uz jautājumiem par šīs regulas īstenošanu.
2. Nosakot maksas par atbilstības novērtēšanu saskaņā ar 43. pantu, ņem vērā mazapjoma sagādātāju īpašās intereses un vajadzības, samazinot šīs maksas proporcionāli to lielumam un tirgus lielumam.

VI SADAĻA

PĀRVALDE

1. NODAĻA

EIROPAS MĀKSLĪGĀ INTELEKTA PADOME

56. pants
Eiropas Mākslīgā intelekta padomes izveidošana

1. Tiek izveidota Eiropas mākslīgā intelekta padome (“AI padome”).
2. AI padome sniedz konsultācijas un palīdzību Komisijai, lai:
 - (a) sekmētu valstu uzraudzības iestāžu un Komisijas efektīvu sadarbību jautājumos, uz kuriem attiecas šī regula;
 - (b) koordinētu un sniegtu ieguldījumu Komisijas, valstu uzraudzības iestāžu un citu kompetento iestāžu sniegtajos norādījumos un veiktajā analīzē par jauniem aspektiem iekšējā tirgū attiecībā uz jautājumiem, uz kuriem attiecas šī regula;
 - (c) palīdzētu valstu uzraudzības iestādēm un Komisijai nodrošināt šīs regulas konsekventu piemērošanu.

57. pants
AI padomes struktūra

1. AI padomi veido valstu uzraudzības iestādes, kuras pārstāv attiecīgās iestādes vadītājs vai līdzvērtīga augsta līmeņa amatpersona, un Eiropas Datu aizsardzības uzraudzītājs. Citas valstu iestādes var izaicināt uz sanāksmēm, ja tajās apspriestie jautājumi tām ir svarīgi.
2. AI padome pēc Komisijas piekrišanas pieņem savu reglamentu ar tās locekļu balsu vienkāršu vairākumu. Reglaments ietver arī darbības aspektus, kas saistīti ar to AI padomes uzdevumu izpildi, kas uzskaitīti 58. pantā. AI padome vajadzības gadījumā var izveidot apakšgrupas īpašu jautājumu izskatīšanai.

3. AI padomi vada Komisija. Komisija sasauc sanāksmes un sagatavo darba kārtību saskaņā ar AI padomes uzdevumiem, kas noteikti šajā regulā un AI padomes reglamentā. Komisija sniedz administratīvu un analītisku atbalstu AI padomes darbībām saskaņā ar šo regulu.
4. AI padome var uzaicināt ārējos ekspertus un novērotājus piedalīties tās sanāsmēs un var rīkot viedokļu apmaiņu ar ieinteresētām trešām personām, lai pienācīgā mērā iegūtu tās darbam nepieciešamo informāciju. Šajā nolūkā Komisija var atbalstīt viedokļu apmaiņu starp AI padomi un citām Savienības struktūrām, birojiem, aģentūrām un konsultatīvajām grupām.

58. pants

AI padomes uzdevumi

Sniedzot konsultācijas un palīdzību Komisijai 56. panta 2. punkta kontekstā, AI padome galvenokārt:

- (a) apkopo un kopīgo zinātību un paraugpraksi dalībvalstu starpā;
- (b) veicina vienotu administratīvo praksi dalībvalstīs, tostarp attiecībā uz 53. pantā minēto “regulatīvo smilškastu” darbību;
- (c) sniedz atzinumus, ieteikumus vai rakstiskas piezīmes par jautājumiem, kas saistīti ar šīs regulas īstenošanu, it īpaši:
 - i) par tehniskajām specifikācijām vai esošajiem standartiem attiecībā uz III sadaļas 2. nodaļā noteiktajām prasībām;
 - ii) par 40. un 41. pantā minēto saskaņoto standartu vai kopīgo specifikāciju izmantošanu;
 - iii) par norādījumu dokumentu sagatavošanu, ietverot pamatnostādnes par 71. pantā minēto administratīvo naudas sodu noteikšanu.

2. NODAĻA

VALSTU KOMPETENTĀS IESTĀDES

59. pants

Valstu kompetento iestāžu norīkošana

1. Katra dalībvalsts izveido vai norīko valsts kompetentās iestādes, lai nodrošinātu šīs regulas piemērošanu un īstenošanu. Valsts kompetentās iestādes organizē tā, lai to darbību un uzdevumu veikšanā nodrošinātu objektivitāti un neitralitāti.
2. Katra dalībvalsts izraugās valsts uzraudzības iestādi no valsts kompetento iestāžu vidus. Valsts uzraudzības iestāde darbojas kā pieteicējierīcība un tirgus uzraudzības iestāde, ja attiecīgajai dalībvalstij nav organizatorisku un administratīvu iemeslu norīkot vairākas iestādes.
3. Dalībvalstis informē Komisiju par savu norīkoto iestādi vai iestādēm un attiecīgā gadījumā norāda iemeslus vairāku iestāžu norīkošanai.
4. Dalībvalstis nodrošina, ka valstu kompetentajām iestādēm tiek nodrošināti pietiekami finanšu resursi un cilvēkresursi, lai tās varētu pildīt uzdevumus, kas tām noteikti ar šo regulu. Galvenais, valsts kompetentajām iestādēm ir pietiekams skaits pastāvīgi pieejama personāla, kura kompetencē un pārziņā ir padziļināta izpratne par mākslīgā

intelekta tehnoloģijām, datiem un datošanu, pamattiesībām, riskiem attiecībā uz veselību un drošību un zināšanas par esošajiem standartiem un juridiskajām prasībām.

5. Dalībvalstis katru gadu ziņo Komisijai par valsts kompetento iestāžu finanšu resursu un cilvēkresursu situāciju, novērtējot to atbilstību. Komisija šo informāciju nosūta AI padomei apspriešanai un iespējamai ieteikumu sniegšanai.
6. Komisija veicina pieredzes apmaiņu starp valstu kompetentajām iestādēm.
7. Valstu kompetentās iestādes var dot norādījumus un padomus par šīs regulas īstenošanu, arī mazapjoma sagādātājiem. Kad valsts kompetentās iestādes plāno dot norādījumus un padomus par AI sistēmu jomās, uz kurām attiecas citi Savienības tiesību akti, vajadzības gadījumā tās apspriežas ar attiecīgajām valsts kompetentajām iestādēm, kas norīkotas saskaņā ar minētajiem Savienības tiesību aktiem. Dalībvalstis var arī izveidot vienu centrālo kontaktpunktu saziņai ar operatoriem.
8. Ja šīs regulas darbības jomā ietilpst Savienības iestādes, aģentūras un struktūras, kā kompetentā iestāde to uzraudzības nolūkā darbojas Eiropas Datu aizsardzības uzraudzītājs.

VII SADAĻA

ES DATUBĀZE PAR SAVRUPĀM AUGSTA RISKA AI SISTĒMĀM

60. pants

ES datubāze par savrupām augsta riska AI sistēmām

1. Komisija sadarbībā ar dalībvalstīm izveido un uztur ES datubāzi, kas ietver 2. punktā minēto informāciju par 6. panta 2. punktā minētajām augsta riska AI sistēmām, kuras reģistrētas saskaņā ar 51. pantu.
2. Sagādātāji ievada ES datubāzē VIII pielikumā uzskaitītos datus. Komisija viņiem nodrošina tehnisko un administratīvo atbalstu.
3. ES datubāzē esošā informācija ir publiski pieejama.
4. ES datubāze satur persondatus tikai tik daudz, cik nepieciešams informācijas vākšanai un apstrādei saskaņā ar šo regulu. Šajā informācijā iekļauj to fizisko personu vārdus un kontaktinformāciju, kuras atbild par sistēmas reģistrēšanu un kurām ir juridiskas pilnvaras pārstāvēt sagādātāju.
5. Komisija ir ES datubāzes pārzine. Tā arī sniedz sagādātājiem atbilstošu tehnisko un administratīvo atbalstu.

VIII SADAĻA

PĒCTIRGUS UZRAUDZĪBA, INFORMĀCIJAS KOPĪGOŠANA, TIRGUS UZRAUDZĪBA

1. NODAĻA

PĒCTIRGUS UZRAUDZĪBA

61. pants

Sagādātāju veikta pēctirgus uzraudzība un augsta riska AI sistēmu pēctirgus uzraudzības plāns

1. Sagādātāji izveido un dokumentē pēctirgus uzraudzības sistēmu tādā veidā, kas ir proporcionāls mākslīgā intelekta tehnoloģiju raksturam un augsta riska AI sistēmas riskiem.
2. Pēctirgus uzraudzības sistēma aktīvi un sistemātiski vāc, dokumentē un analizē attiecīgos datus, kurus sniedz lietotāji vai kuri savākti no citiem avotiem par augsta riska AI sistēmu veikspēju visā to darbības laikā, un ļauj sagādātājam izvērtēt AI sistēmu nepārtrauktu atbilstību III sadaļas 2. nodaļā noteiktajām prasībām.
3. Pēctirgus uzraudzības sistēmas pamatā ir pēctirgus uzraudzības plāns. Pēctirgus uzraudzības plāns ir IV pielikumā minētās tehniskās dokumentācijas daļa. Komisija pieņem īstenošanas aktu, ar ko nosaka sīki izstrādātus noteikumus, ar kuriem izveido paraugu pēctirgus uzraudzības plānam un plānā iekļaujamo elementu sarakstu.
4. Augsta riska AI sistēmām, uz kurām attiecas II pielikumā minētie tiesību akti, ja saskaņā ar šiem tiesību aktiem jau ir izveidota pēctirgus uzraudzības sistēma un plāns, 1., 2. un 3. punktā aprakstītos elementus pēc vajadzības integrē šajā sistēmā un plānā.

Pirmo daļu piemēro arī III pielikuma 5. punkta b) apakšpunktā minētajām augsta riska AI sistēmām, ko laiž tirgū vai nodod ekspluatācijā kredītiestādes, kuru darbību regulē Direktīva 2013/36/ES.

2. NODAĻA

INFORMĀCIJAS KOPĪGOŠANA PAR INCIDENTIEM UN DARBĪBAS TRAUCĒJUMIEM

62. pants

Ziņošana par nopietniem incidentiem un darbības traucējumiem

1. Savienības tirgū laistu augsta riska AI sistēmu sagādātāji par visiem nopietniem incidentiem vai šo sistēmu darbības traucējumiem, kas ietver Savienības tiesību aktos, kuru mērķis ir aizsargāt pamattiesības, paredzēto pienākumu pārkāpumu, ziņo tirgus uzraudzības iestādēm dalībvalstīs, kur noticis šis incidents vai pārkāpums.
Šādu paziņojumu sniedz tūlīt pēc tam, kad sagādātājs ir konstatējis cēloņsakarību starp AI sistēmu un incidentu vai darbības traucējumiem, vai šādas saiknes pamatotu iespējamību, un jebkurā gadījumā ne vēlāk kā 15 dienas pēc tam, kad sagādātājs uzzinājis par nopietnu incidentu vai darbības traucējumiem.

2. Saņēmusi paziņojumu par tādu pienākumu neizpildi, kas noteikti Savienības tiesību aktos, kuru mērķis ir aizsargāt pamattiesības, tirgus uzraudzības iestāde informē 64. panta 3. punktā minētās publiskā sektora iestādes vai struktūras. Komisija izstrādā īpašus norādījumus, lai veicinātu 1. punktā noteikto pienākumu izpildi. Minētos norādījumus izdod ne vēlāk kā 12 mēnešus pēc šīs regulas stāšanās spēkā.
3. III pielikuma 5. punkta b) apakšpunktā minētajām augsta riska AI sistēmām, kuras laiž tirgū vai nodod ekspluatācijā sagādātāji, kas ir ar Direktīvu 2013/36/ES regulētas kredītiestādes, un augsta riska AI sistēmām, kuras ir ierīču drošības sastāvdaļas vai arī pašas uzskatāmas par ierīcēm, uz ko attiecas Regula (ES) 2017/745 un Regula (ES) 2017/746, ziņošana par nopietniem incidentiem vai darbības traucējumiem attiecas tikai uz gadījumiem, kad tiek pārkāpti pienākumi, kas noteikti Savienības tiesību aktos, kuru mērķis ir aizsargāt pamattiesības.

3. NODAĻA

IZPILDES PANĀKŠANA

63. pants

Tirgus uzraudzība un AI sistēmu pārziņa Savienības tirgū

1. Uz AI sistēmām, kas ir šīs regulas darbības jomā, attiecas Regula (ES) 2019/1020. Tomēr šīs regulas efektīvas izpildes nolūkos:
 - (a) atsauces uz Regulas (ES) 2019/1020 terminu “uzņēmējs” saprot kā tādas, kas ietver visus šīs regulas III sadaļā norādītos operatorus;
 - (b) atsauces uz Regulā (ES) 2019/1020 lietoto apzīmējumu “produkts” saprot kā tādas, kas ietver visas AI sistēmas, uz kurām attiecas šī regula.
2. Valsts uzraudzības iestāde regulāri ziņo Komisijai par attiecīgo tirgus uzraudzības darbību rezultātiem. Valsts uzraudzības iestāde nekavējoties ziņo Komisijai un attiecīgajām valsts konkurences iestādēm par visu tirgus uzraudzības darbībās identificēto informāciju, kas tās varētu interesēt Savienības konkurences tiesību normu piemērošanā.
3. Augsta riska AI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas II pielikuma A iedaļā uzskaitītie tiesību akti, tirgus uzraudzības iestāde šīs regulas vajadzībām ir iestāde, kas atbild par tirgus uzraudzības darbībām, kuras noteiktas saskaņā ar minētajiem tiesību aktiem.
4. AI sistēmām, ko laiž tirgū, nodod ekspluatācijā vai izmanto finanšu iestādes, kuras reglamentē Savienības tiesību akti par finanšu pakalpojumiem, tirgus uzraudzības iestāde šīs regulas vajadzībām ir attiecīgā iestāde, kas saskaņā ar minētajiem tiesību aktiem atbild par šo iestāžu finanšu uzraudzību.
5. 1. punkta a) apakšpunktā minētajām AI sistēmām, ciktāl sistēmas izmanto tiesībaizsardzības nolūkos, kā minēts III pielikuma 6. un 7. punktā, dalībvalstis šīs regulas vajadzībām par tirgus uzraudzības iestādēm ieceļ vai nu kompetentās datu aizsardzības uzraudzības iestādes saskaņā ar Direktīvu (ES) 2016/680 vai Regulu 2016/679, vai valstu kompetentās iestādes, kas uzrauga to tiesībaizsardzības, imigrācijas vai patvēruma iestāžu darbu, kuras nodod ekspluatācijā vai izmanto šīs sistēmas.

6. Ja šīs regulas darbības jomā ietilpst Savienības iestādes, aģentūras un struktūras, kā to tirgus uzraudzības iestāde darbojas Eiropas Datu aizsardzības uzraudzītājs.
7. Dalībvalstis atbalsta koordināciju starp tirgus uzraudzības iestādēm, kas norīkotas saskaņā ar šo regulu, un citām attiecīgām valsts iestādēm vai struktūrām, kas pārrauga II pielikumā uzskaitīto Savienības saskaņošanas tiesību aktu vai citu tādu Savienības tiesību aktu piemērošanu, kuri varētu būt svarīgi attiecībā uz III pielikumā minētajām augsta riska AI sistēmām.

64. pants

Piekļuve datiem un dokumentācijai

1. Attiecībā uz piekļuvi datiem un dokumentācijai saistībā ar to darbību tirgus uzraudzības iestādēm piešķir pilnu piekļuvi sagādātāja izmantotajām apmācības, validēšanas un testēšanas datu kopām – arī ar lietojumprogrammu saskarnēm (API) vai citiem piemērotiem līdzekļiem un rīkiem, kas nodrošina attālu piekļuvi.
2. Ja tas nepieciešams, lai novērtētu augsta riska AI sistēmas atbilstību III sadaļas 2. nodaļā noteiktajām prasībām, un pēc pamatota pieprasījuma tirgus uzraudzības iestādēm piešķir piekļuvi AI sistēmas pirmkodam.
3. Valstu publiskā sektora iestādēm vai struktūrām, kas uzrauga vai panāk to pienākumu izpildi, kuri noteikti Savienības tiesību aktos, kas aizsargā pamattiesības saistībā ar III pielikumā minēto augsta riska AI sistēmu izmantošanu, ir tiesības pieprasīt un piekļūt jebkurai dokumentācijai, kas sagatavota vai tiek uzturēta saskaņā ar šo regulu, ja piekļuve šai dokumentācijai ir nepieciešama, lai izpildītu to pilnvarās noteiktās kompetences savas jurisdikcijas robežās. Attiecīgā publiskā sektora iestāde vai struktūra par tādu pieprasījumu informē attiecīgās dalībvalsts tirgus uzraudzības iestādi.
4. Trīs mēnešus pēc šīs regulas stāšanās spēkā katra dalībvalsts identificē 3. punktā minētās publiskā sektora iestādes vai struktūras un šo sarakstu dara publiski pieejamu valsts uzraudzības iestādes tīmekļa vietnē. Dalībvalstis sarakstu dara zināmu Komisijai un visām pārējām dalībvalstīm un to regulāri atjaunina.
5. Ja 3. punktā minētā dokumentācija nav pietiekama, lai pārliecinātos, vai ir notikusi tādu pienākumu neizpilde, kas noteikti Savienības tiesību aktos, kuru mērķis ir aizsargāt pamattiesības, 3. punktā minētā publiskā sektora iestāde vai struktūra tirgus uzraudzības iestādei var iesniegt pamatotu pieprasījumu organizēt augsta riska AI sistēmas testēšanu ar tehniskiem līdzekļiem. Tirgus uzraudzības iestāde saprātīgā laikposmā pēc pieprasījuma organizē testēšanu, cieši iesaistot pieprasījuma iesniedzēju publiskā sektora iestādē vai struktūrā.
6. Informācija un dokumentācija, ko saskaņā ar šā panta noteikumiem ieguvušas 3. punktā minētās publiskā sektora iestādes vai struktūras, tiek apstrādāta saskaņā ar 70. pantā noteiktajiem konfidencialitātes pienākumiem.

65. pants

Procedūra darbībām ar AI sistēmām, kuras rada risku valsts līmenī

1. AI sistēmas, kas rada risku, ir jāsaprot kā Regulas (ES) 2019/1020 3. panta 19. punktā definētais produkts, kas rada risku, cik tas attiecas uz risku cilvēku veselībai, drošībai vai cilvēku pamattiesību aizsardzībai.

2. Ja dalībvalsts tirgus uzraudzības iestādei ir pietiekami daudz iemeslu uzskatīt, ka AI sistēma rada 1. punktā minēto risku, tā veic attiecīgās AI sistēmas izvērtēšanu attiecībā uz tās atbilstību visām prasībām un pienākumiem, kas noteikti šajā regulā. Ja pastāv riski attiecībā uz pamattiesību aizsardzību, tirgus uzraudzības iestāde informē arī attiecīgās publiskā sektora iestādes vai struktūras, kas minētas 64. panta 3. punktā. Attiecīgie operatori pēc vajadzības sadarbojas ar tirgus uzraudzības iestādēm un pārējām 64. panta 3. punktā minētajām publiskā sektora iestādēm vai struktūrām.

Ja izvērtēšanā tirgus uzraudzības iestāde konstatē, ka augsta riska AI sistēma neatbilst šīs regulas prasībām un pienākumiem, tā nekavējoties pieprasa attiecīgajam operatoram veikt visus attiecīgos korektīvos pasākumus, kas vajadzīgi, lai panāktu AI sistēmas atbilstību vai lai samērīgi riskam to izņemtu no tirgus vai atsauktu šīs iestādes noteiktā pienācīgā termiņā.

Tirgus uzraudzības iestāde attiecīgi informē attiecīgo pieteikto struktūru. Uz otrajā daļā minētajiem pasākumiem attiecas Regulas (ES) 2019/1020 18. pants.
3. Ja tirgus uzraudzības iestāde uzskata, ka neatbilstība ir vērojama ne tikai tās valsts teritorijā, tā informē Komisiju un pārējās dalībvalstis par izvērtēšanas rezultātiem un par pasākumiem, ko tās pieprasījušas veikt operatoram.
4. Operators nodrošina, ka visi piemērotie korektīvie pasākumi tiek veikti attiecībā uz visām attiecīgajām AI sistēmām, kuras tas darījis pieejamas visā Savienības tirgū.
5. Ja attiecīgais AI sistēmas operators neveic pienācīgus korektīvus pasākumus 2. punktā noteiktajā termiņā, tirgus uzraudzības iestāde veic visus vajadzīgos pagaidu pasākumus, lai aizliegtu vai ierobežotu to, ka AI sistēma tiek darīta pieejama tās valsts tirgū, izņemtu to no minētā tirgus vai atsauktu to. Par šiem pasākumiem šī iestāde nekavējoties informē Komisiju un pārējās dalībvalstis.
6. Šā panta 5. punktā minētajā informācijā ietver visas pieejamās ziņas, sevišķi datus neatbilstīgās AI sistēmas identificēšanai, datus par AI sistēmas izcelsmi, attiecīgo neatbilstības veidu un ar to saistīto risku, veikto valsts pasākumu veidu un ilgumu, kā arī attiecīgā operatora viedokli. Tirgus uzraudzības iestādes īpaši norāda, vai neatbilstība ir saistīta ar vienu vai vairākiem šādiem aspektiem:
 - (a) AI sistēmas neatbilstība III sadaļas 2. nodaļā noteiktajām prasībām;
 - (b) trūkumi 40. un 41. pantā minētajos saskaņotajos standartos vai kopīgās specifikācijās, uz kuru pamata piešķir atbilstības prezumpciju.
7. Dalībvalstu tirgus uzraudzības iestādes, kas nav procedūru sākušās dalībvalsts tirgus uzraudzības iestādes, nekavējoties informē Komisiju un pārējās dalībvalstis par visiem pieņemtajiem pasākumiem un visu savā rīcībā esošo papildu informāciju par attiecīgās AI sistēmas neatbilstību un – ja tās nepiekrīt pieņemtajam valsts pasākumam – informē par saviem iebildumiem.
8. Ja triju mēnešu laikā pēc 5. punktā minētās informācijas saņemšanas neviena dalībvalsts vai Komisija nav cēlusi iebildumus pret kādas dalībvalsts veiktu pagaidu pasākumu, minēto pasākumu uzskata par pamatotu. Tas neskar attiecīgā operatora procesuālās tiesības saskaņā ar Regulas (ES) 2019/1020 18. pantu.
9. Visu dalībvalstu tirgus uzraudzības iestādes nodrošina, ka attiecībā uz attiecīgo produktu nekavējoties tiek veikti atbilstoši ierobežojoši pasākumi, piemēram, produkta izņemšana no to tirgus.

*66. pants
Savienības drošības procedūra*

1. Ja trīs mēnešu laikā pēc 65. panta 5. punktā minētā paziņojuma saņemšanas dalībvalsts ceļ iebildumus par citas dalībvalsts veiktu pasākumu vai ja Komisija uzskata, ka pasākums ir pretrunā Savienības tiesību aktiem, Komisija nekavējoties uzsāk apspriešanos ar attiecīgo dalībvalsti un operatoru vai operatoriem un izvērtē valsts pasākumu. Pamatojoties uz šā izvērtējuma rezultātiem, Komisija deviņu mēnešu laikā pēc 65. panta 5. punktā minētā paziņojuma saņemšanas izlemj, vai valsts pasākums ir pamatots, un šo lēmumu dara zināmu attiecīgajai dalībvalstij.
2. Ja valsts pasākums tiek atzīts par pamatotu, visas dalībvalstis veic nepieciešamos pasākumus, lai panāktu neatbilstīgās AI sistēmas izņemšanu no sava tirgus, un par to attiecīgi informē Komisiju. Ja valsts pasākums tiek atzīts par nepamatotu, attiecīgā dalībvalsts pasākumu atceļ.
3. Ja valsts pasākums tiek uzskatīts par pamatotu un AI sistēmas neatbilstība tiek saistīta ar trūkumiem šīs regulas 40. un 41. pantā minētajos saskaņotajos standartos vai kopīgās specifikācijās, Komisija piemēro Regulas (ES) Nr. 1025/2012 11. pantā paredzēto procedūru.

*67. pants
Atbilstīgas AI sistēmas, kas rada risku*

1. Ja dalībvalsts tirgus uzraudzības iestāde pēc izvērtēšanas saskaņā ar 65. pantu secina, ka AI sistēma gan atbilst šai regulai, bet rada risku cilvēku veselībai vai drošībai, Savienības vai valsts tiesību aktu noteikto pienākumu izpildei vai citiem vispārības interešu aizsardzības aspektiem, ko aptver šī regula, tā pieprasa attiecīgajam operatoram veikt visus attiecīgos pasākumus, kas vajadzīgi, lai nodrošinātu, ka attiecīgā AI sistēma, kad tā tiek laista tirgū vai nodota ekspluatācijā, vairs nerada šo risku, vai lai samērīgi riskam šo AI sistēmu izņemtu no tirgus vai atsauktu šīs iestādes noteiktā pienācīgā termiņā.
2. Sagādātājs vai citi attiecīgie operatori 1. punktā minētās dalībvalsts tirgus uzraudzības iestādes noteiktajā termiņā nodrošina, ka tiek veikti korektīvi pasākumi attiecībā uz visām attiecīgajām AI sistēmām, kuras viņi ir darījuši pieejamas tirgū Savienībā.
3. Dalībvalsts nekavējoties informē Komisiju un pārējās dalībvalstis. Informācijā ietver visas pieejamās ziņas, sevišķi datus, kas nepieciešami attiecīgās AI sistēmas identificēšanai, datus par tās izcelsmi un piegādes ķēdi, konkrētā riska veidu un veikto valsts pasākumu veidu un ilgumu.
4. Komisija nekavējoties sāk apspriešanos ar dalībvalstīm un attiecīgo operatoru un izvērtē valsts veiktos pasākumus. Pamatojoties uz minētā izvērtējuma rezultātiem, Komisija pieņem lēmumu par to, vai pasākums ir vai nav pamatots, un attiecīgā gadījumā ierosina pienācīgus pasākumus.
5. Minēto lēmumu Komisija adresē dalībvalstīm.

*68. pants
Formāla neatbilstība*

1. Ja dalībvalsts tirgus uzraudzības iestāde konstatē kādu no tālāk norādītajām problēmām, tā pieprasa, lai attiecīgais sagādātājs novērst attiecīgo neatbilstību:

- (a) atbilstības zīme ir uzlikta, pārkāpjot 49. pantu;
 - (b) atbilstības zīme nav uzlikta;
 - (c) nav sagatavota ES atbilstības deklarācija;
 - (d) ES atbilstības deklarācija ir sagatavota nepareizi;
 - (e) attiecīgā gadījumā nav norādīts tās pieteiktās struktūras identifikācijas numurs, kura ir iesaistīta atbilstības novērtēšanas procedūrā.
2. Ja 1. punktā minētā neatbilstība netiek novērsta, attiecīgā dalībvalsts veic pienācīgus pasākumus, lai ierobežotu vai aizliegtu augsta riska AI sistēmu darīt pieejamu tirgū vai panāktu tās atsaukšanu vai izņemšanu no tirgus.

IX SADAĻA

RĪCĪBAS KODEKSI

69. pants

Rīcības kodeksi

1. Komisija un dalībvalstis veicina un atvieglo tādu rīcības kodeksu izstrādi, kuru mērķis ir veicināt III sadaļas 2. nodaļā noteikto prasību brīvprātīgu piemērošanu AI sistēmām, kuras nav augsta riska AI sistēmas, pamatojoties uz tehniskajām specifikācijām un risinājumiem, kas ir piemēroti līdzekļi, ar kuriem nodrošināt atbilstību šādām prasībām, ņemot vērā sistēmām paredzēto nolūku.
2. Komisija un AI padome veicina un atvieglo tādu rīcības kodeksu izstrādi, kuru mērķis ir veicināt tādu prasību brīvprātīgu piemērošanu AI sistēmām, kas saistītas, piemēram, ar vides ilgtspēju, pieejamību invalīdiem, ieinteresēto personu dalību AI sistēmu projektēšanā un izstrādē un projektēšanas komandu daudzveidību, pamatojoties uz skaidriem mērķiem un svarīgākajiem veikspējas rādītājiem, pēc kuriem var novērtēt šo mērķu sasniegšanu.
3. Rīcības kodeksus var izstrādāt atsevišķi AI sistēmu sagādātāji vai organizācijas, kas tos pārstāv, vai abēji, arī – iesaistot lietotājus un ieinteresētās personas un organizācijas, kas tās pārstāv. Rīcības kodeksi var aptvert vienu vai vairākas AI sistēmas, ņemot vērā attiecīgajām sistēmām paredzētā nolūka līdzību.
4. Veicinot un atvieglojot rīcības kodeksu izstrādi, Komisija un AI padome ņem vērā mazapjoma sagādātāju un jaunuzņēmumu īpašās intereses un vajadzības.

X SADAĻA

KONFIDENCIALITĀTE UN SODI

70. pants

Konfidencialitāte

1. Valstu kompetentās iestādes un pieteiktās struktūras, kas iesaistītas šīs regulas piemērošanā, ievēro to uzdevumu un darbību izpildes gaitā iegūtas informācijas un datu konfidencialitāti tādā veidā, lai sevišķi aizsargātu:
 - (a) intelektuālā īpašuma tiesības un fiziskas vai juridiskas personas konfidencialu uzņēmējdarbības informāciju vai komercnoslēpumus, ieskaitot pirmkodu,

izņemot gadījumus, kas minēti 5. pantā Direktīvā (ES) 2016/943 par zinātnības un darījumdarbības neizpaužamas informācijas (komercnoslēpumu) aizsardzību pret nelikumīgu iegūšanu, izmantošanu un izpaušanu;

- (b) šīs regulas efektīvu īstenošanu, sevišķi pārbaudi, izmeklēšanas vai revīzijas nolūkos;
 - (c) sabiedrības un valsts drošības intereses;
 - (d) kriminālprocesu vai administratīvo procesu neaizskaramību.
2. Neskarot 1. punktu, informāciju, ar kuru konfidenciali apmainās valstu kompetentās iestādes savā starpā, kā arī valstu kompetentās iestādes un Komisija, neizpauž bez iepriekšējas apspriešanās ar izcelsmes valsts kompetento iestādi un lietotāju, ja III pielikuma 1., 6. un 7. punktā minētās augsta riska AI sistēmas lieto tiesībaizsardzības, imigrācijas vai patvēruma iestādes un izpaušana apdraudētu sabiedrības un valsts drošības intereses.
- Ja tiesībaizsardzības, imigrācijas vai patvēruma iestādes ir III pielikuma 1., 6. un 7. punktā minēto augsta riska AI sistēmu sagādātāji, IV pielikumā minētā tehniskā dokumentācija glabājas šo iestāžu telpās. Šīs iestādes nodrošina, ka tirgus uzraudzības iestādes, kas attiecīgi minētas 63. panta 5. un 6. punktā, pēc pieprasījuma var nekavējoties piekļūt dokumentācijai vai iegūt tās kopiju. Tikai tirgus uzraudzības iestādes darbiniekiem, kuriem ir atbilstoša drošības pielaide, ir atļauts piekļūt šai dokumentācijai vai tās kopijai.
3. 1. un 2. punkts neietekmē Komisijas, dalībvalstu un pieteikto struktūru tiesības un pienākumus attiecībā uz informācijas apmaiņu un brīdinājumu izplatīšanu, kā arī attiecīgo pušu pienākumu sniegt informāciju saskaņā ar dalībvalstu krimināltiesībām.
4. Vajadzības gadījumā Komisija un dalībvalstis var apmainīties ar konfidencialu informāciju ar tām trešo valstu regulatīvajām iestādēm, ar kurām tās ir noslēgušas divpusējus vai daudzpusējus konfidencialitātes nolīgumus, kas garantē pietiekamu konfidencialitātes līmeni.

71. pants Sodi

1. Saskaņā ar šīs regulas noteikumiem dalībvalstis nosaka noteikumus par sodiem, arī administratīvajiem naudas sodiem, kas piemērojami par šīs regulas pārkāpumiem, un veic visus nepieciešamos pasākumus, lai nodrošinātu to pareizu un efektīvu īstenošanu. Paredzētie sodi ir efektīvi, samērīgi un atturoši. Tajos īpaši ņem vērā mazapjoma sagādātāju un jaunuzņēmumu intereses un ekonomisko dzīvotspēju.
2. Dalībvalstis minētos noteikumus un pasākumus dara zināmus Komisijai un nekavējoties tai paziņo par pēckākiem grozījumiem, kas tos ietekmē.
3. Par šādiem pārkāpumiem piemēro administratīvos naudas sodus līdz 30 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 6 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarā no tā, kurš no tiem ir lielāks:
- (a) 5. pantā minētās mākslīgā intelekta prakses aizlieguma neievērošana;
 - (b) AI sistēmas neatbilstība 10. pantā noteiktajām prasībām.
4. Par AI sistēmas neatbilstību šajā regulā noteiktajām prasībām vai pienākumiem, izņemot tos, kas noteikti 5. un 10. pantā, piemēro administratīvos naudas sodus līdz

20 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 4 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarā no tā, kurš no tiem ir lielāks.

5. Par nepareizas, nepilnīgas vai maldinošas informācijas sniegšanu pieteiktajām struktūrām un valsts kompetentajām iestādēm atbildē uz pieprasījumu piemēro administratīvos naudas sodus līdz 10 000 000 EUR apmērā vai, ja pārkāpējs ir uzņēmums, līdz 2 % apmērā no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarā no tā, kurš no tiem ir lielāks.
6. Lemjot par administratīvā naudas soda apmēru, katrā atsevišķā gadījumā ņem vērā visus īpašos konkrētās situācijas apstākļus un rūpīgi izvērtē šādus elementus:
 - (a) pārkāpuma un tā seku raksturu, smagumu un ilgumu;
 - (b) to, vai citas tirgus uzraudzības iestādes jau ir piemērojušas administratīvos naudas sodus tam pašam operatoram par to pašu pārkāpumu;
 - (c) operatora, kurš veicis pārkāpumu, lielumu un tirgus daļu.
7. Katra dalībvalsts pieņem noteikumus par to, vai šīs dalībvalsts publiskā sektora iestādēm un struktūrām var uzlikt administratīvos naudas sodus un cik lielā apmērā.
8. Atkarā no dalībvalstu tiesību sistēmas noteikumus par administratīvajiem naudas sodiem var piemērot tādā veidā, ka naudas sodus uzliek citu struktūru kompetentās valsts tiesas tā, kā tas ir piemērojams šajās dalībvalstīs. Šādu noteikumu piemērošanai šajās dalībvalstīs ir līdzvērtīga ietekme.

72. pants

Administratīvie naudas sodi Savienības iestādēm, aģentūrām un struktūrām

1. Eiropas Datu aizsardzības uzraudzītājs var uzlikt administratīvus naudas sodus Savienības iestādēm, aģentūrām un struktūrām, uz kurām attiecas šī regula. Lemjot par to, vai piemērot administratīvo naudas sodu, un pieņemot lēmumu par administratīvā naudas soda apmēru, katrā atsevišķā gadījumā ņem vērā visus īpašos konkrētās situācijas apstākļus un rūpīgi izvērtē šādus elementus:
 - (a) pārkāpuma un tā seku raksturu, smagumu un ilgumu;
 - (b) sadarbību ar Eiropas Datu aizsardzības uzraudzītāju nolūkā novērst pārkāpumu un mazināt iespējamās pārkāpuma nelabvēlīgās sekas, ieskaitot tādu pasākumu izpildi, kurus Eiropas Datu aizsardzības uzraudzītājs jau iepriekš ir noteicis attiecīgajai Savienības iestādei, aģentūrai vai struktūrai tajā pašā jautājumā;
 - (c) līdzīgus agrākus Savienības iestādes, aģentūras vai struktūras pārkāpumus.
2. Par šādiem pārkāpumiem piemēro administratīvos naudas sodus līdz 500 000 EUR apmērā:
 - (a) 5. pantā minētās mākslīgā intelekta prakses aizlieguma neievērošana;
 - (b) AI sistēmas neatbilstība 10. pantā noteiktajām prasībām.
3. Par AI sistēmas neatbilstību šajā regulā noteiktajām prasībām vai pienākumiem, atskaitot tos, kas noteikti 5. un 10. pantā, piemēro administratīvos naudas sodus līdz 250 000 EUR apmērā.
4. Pirms lēmumu pieņemšanas saskaņā ar šo pantu Eiropas Datu aizsardzības uzraudzītājs dod Savienības iestādei, aģentūrai vai struktūrai, kura ir Eiropas Datu aizsardzības uzraudzītāja veikto procedūru subjekts, iespēju izteikt viedokli

jautājumā par iespējamo pārkāpumu. Eiropas Datu aizsardzības uzraudzītājs balsta savus lēmumus vienīgi uz tiem elementiem un apstākļiem, kurus iesaistītās personas ir varējušas komentēt. Sūdzību iesniedzējus, ja tādi ir, cieši iesaista procedūrās.

5. Procedūrās pilnībā ievēro attiecīgo pušu aizstāvības tiesības. Tām ir tiesības piekļūt Eiropas Datu aizsardzības uzraudzītāja lietas materiāliem, ievērojot fizisku personu likumīgās intereses persondatu aizsardzībā un uzņēmumu likumīgās intereses darījumdarbības noslēpumu aizsardzībā.
6. Līdzekļi, kas iegūti, uzliekot naudas sodus saskaņā ar šo pantu, ir Savienības vispārējā budžeta ieņēmumi.

XI SADAĻA

PILNVARU DELEĢĒŠANA UN KOMITEJU PROCEDŪRA

73. pants

Deleģēšanas īstenošana

1. Komisijai tiek piešķirtas pilnvaras pieņemt deleģētos aktus, ievērojot šajā pantā izklāstītos nosacījumus.
2. Uz neierobežotu laiku no *[datums, kad stājas spēkā šī regula]* Komisija tiek pilnvarota pieņemt 4. pantā, 7. panta 1. punktā, 11. panta 3. punktā, 43. panta 5. un 6. punktā un 48. panta 5. punktā minētos deleģētos aktus.
3. Eiropas Parlaments vai Padome jebkurā brīdī var atsaukt 4. pantā, 7. panta 1. punktā, 11. panta 3. punktā, 43. panta 5. un 6. punktā un 48. panta 5. punktā minēto pilnvaru deleģējumu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģējumu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.
4. Tiklīdz Komisija pieņem deleģētu aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.
5. Saskaņā ar 4. pantu, 7. panta 1. punktu, 11. panta 3. punktu, 43. panta 5. un 6. punktu un 48. panta 5. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts izziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par trim mēnešiem.

74. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.
2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

XII SADAĻA

NOBEIGUMA NOTEIKUMI

75. pants

Grozījums Regulā (EK) Nr. 300/2008

Regulas (EK) Nr. 300/2008 4. panta 3. punktam pievieno šādu daļu:

“Pieņemot detalizētus pasākumus, kas skar tehniskās specifikācijas un drošības aprīkojuma apstiprināšanas un lietošanas procedūras, kuras attiecas uz mākslīgā intelekta sistēmām Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

76. pants

Grozījums Regulā (ES) Nr. 167/2013

Regulas (ES) Nr. 167/2013 17. panta 5. punktam pievieno šādu daļu:

“Uz šā punkta pirmās daļas pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

77. pants

Grozījums Regulā (ES) Nr. 168/2013

Regulas (ES) Nr. 168/2013 22. panta 5. punktam pievieno šādu daļu:

“Uz šā punkta pirmās daļas pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

78. pants

Grozījums Direktīvā 2014/90/ES

Direktīvas 2014/90/ES 8. pantam pievieno šādu punktu:

“4. Attiecībā uz mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, veicot darbības saskaņā ar 1. punktu un pieņemot tehniskās specifikācijas un testēšanas standartus saskaņā ar 2. un 3. punktu, Komisija ņem vērā prasības, kas noteiktas minētās regulas III sadaļas 2. nodaļā.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

*79. pants
Grozījums Direktīvā (ES) 2016/797*

Direktīvas (ES) 2016/797 5. pantam pievieno šādu punktu:

“12. Atbilstoši 1. punktam un uz 11. punkta pamata pieņemtajiem īstenošanas aktiem pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

*80. pants
Grozījums Regulā (ES) 2018/858*

Regulas (ES) 2018/858 5. pantam pievieno šādu punktu:

“4. Uz 3. punkta pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

*81. pants
Grozījumi Regulā (ES) 2018/1139*

Regulu (ES) 2018/1139 groza šādi:

1) regulas 17. pantam pievieno šādu punktu:

“3. Neskarot 2. punktu, uz 1. punkta pamata pieņemot īstenošanas aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”;

2) regulas 19. pantam pievieno šādu punktu:

“4. Uz 1. un 2. punkta pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

3) regulas 43. pantam pievieno šādu punktu:

“4. Uz 1. punkta pamata pieņemot īstenošanas aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.”

4) regulas 47. pantam pievieno šādu punktu:

“3. Uz 1. un 2. punkta pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

5) regulas 57. pantam pievieno šādu daļu:

“Pieņemot minētos īstenošanas aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.”

6) regulas 58. pantam pievieno šādu punktu:

“3. Uz 1. un 2. punkta pamata pieņemot deleģētos aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.”

82. pants

Grozījums Regulā (ES) 2019/2144

Regulas (ES) 2019/2144 11. pantam pievieno šādu punktu:

“3. Uz 2. punkta pamata pieņemot īstenošanas aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) YYYY/XX [par mākslīgo intelektu]* nozīmē, ņem vērā minētās regulas III sadaļas 2. nodaļā noteiktās prasības.

* Regula (ES) YYYY/XX [par mākslīgo intelektu] (OV ...).”.

83. pants

AI sistēmas, kas jau ir laistas tirgū vai nodotas ekspluatācijā

1. Šī regula neattiecas uz AI sistēmām, kas ir tādu lielapjoma IT sistēmu sastāvdaļas, kuras izveidotas ar IX pielikumā uzskaitītajiem tiesību aktiem, un kas ir laistas tirgū vai nodotas ekspluatācijā pirms [12 mēneši pēc šīs regulas piemērošanas dienas, kā minēts 85. panta 2. punktā], ja minēto tiesību aktu aizstāšana vai grozīšana nerada būtiskas izmaiņas attiecīgās AI sistēmas vai AI sistēmu uzbūvē vai tām paredzētajā nolūkā.

Šajā regulā noteiktās prasības attiecīgā gadījumā ņem vērā, veicot katras ar IX pielikumā uzskaitītajiem tiesību aktiem izveidotās lielapjoma IT sistēmas izvērtēšanu, kas jāveic tā, kā paredzēts šajos attiecīgajos tiesību aktos.

2. Uz augsta riska AI sistēmām, kuras ir laistas tirgū vai nodotas ekspluatācijā pirms [šīs regulas piemērošanas datums, kas minēts 85. panta 2. punktā], atskaitot 1. punktā minētās, šī regula attiecas tikai tad, ja no minētā datuma šajās sistēmās notikušas būtiskas izmaiņas to uzbūvē vai tām paredzētajā nolūkā.

84. pants

Izvērtēšana un pārskatīšana

1. Reizi gadā pēc šīs regulas stāšanās spēkā Komisija novērtē nepieciešamību grozīt III pielikuma sarakstu.
2. Līdz [trīs gadus pēc šīs regulas piemērošanas dienas, kas minēta 85. panta 2. punktā] un pēc tam ik pēc četriem gadiem Komisija iesniedz Eiropas Parlamentam

un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu. Šos ziņojumus publicē.

3. Ziņojumos, kas minēti 2. punktā, īpašu uzmanību pievērš šādiem jautājumiem:
 - (a) to valstu kompetento iestāžu finanšu resursu un cilvēkresursu statuss, kas vajadzīgi, lai efektīvi veiktu uzdevumus, kuri tām uzticēti saskaņā ar šo regulu;
 - (b) sodu sistēma, it īpaši administratīvie naudas sodi, kas minēti 71. panta 1. punktā, kurus dalībvalstis piemēro par šīs regulas noteikumu pārkāpumiem.
4. [Trīs gadu laikā pēc šīs regulas piemērošanas dienas, kas minēta 85. panta 2. punktā] un pēc tam ik pēc četriem gadiem Komisija izvērtē rīcības kodeksu ietekmi un efektivitāti, lai veicinātu III sadaļas 2. nodaļas prasību piemērošanu un, iespējams, citu papildu prasību piemērošanu attiecībā uz AI sistēmām, kas nav augsta riska AI sistēmas.
5. Šā panta 1.–4. punkta vajadzībām AI padome, dalībvalstis un valstu kompetentās iestādes Komisijai pēc tās pieprasījuma sniedz informāciju.
6. Veicot 1.–4. punktā minēto izvērtēšanu un pārskatīšanu, Komisija ņem vērā AI padomes, Eiropas Parlamenta, Padomes un citu attiecīgo struktūru vai avotu nostāju un konstatējumus.
7. Vajadzības gadījumā Komisija iesniedz attiecīgus priekšlikumus par šīs regulas grozīšanu, ņemot vērā galvenokārt norises tehnoloģiju jomā un attīstības stāvokli informācijas sabiedrībā.

85. pants

Stāšanās spēkā un piemērošana

1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.
2. Šo regulu piemēro no [24 mēneši pēc šīs regulas stāšanās spēkā].
3. Atkāpjoties no 2. punkta:
 - (a) III sadaļu, 4. nodaļu un VI sadaļu piemēro no [trīs mēneši pēc šīs regulas stāšanās spēkā];
 - (b) 71. pantu piemēro no [12 mēneši pēc šīs regulas stāšanās spēkā].

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

*Eiropas Parlamenta vārdā –
priekšsēdētājs*

*Padomes vārdā –
priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

- 1.1. Priekšlikuma/iniciatīvas nosaukums
- 1.2. Attiecīgā rīcībpolitikas joma
- 1.3. Priekšlikums/iniciatīva attiecas uz:
- 1.4. Mērķi
 - 1.4.1. Vispārīgie mērķi
 - 1.4.2. Specifiskie mērķi
 - 1.4.3. Paredzami rezultāti un ietekme
 - 1.4.4. Veiktspējas rādītāji
- 1.5. Priekšlikuma/iniciatīvas pamatojums
 - 1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvērtēšanas grafiks
 - 1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.
 - 1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas
 - 1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem
 - 1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtēšana
- 1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme
- 1.7. Paredzētie pārvaldības veidi

2. PĀRVALDĪBAS PASĀKUMI

- 2.1. Pārraudzības un ziņošanas noteikumi
- 2.2. Pārvaldības un kontroles sistēma
 - 2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums
 - 2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu
 - 2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Aplēstā ietekme uz ieņēmumiem

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Eiropas Parlamenta un Padomes Regula, ar ko nosaka saskaņotus noteikumus mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus

1.2. Attiecīgā rīcībpolitikas joma

Komunikācijas tīkli, saturs un tehnoloģijas.

Iekšējais tirgus, rūpniecība, uzņēmējdarbība un MVU.

Ietekme uz budžetu ir saistīta ar jaunajiem uzdevumiem, kas tiek uzticēti Komisijai, tostarp atbalstu ES AI padomei.

Darbība: Eiropas digitālās nākotnes veidošana.

1.3. Priekšlikums/iniciatīva attiecas uz:

X jaunu darbību

☐ jaunu darbību, pamatojoties uz izmēģinājuma projektu/sagatavošanas darbību⁶⁴

☐ esošas darbības pagarināšanu

☐ darbību, kas pārorientēta uz jaunu darbību

1.4. Mērķi

1.4.1. Vispārīgie mērķi

Pasākuma vispārīgais mērķis ir nodrošināt pareizu vienotā tirgus darbību, radot piemērotus apstākļus uzticama mākslīgā intelekta attīstībai un izmantošanai Savienībā.

1.4.2. Specifiskie mērķi

1. specifiskais mērķis

Noteikt prasības AI sistēmām un pienākumus visiem vērtības ķēdes dalībniekiem, lai nodrošinātu, ka tirgū laistās un izmantotās AI sistēmas ir drošas un atbilst pašreizējiem tiesību aktiem par pamattiesībām un Savienības vērtībām.

2. specifiskais mērķis

Nodrošināt juridisko noteiktību, lai veicinātu ieguldījumus AI un ar to saistītu inovāciju, skaidri nosakot, kādas būtiskās prasības, pienākumi un atbilstības noskaidrošanas un nodrošināšanas procedūras ir jāizpilda, lai Savienības tirgū laistu AI sistēmu vai to izmantotu.

3. specifiskais mērķis

Uzlabot pārvaldi un to pašreizējo AI sistēmām piemērojamo tiesību aktu efektīvu izpildi, kuros noteiktas pamattiesības un drošuma prasības, šajā nolūkā nodrošinot

⁶⁴

Kā paredzēts Finanšu regulas 54. panta 2. punkta a) vai b) apakšpunktā.

attiecīgajām iestādēm jaunas pilnvaras, resursus un skaidrus noteikumus par atbilstības novērtēšanu un pēcuzraudzības procedūrām, kā arī par pārvaldes un uzraudzības uzdevumu sadalījumu starp valsts un ES līmeni.

4. specifiskais mērķis

Veicināt vienota tirgus attīstību likumīgiem, drošiem un uzticamiem AI lietojumiem un novērst tirgus sadrumstalotību, rīkojoties ES līmenī, lai saskaņā ar pašreizējiem pamattiesību un drošuma jomas tiesību aktiem noteiktu minimālās prasības AI sistēmām, ko paredzēts laist un izmantot Savienības tirgū.

1.4.3. *Paredzami rezultāti un ietekme*

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem/mērķgrupām.

Paredzams, ka AI piegādātāji gūs labumu no minimāla, bet skaidra prasību kopuma, kas sniedz juridisko noteiktību un nodrošina piekļuvi visam vienotajam tirgum.

Paredzams, ka AI lietotājiem dos labumu juridiskā noteiktība, ka augsta riska AI sistēmas, ko tie iegādājas, atbilst Eiropas tiesību aktiem un vērtībām.

Paredzamais ieguvums patērētājiem ir samazināts risks, ka tiks pārkāpta viņu drošība vai pamattiesības.

1.4.4. *Veiktspējas rādītāji*

Norādīt priekšlikuma/iniciatīvas īstenošanas uzraudzībā izmantojamus rādītājus.

Pirmais rādītājs

Nopietnu incidentu skaits (pusgadā) vai tādu AI darbības gadījumu skaits (pusgadā), kuri uzskatāmi par nopietniem incidentiem vai pārkāpj pamattiesību pienākumus, sadalījumā pēc lietojumu jomām, aprēķināts a) absolūtā izteiksmē, b) kā daļa no ieviestajiem lietojumiem un c) kā skarto pilsoņu daļa.

Otrais rādītājs

a) Ieguldījumi mākslīgajā intelektā kopā ES (gadā)

b) Kopējie ieguldījumi mākslīgajā intelektā katrā dalībvalstī (gadā)

c) Tādu uzņēmumu daļa, kuri izmanto AI (gadā)

d) Tādu MVU daļa, kuri izmanto AI (gadā)

Rādītājus, kas minēti a) un b) punktā, aprēķinās pēc oficiāliem avotiem un salīdzinās ar privātām aplēsēm.

Datus c) un d) punktā minētajiem rādītājiem savāks regulāros uzņēmumu apsekojumos.

1.5. **Priekšlikuma/iniciatīvas pamatojums**

1.5.1. *Īstermiņā vai ilgtermiņā izpildāmās vajadzības, ieskaitot sīku iniciatīvas izvēršanas grafiku*

Regulai būtu jābūt pilnīgi piemērojamai pusotru gadu pēc tās pieņemšanas. Taču pārvaldes struktūras elementi būtu jāievieš agrāk. Konkrēti – dalībvalstīm jau iepriekš jānorīko pastāvošas iestādes un/vai jāizveido jaunas iestādes regulējumā noteikto uzdevumu izpildei, un ES AI padomei jābūt izveidotai un spējīgai rīkoties. Piemērošanas sākuma brīdī Eiropas AI sistēmu datubāzei jābūt pilnīgi darbīgai. Tādēļ līdztekus pieņemšanas procesam ir jāizstrādā datubāze, lai tās izstrāde būtu pabeigta, kad regula stājas spēkā.

1.5.2. *Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē “Savienības iesaistīšanās pievienotā vērtība” ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.*

Jauns, sadrumstalots iespējami atšķirīgu valstu noteikumu kopums apgrūtinātu AI sistēmu raitu sagādāšanu Eiropas Savienībā un nespētu atšķirīgajās dalībvalstīs

efektīvi garantēt drošumu un pamattiesību un Savienības vērtību aizsardzību. Kopīga ES rīcība AI jomā varētu stimulēt iekšējo tirgu, un tai ir lielas iespējas sniegt Eiropas nozares dalībniekiem konkurences priekšrocību globālā mērogā, kā arī panākt apjomradītus ietaupījumus, kurus dalībvalstis nevar panākt, rīkodamās atsevišķi.

1.5.3. *Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas*

Direktīvā par elektronisko tirdzniecību (Direktīvā 2000/31/EK) ir sniegts pamata satvars vienotā tirgus darbībai un digitālo pakalpojumu uzraudzībai, kā arī noteikta dalībvalstu sadarbības mehānisma pamatstruktūra; principā tā aptver visas digitālajiem pakalpojumiem piemērojamās prasības. Direktīvas izvērtējumā tika norādīts uz trūkumiem vairākos minētā sadarbības mehānisma aspektos, arī svarīgos procesuālajos aspektos, piemēram, uz to, ka nav skaidru termiņu, kādos dalībvalstīm jāsniedz atbildes, kā arī kopumā trūkst atsaučības, atbildot uz sadarbības partneru pieprasījumiem. Tādēļ gadu gaitā izveidojusies dalībvalstu savstarpēja neuzticēšanās gadījumos, kad jārisina bažas par sagādātājiem, kuri piedāvā digitālos pakalpojumus pāri robežām. Direktīvas izvērtējums parādīja, ka nepieciešams Eiropas līmenī noteikt diferencētu noteikumu un prasību kopumu. Šā iemesla dēļ, lai īstenotu konkrētās šajā regulā noteiktās prasības, būtu nepieciešams īpašs ES līmeņa sadarbības mehānisms, kura pārvaldes struktūra nodrošinātu īpašu atbildīgo struktūru koordināciju ES līmenī.

1.5.4. *Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

Regula, ar ko nosaka saskaņotus noteikumus mākslīgā intelekta jomā un groza dažus Savienības leģislatīvos aktus, nosaka jaunu, kopīgu AI sistēmām piemērojamu prasību satvaru, kas ir ievērojami plašāks nekā pašreizējos tiesību aktos noteiktais satvars. Tādēļ ar šo priekšlikumu ir jāizveido jauna valstu un Eiropas līmeņa regulatīvā un koordinācijas funkcija.

Attiecībā uz iespējamu sinerģiju ar citiem atbilstošiem instrumentiem – pieteicējiestāžu lomu valstu līmenī var pildīt tās valstu iestādes, kuras veic līdzīgus uzdevumus saskaņā ar citām ES regulām.

Turklāt, vairojot uzticēšanos AI un tādējādi veicinot ieguldījumus AI risinājumu izstrādē un ieviešanā, šī regula papildina programmu “Digitālā Eiropa”, kurā AI izplatības veicināšana ir viena no piecām prioritātēm.

1.5.5. *Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums*

Darbinieki tiks pārgrupēti. Pārējās izmaksas tiks segtas no programmas “Digitālā Eiropa” finansējuma, ņemot vērā, ka šīs regulas mērķis – uzticama AI nodrošināšana – tiešā veidā sekmē vienu no programmas “Digitālā Eiropa” galvenajiem mērķiem, proti, AI izstrādes un ieviešanas Eiropā paātrināšanu.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ Ierobežots ilgums

- ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.
- ☐ Finansiālā ietekme uz saistību apropriācijām – no GGGG. līdz GGGG. gadam, uz maksājumu apropriācijām – no GGGG. līdz GGGG. gadam.

X Beztermiņa

- Īstenošana ar sākumposmu no **viena/diviem (jāapstiprina)** gada,
- pēc kura turpinās normāla darbība.

1.7. Paredzētie pārvaldības veidi⁶⁵

X Komisijas īstenota tieša pārvaldība:

- ☐ ko veic tās struktūrvienības, ieskaitot personālu Savienības delegācijās;
- ☐ ko veic izpildaģentūras.

☐ Dalīta pārvaldība kopā ar dalībvalstīm

☐ Netieša pārvaldība, kurā budžeta izpildes uzdevumi uzticēti:

- ☐ trešām valstīm vai to norīkotām struktūrām;
- ☐ starptautiskām organizācijām un to aģentūrām (precizēt);
- ☐ EIB un Eiropas Investīciju fondam;
- ☐ Finanšu regulas 70. un 71. pantā minētajām struktūrām;
- ☐ publisko tiesību subjektiem;
- ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tie dod pienācīgas finansiālas garantijas;
- ☐ dalībvalstu privāttiesību subjektiem, kuriem ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuri dod pienācīgas finansiālas garantijas;
- ☐ personām, kurām, ievērojot Līguma par Eiropas Savienību V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.
- *Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā "Piezīmes".*

Piezīmes

--

⁶⁵

Sīkāku informāciju par pārvaldības veidiem un atsaucies uz Finanšu regulu sk. *BudgWeb* vietnē: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt biežumu un nosacījumus.

Regula tiks pārskatīta un izvērtēta piecus gadus pēc tās stāšanās spēkā. Komisija ziņos par izvērtēšanas rezultātiem Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai.

2.2. Pārvaldības un kontroles sistēma

2.2.1. *Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums*

Regula nosaka jaunu politiku attiecībā uz saskaņotiem noteikumiem par mākslīgā intelekta sistēmu sagādāšanu iekšējā tirgū, vienlaikus garantējot drošību un pamattiesību ievērošanu. Šie jaunie noteikumi prasa konsekvences mehānismu šajā regulā noteikto pienākumu pārrobežu piemērošanai – šajā nolūkā jāizveido jauna konsultatīvā grupa, kas koordinē valstu iestāžu darbu.

Lai Komisijas dienesti spētu veikt šos jaunus uzdevumus, tiem jāpiešķir attiecīgi resursi. Aplēsts, ka jaunās regulas izpildei būs nepieciešami 10 FTE (5 FTE AI padomes darba atbalstam un 5 FTE Eiropas Datu aizsardzības uzraudzītājam, kas darbosies kā pieteicējietāde attiecībā uz tām AI sistēmām, ko ievieš Eiropas Savienības struktūras.

2.2.2. *Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu*

Lai nodrošinātu AI padomes locekļiem iespēju veikt informētu analīzi, pamatojoties uz faktiskiem pierādījumiem, paredzēts, ka AI padomi atbalstīs Komisijas administratīvā struktūra un tiks izveidota ekspertu grupa, kas nepieciešamības gadījumā gādās par plašākām zināšanām.

2.2.3. *Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)*

Sanāksmju izdevumiem pietiekamas šķiet standarta kontroles procedūras, jo viena darījuma (piem., ceļa izdevumu atmaksāšana delegātam pēc dalības sanāksmē) vērtība ir zema. Attiecībā uz datubāzes izstrādi – CNECT ĢD ir ieviesta stingra iekšējās kontroles sistēma, kuras ietvaros kontrolē līgumu piešķiršanu centralizētu iepirkumu ceļā.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Pašreizējie krāpšanas novēršanas pasākumi, kas piemērojami Komisijai, attieksies arī uz papildu apropriācijām, kas nepieciešamas saskaņā ar šo regulu.

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Nr.	Dif./nedif. 66	no EBTA valstīm 67	no kandidātvalstīm 68	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
7	20 02 06 Administratīvie izdevumi	Nedif.	NĒ	NĒ	NĒ	NĒ
1	02 04 03 Programma “Digitālā Eiropa”, mākslīgais intelekts	Dif.	JĀ	NĒ	NĒ	NĒ
1	02 01 30 01 Atbalsta izdevumi programmai “Digitālā Eiropa”	Nedif.	JĀ	NĒ	NĒ	NĒ

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriāciju izdevumiem

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas darbības apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

⁶⁶ Dif. – diferencētās apropriācijas, nedif. – nediferencētās apropriācijas.

⁶⁷ EBTA – Eiropas Brīvās tirdzniecības asociācija.

⁶⁸ Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

Daudzgadu finanšu shēmas izdevumu kategorija	1	
---	----------	--

CNECT ĢD				2022	2023	2024	2025	2026	2027 ⁶⁹	KOPĀ	
• Darbības apropriācijas											
Budžeta pozīcija ⁷⁰ 02 04 03	Saistības	(1a)			1,000						1,000
	Maksājumi	(2a)			0,600	0,100	0,100	0,100	0,100		1,000
Budžeta pozīcija	Saistības	(1b)									
	Maksājumi	(2b)									
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķirumiem ⁷¹											
Budžeta pozīcija 02 01 30 01		(3)			0,240	0,240	0,240	0,240	0,240		1,200
KOPĀ CNECT ĢD apropriācijas	Saistības	= 1a + 1b + 3			1,240		0,240	0,240	0,240		2,200
	Maksājumi	= 2a + 2b + 3			0,840	0,340	0,340	0,340	0,340		2,200

⁶⁹ Indikatīva aplēse; summa atkarīga no budžeta pieejamības.

⁷⁰ Saskaņā ar oficiālo budžeta nomenklatūru.

⁷¹ Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

• KOPĀ darbības apropriācijas	Saistības	(4)		1,000						1,000
	Maksājumi	(5)		0,600	0,100	0,100	0,100	0,100		1,000
• KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķirumiem		(6)		0,240	0,240	0,240	0,240	0,240		1,200
KOPĀ daudzgadu finanšu shēmas 1. IZDEVUMU KATEGORIJAS apropriācijas	Saistības	= 4 + 6		1,240	0,240	0,240	0,240	0,240		2,200
	Maksājumi	= 5 + 6		0,840	0,340	0,340	0,340	0,340		2,200

Ja priekšlikums/iniciatīva ietekmē vairāk nekā vienu izdevumu kategoriju, atkārtot iepriekš minēto iedaļu:

• KOPĀ darbības apropriācijas (visas darbības izdevumu kategorijas)	Saistības	(4)								
	Maksājumi	(5)								
• KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķirumiem (visas darbības izdevumu kategorijas)		(6)								
KOPĀ daudzgadu finanšu shēmas 1.–6. IZDEVUMU KATEGORIJAS apropriācijas (atsauces summa)	Saistības	= 4 + 6								
	Maksājumi	= 5 + 6								

Daudzgažu finanšu shēmas izdevumu kategorija	7	“Administratīvie izdevumi”
---	----------	----------------------------

Šī iedaļa jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē [tiesību akta finanšu pārskata pielikumā](#) (iekšējo noteikumu V pielikums), kurš dienestu konsultēšanās vajadzībām tiek augšupielādēts sistēmā *DECIDE*.

miljonos EUR (trīs zīmes aiz komata)

		2023	2024	2025	2026	2027	Pēc 2027 ⁷²	KOPĀ
CNECT ĢD								
• Cilvēkresursi		0,760	0,760	0,760	0,760	0,760	0,760	3,800
• Citi administratīvie izdevumi		0,010	0,010	0,010	0,010	0,010	0,010	0,050
KOPĀ CNECT ĢD	Apropriācijas	0,760	0,760	0,760	0,760	0,760	0,760	3,850
Eiropas Datu aizsardzības uzraudzītājs								
• Cilvēkresursi		0,760	0,760	0,760	0,760	0,760	0,760	3,800
• Citi administratīvie izdevumi								
KOPĀ EDAU	Apropriācijas	0,760	0,760	0,760	0,760	0,760	0,760	3,800
KOPĀ daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)	1,530	1,530	1,530	1,530	1,530	1,530	7,650

miljonos EUR (trīs zīmes aiz komata)

	2022	2023	2024	2025	2026	2027		KOPĀ
--	------	------	------	------	------	------	--	------

⁷²

Visi šajā ailē norādītie skaitļi ir indikatīvi, summas ir atkarīgas no programmu turpināšanas un apropriāciju pieejamības.

KOPĀ daudzgadu finanšu shēmas 1.–7. IZDEVUMU KATEGORIJAS apropriācijas	Saistības		2,770	1,770	1,770	1,770	1,770		9,850
	Maksājumi		2,370	1,870	1,870	1,870	1,870		9,850

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

Saistību apropriācijas miljonos EUR (trīs zīmes aiz komata)

Norādīt mērķus un iznākumus ↓			2022		2023		2024		2025		2026		2027		Pēc 2027 ⁷³		KOPĀ	
	Iznākumi																	
	Veids	Vidējās izmaksas	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izmaksa s	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izmak sas	Kop ējais daud zum s	Kopējā s izmaks as
1. SPECIFISKAIS MĒRĶIS ⁷⁴ ...																		
Datubāze					1	1,000	1		1		1		1		1	0,100	1	1,000
Sanāksmes –					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Komunikācijas pasākumi					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Starpsumma – 1. specifiskais mērķis																		
2. SPECIFISKAIS MĒRĶIS ...																		
– Iznākums																		
Starpsumma – 2. specifiskais mērķis																		
KOPSUMMAS					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

⁷³

Visi šajā ailē norādītie skaitļi ir indikatīvi, summas ir atkarīgas no programmu turpināšanas un apropriāciju pieejamības.

⁷⁴

Norādīti 1.4.2. punktā “Specifiskie mērķi”.

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgas administratīvās apropriācijas
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas administratīvās apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

	2022	2023	2024	2025	2026	2027	Ik gadu pēc 2027 ⁷⁵	KOPĀ
--	------	------	------	------	------	------	-----------------------------------	------

Daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJA								
Cilvēkresursi		1,520	1,520	1,520	1,520	1,520	1,520	7,600
Citi administratīvie izdevumi		0,010	0,010	0,010	0,010	0,010	0,010	0,050
Daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJAS starpsumma		1,530	1,530	1,530	1,530	1,530	1,530	7,650

Ārpus daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJAS ⁷⁶								
Cilvēkresursi								
Pārējie administratīvie izdevumi		0,240	0,240	0,240	0,240	0,240	0,240	1,20
Starpsumma ārpus daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJAS		0,240	0,240	0,240	0,240	0,240	0,240	1,20

KOPĀ		1,770	1,770	1,770	1,770	1,770	1,770	8,850
-------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Vajadzīgās cilvēkresursu un citu administratīvu izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau ir piešķirtas darbības pārvaldībai un/vai ir pārdalītas attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

⁷⁵ Visi šajā ailē norādītie skaitļi ir indikatīvi, summas ir atkarīgas no programmu turpināšanas un apropriāciju pieejamības.

⁷⁶ Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.3.1. Aplēstās cilvēkresursu vajadzības

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

Aplēse izsakāma ar pilnslodzes ekvivalentu

		2023	2024	2025	2026	2027	Pēc 2027 ⁷⁷	
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)								
20 01 02 01 (Galvenā mītne un Komisijas pārstāvniecības)		10	10	10	10	10	10	
20 01 02 03 (Delegācijas)								
01 01 01 01 (Netiešā pētniecība)								
01 01 01 11 (Tiešā pētniecība)								
Citas budžeta pozīcijas (norādīt)								
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu FTE)⁷⁸								
20 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)								
20 02 03 (AC, AL, END, INT un JPD delegācijās)								
XX 01 xx yy zz⁷⁹	– galvenajā mītnē							
	– delegācijās							
01 01 01 02 (AC, END, INT – netiešā pētniecība)								
01 01 01 12 (AC, END, INT – tiešā pētniecība)								
Citas budžeta pozīcijas (norādīt)								
KOPĀ		10	10	10	10	10	10	

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Nepieciešamie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Paredzēts, ka EDAU sniegs pusi no nepieciešamajiem resursiem.

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	Lai sagatavotu kopā 13–16 sanāksmes, izstrādātu ziņojumu projektus, turpinātu politikas darbu, piemēram, saistībā ar augsta riska AI lietojumu saraksta turpmākiem grozījumiem, un uzturētu attiecības ar dalībvalstu iestādēm, būs vajadzīgi četri FTE AD pozīcijās un viens FTE AST pozīcijā. Par AI sistēmām, ko izstrādā ES iestādes, atbild Eiropas Datu aizsardzības uzraudzītājs. Balstoties līdzšinējā pieredzē, var lēst, ka tiesību akta projektā paredzēto EDAU pienākumu izpildei ir nepieciešami 5 FTE AD pozīcijās.
-------------------------------	---

⁷⁷ Visi šajā ailē norādītie skaitļi ir indikatīvi, summas ir atkarīgas no programmu turpināšanas un apropriāciju pieejamības.

⁷⁸ AC – līgumdarbinieki, AL – vietējie darbinieki, END – valstu norīkotie eksperti, INT – aģentūru darbinieki, JPD – jaunākie eksperti delegācijās.

⁷⁹ Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām BA pozīcijām).

Ārštata darbinieki	
--------------------	--

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

Priekšlikuma/iniciatīvas finansēšanai:

- ☒ pilnībā pietiek ar līdzekļu pārvietošanu daudzgadu finanšu shēmas (DFS) attiecīgajā izdevumu kategorijā

Pārplānošana nav nepieciešama.

- ☐ jāizmanto no DFS attiecīgās izdevumu kategorijas nepiešķirtās rezerves un/vai īpašie instrumenti, kas noteikti DFS regulā

Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas un budžeta pozīcijas, atbilstošās summas un instrumentus, kurus ierosināts izmantot.

- ☐ jāpārskata DFS

Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas.

3.2.5. Trešo personu iemaksas

Priekšlikums/iniciatīva:

- ☒ neparedz trešo personu līdzfinansējumu
- ☐ paredz trešo personu sniegtu līdzfinansējumu atbilstoši šādai aplēsei:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

	N gads ⁸⁰	N+1 gads	N+2 gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansētāju struktūru								
KOPĀ līdzfinansētās apropriācijas								

⁸⁰

N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021). Tas pats attiecas uz turpmākajiem gadiem.

3.3. Aplēstā ietekme uz ieņēmumiem

- ☐ Priekšlikums/iniciatīva finansiāli ietekmē:
- ☐ Priekšlikums/iniciatīva finansiāli ietekmē:
 - ☐ citus ieņēmumus
 - ☐ citus ieņēmumus
 - Atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

Budžeta ieņēmumu pozīcija:	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme ⁸¹						
		N gads	N+1 gads	N+2 gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
..... pants								

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgās budžeta izdevumu pozīcijas.

--

Citas piezīmes (piemēram, metode/formula, ko izmanto, lai aprēķinātu ietekmi uz ieņēmumiem, vai jebkura cita informācija).

--

⁸¹

Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.