



2024/1689

12.7.2024.

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2024/1689

(2024. gada 13. jūnijs),

ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts)

(Dokuments attiecas uz EEZ)

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 legislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ⁽¹⁾,

ņemot vērā Eiropas Centrālās bankas atzinumu ⁽²⁾,

ņemot vērā Reģionu komitejas atzinumu ⁽³⁾,

saskaņā ar parasto likumdošanas procedūru ⁽⁴⁾,

tā kā:

- (1) Šīs regulas mērķis ir uzlabot iekšējā tirgus darbību, nosakot vienotu tiesisko regulējumu, jo īpaši mākslīgā intelekta sistēmu (MI sistēmu) izstrādei, laišanai tirgū, nodošanai ekspluatācijā un lietošanai Savienībā saskaņā ar Savienības vērtībām, veicināt uz cilvēku orientēta un uzticama mākslīgā intelekta (MI) ieviešanu, vienlaikus nodrošinot augstu veselības, drošuma, Pamattiesību hartā (Harta) nostiprināto pamattiesību, tostarp demokrātijas un tiesiskuma, un vides aizsardzības līmeni, aizsargāt pret MI sistēmu radītām kaitīgām sekām Savienībā un atbalstīt inovāciju. Šī regula nodrošina uz MI bāzētu preču un pakalpojumu brīvu apriti pāri robežām, tādējādi nepieļaujot, ka dalībvalstis uzliek ierobežojumus MI sistēmu izstrādei, laišanai tirgū un lietošanai, ja vien šī regula tos nepārprotami neatļauj.
- (2) Šī regula būtu jāpiemēro saskaņā ar Hartā nostiprinātajām Savienības vērtībām, veicinot fizisku personu, uzņēmumu, demokrātijas, tiesiskuma un vides aizsardzību, vienlaikus veicinot inovāciju un nodarbinātību un padarot Savienību par līderi uzticama MI ieviešanā.
- (3) MI sistēmas var viegli ieviest daudzos un dažādos ekonomikas sektoros un daudzās sabiedrības daļās, 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 MI ir uzticams un drošs un to izstrādā un izmanto saskaņā ar pienākumiem ievērot pamattiesības. Atšķirīgi valstu noteikumi var izraisīt iekšējā tirgus sadrumstalotību un mazināt juridisko noteiktību operatoriem, kuri izstrādā, importē vai izmanto MI sistēmas. Tāpēc visā Savienībā būtu jānodrošina konsekvents un augsts aizsardzības līmenis, lai panāktu uzticamu MI, turpretim atšķirības, kuras kavē MI sistēmu un saistīto produktu un pakalpojumu brīvu apriti, inovāciju, ieviešanu un izmantošanu iekšējā tirgū, būtu jānovērš,

⁽¹⁾ OV C 517, 22.12.2021., 56. lpp.

⁽²⁾ OV C 115, 11.3.2022., 5. lpp.

⁽³⁾ OV C 97, 28.2.2022., 60. lpp.

⁽⁴⁾ Eiropas Parlamenta 2024. gada 13. marta nostāja (Oficiālajā Vēstnesī vēl nav publicēta) un Padomes 2024. gada 21. maija lēmums.

nosakot vienotus pienākumus operatoriem un garantējot sevišķi svarīgu sabiedrības interešu un personu tiesību vienotu aizsardzību visā iekšējā tirgū, pamatojoties uz Līguma par Eiropas Savienības darbību (LESD) 114. pantu. Ciktāl šī regula satur konkrētus noteikumus par individu aizsardzību attiecībā uz personas datu apstrādi saistībā ar ierobežojumiem MI sistēmu lietošanā biometriskajai tālidentifikācijai tiesībaizsardzības nolūkos, MI sistēmu lietošanā fizisku personu radītā riska novērtējuma veikšanai tiesībaizsardzības nolūkos un biometriskās kategorizācijas MI sistēmu lietošanā tiesībaizsardzības nolūkos, ir piemēroti par šīs regulas pamatu, ciktāl tas attiecas uz minētajiem konkrētajiem noteikumiem, noteikt LESD 16. pantu. Ņemot vērā minētos konkrētos noteikumus un LESD 16. panta izmantošanu, ir lietderīgi apspriesties ar Eiropas Datu aizsardzības kolēģiju.

- (4) MI ir tehnoloģiju kopa, kas strauji attīstās un sniedz dažādus ieguvumus ekonomikai, videi un sabiedrībai visās nozarēs un sociālajās darbībās. Uzlabojot prognozēšanu, optimizējot darbības un resursu piešķiršanu un personalizējot indivīdiem un organizācijām pieejamos digitālos risinājumus, MI lietošana var nodrošināt būtiskas konkurences priekšrocības uzņēmumiem un sekmēt sabiedrībai un videi labvēlīgus rezultātus, piemēram, veselības aprūpē, lauksaimniecībā, pārtikas nekaitīguma nodrošināšanā, izglītībā un mācībās, mediju, sporta un kultūras jomā, infrastruktūras apsaimniekošanā, enerģētikā, transportā un loģistikā, sabiedriskajos pakalpojumos, drošībā, tieslietās, resursefektivitātē un energoefektivitātē, vides monitoringā, biodaudzveidības un ekosistēmu saglabāšanā un atjaunošanā un klimata pārmaiņu mazināšanas un pielāgošanās tām jomā.
- (5) Tajā pašā laikā atkarībā no MI konkrētā lietojuma apstākļiem, izmantošanas un tehnoloģiskās attīstības pakāpes, tas var radīt riskus un nodarīt kaitējumu sabiedrības interesēm un pamattiesībām, kuras aizsargā Savienības tiesību akti. Šāds kaitējums var būt materiāls vai nemateriāls, tostarp fizisks, psiholoģisks, sabiedrisks vai ekonomisks.
- (6) Ņemot vērā MI potenciālo lielo ietekmi uz sabiedrību un nepieciešamību veidot uzticēšanos, ir būtiski, lai MI un tā tiesiskais regulējums tiktu izstrādāts saskaņā ar Savienības vērtībām, kas nostiprinātas Līguma par Eiropas Savienību (LES) 2. pantā, un Līgumos nostiprinātajām pamattiesībām un brīvībām un, ievērojot LESD 6. pantu – Hartā. Priekšnosacījums tam – MI vajadzētu būt uz cilvēku orientētai tehnoloģijai. Tai vajadzētu būt cilvēkiem domātam instrumentam, kura galvenais mērķis ir vairot cilvēku labklājību.
- (7) Lai nodrošinātu konsekventu un augstu sabiedrības interešu aizsardzības līmeni attiecībā uz veselību, drošību un pamattiesībām, būtu jāizveido kopīgi noteikumi augsta riska MI sistēmām. Minētajiem noteikumiem būtu jāsaucina ar Hartu un jābūt nediskriminējošiem un saskaņā ar Savienības starptautiskās tirdzniecības saistībām. Tajos būtu jāņem vērā arī Eiropas deklarācija par digitālajām tiesībām un principiem digitālajai desmitgadei un Mākslīgā intelekta augsta līmeņa ekspertu grupas (AI HLEG) Ētikas vadlīnijas uzticamam mākslīgajam intelektam.
- (8) Tāpēc ir nepieciešams Savienības tiesiskais regulējums, kas nosaka saskaņotus noteikumus MI jomā ar mērķi veicināt MI izstrādi, ieviešanu un izmantošanu iekšējā tirgū, kas vienlaikus nodrošina augstu aizsardzības līmeni tādām sabiedrības interesēm kā veselība un drošība, un pamattiesību aizsardzība, tostarp demokrātija, tiesiskums un vides aizsardzība, kā tas atzīts un aizsargāts Savienības tiesību aktos. Lai sasniegtu minēto mērķi, būtu jānosaka noteikumi par dažu MI sistēmu laišanu tirgū, nodošanu ekspluatācijā un lietošanu, tādējādi nodrošinot netraucētu iekšējā tirgus darbību un ļaujot saistībā ar minētajām sistēmām izmantot preču un pakalpojumu brīvas aprites principa radītos ieguvumus. Minētajiem noteikumiem vajadzētu būt skaidriem un stingriem, lai aizsargātu pamattiesības, atbalstītu jaunus novatoriskus risinājumus, nodrošinātu Eiropas ekosistēmu publiskā un privātā sektora dalībniekiem, kas izstrādā MI sistēmas saskaņā ar Savienības vērtībām, un atraisītu digitālās pārveides potenciālu visos Savienības reģionos. Paredzot minētos noteikumus, kā arī pasākumus inovācijas atbalstam, īpašu uzmanību pievēršot maziem un vidējiem uzņēmumiem (MVU), tostarp jaunuzņēmumiem, šī regula atbalsta Eiropadomes⁽⁵⁾ nosprausto Savienības mērķi – veicināt uz cilvēku orientētu pieeju MI un būt pasaules līderei droša, uzticama un ētiska mākslīgā intelekta attīstīšanā, kā arī tā nodrošina ētikas principu aizsardzību, kā to īpaši lūdzis Eiropas Parlaments⁽⁶⁾.

⁽⁵⁾ Eiropadome (2020), Eiropadomes ārkārtas sanāksme (2020. gada 1. un 2. oktobrī) – secinājumi, EUCO 13/20, 6. lpp.

⁽⁶⁾ Eiropas Parlamenta 2020. gada 20. oktobra rezolūcija ar ieteikumiem Komisijai par mākslīgā intelekta, robotikas un saistīto tehnoloģiju ētisko aspektu satvaru, 2020/2012(INL).

- (9) Augsta riska MI sistēmu laišanai tirdzniecībā, nodošanai ekspluatācijā un lietošanai piemērojamie saskaņotie noteikumi būtu jānosaka saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008⁽⁷⁾, Eiropas Parlamenta un Padomes Lēmumu Nr. 768/2008/EK⁽⁸⁾ un Eiropas Parlamenta un Padomes Regulu (ES) 2019/1020⁽⁹⁾ ("Jaunais tiesiskais regulējums"). Šīs regulas saskaņotie noteikumi būtu jāpiemēro visos sektoros un saskaņā ar Jauno tiesisko regulējumu un tiem nebūtu jāskar spēkā esošie Savienības tiesību akti, jo īpaši tie akti datu aizsardzības, patērētāju aizsardzības, pamattiesību, nodarbinātības, darba ņēmēju aizsardzības un produktu drošības jomā, kurus šī regula papildina. Tādējādi netiek skartas un ir pilnībā piemērojamas visas tiesības un tiesiskās aizsardzības līdzekļi, kas šajos Savienības tiesību aktos paredzēti patērētājiem un citām personām, kuras MI sistēmas var nelabvēlīgi ietekmēt, tostarp tas attiecas uz iespējamo zaudējumu atlīdzināšanu, ievērojot Padomes Direktīvu 85/374/EEK⁽¹⁰⁾. Turklāt saskaņā ar Savienības tiesību aktiem – saistībā ar nodarbinātību un darba ņēmēju aizsardzību šai regulai nevajadzētu ietekmēt Savienības tiesību aktus sociālās politikas jomā un valstu darba tiesības, kas skar nodarbinātības apstākļus, darba apstākļus, tostarp veselību un drošību darbā, un attiecības starp darba devējiem un darba ņēmējiem. Šai regulai arī nevajadzētu ietekmēt dalībvalstīs un Savienības līmenī atzīto pamattiesību īstenošanu, tostarp tiesības vai brīvību streikot vai veikt citu rīcību, kas paredzēta konkrētajās dalībvalstu darba attiecību sistēmās, kā arī tiesības apspriest, noslēgt un izpildīt koplīgumus vai kolektīvi rīkoties saskaņā ar valsts tiesību aktiem. Šai regulai nebūtu jāietekmē Eiropas Parlamenta un Padomes Direktīvā par darba nosacījumu uzlabošanu platformu darbā paredzētie noteikumi, kuru mērķis ir uzlabot darba apstākļus platformu darbā. Papildus tam šīs regulas mērķis ir stiprināt šādu esošo tiesību un tiesiskās aizsardzības līdzekļu efektivitāti, nosakot konkrētas prasības un pienākumus, tostarp attiecībā uz MI sistēmu pārredzamību, tehnisko dokumentāciju un uzskaiti. Turklāt pienākumi, kas šajā regulā paredzēti dažādiem operatoriem, kuri iesaistīti MI vērtības ķēdē, būtu jāpiemēro, neskarot valstu tiesību aktus, atbilstoši Savienības tiesību aktiem, ar ierobežojošu ietekmi uz dažu MI sistēmu lietošanu, ja šādi tiesību akti neietilpst šīs regulas darbības jomā vai tiem ir leģitīmi sabiedrības interešu mērķi, kas nav šīs regulas mērķi. Piemēram, šai regulai nebūtu jāietekmē valsts darba tiesības un tiesību akti par nepilngadīgo, proti, personu, kas jaunākas par 18 gadiem, aizsardzību, ņemot vērā ANO Vispārējo komentāru Nr. 25 (2021) par bērnu tiesībām saistībā ar digitālo vidi, ciktāl tie konkrēti neattiecas uz MI sistēmām un tiem ir citi leģitīmi sabiedrības interešu mērķi.

- (10) Pamattiesības uz personas datu aizsardzību ir aizsargātas jo īpaši ar Eiropas Parlamenta un Padomes Regulām (ES) 2016/679⁽¹¹⁾ un (ES) 2018/1725⁽¹²⁾ un Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680⁽¹³⁾. Papildus Eiropas Parlamenta un Padomes Direktīva 2002/58/EK⁽¹⁴⁾ aizsargā privāto dzīvi un saziņas konfidencialitāti, tostarp, paredzot nosacījumus personas datu un nepersondatu glabāšanai galiekārtās un piekļuvei tiem no galiekārtām. Minētie Savienības tiesību akti nodrošina pamatu ilgtspējīgai un atbildīgai datu apstrādei, arī gadījumos, kad datu kopās ir gan personas dati, gan nepersondati. Šīs regulas mērķis nav ietekmēt to spēkā esošo Savienības tiesību aktu piemērošanu, kas reglamentē personas datu apstrādi, tostarp to neatkarīgo uzraudzības iestāžu uzdevumus un pilnvaras, kas ir kompetentas uzraudzīt atbilstību minētajiem instrumentiem. Tā arī neietekmē MI sistēmu nodrošinātāju un uzturētāju – kā datu pārziņu vai apstrādātāju – pienākumus, kas izriet no Savienības vai valsts tiesību aktiem par personas datu aizsardzību, ciktāl MI sistēmu projektēšana, izstrāde vai lietošana ietver personas datu apstrādi. Ir lietderīgi arī precizēt, ka datu subjektiem joprojām ir visas tiesības un garantijas, kas tiem piešķirtas

(7) Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

(8) 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.).

(9) 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 (OV L 169, 25.6.2019., 1. lpp.).

(10) Padomes Direktīva 85/374/EEK (1985. gada 25. jūlijs) par dalībvalstu normatīvo un administratīvo aktu tuvināšanu attiecībā uz atbilstību par produktiem ar trūkumiem (OV L 210, 7.8.1985., 29. lpp.).

(11) 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.).

(12) 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.).

(13) 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 (Tiesībaizsardzības direktīva) (OV L 119, 4.5.2016., 89. lpp.).

(14) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privātās dzīves aizsardzību un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

ar šādiem Savienības tiesību aktiem, tostarp tiesības, kas saistītas tikai ar automatizētu individuālu lēmumu pieņemšanu, tostarp profilēšanu. Saskaņotiem noteikumiem par MI sistēmu laišanu tirgū, nodošanu ekspluatācijā un lietošanu, kas paredzēti šajā regulā, būtu jāveicina efektīva īstenošana un jādara iespējama datu subjektu tiesību un citu tiesiskās aizsardzības līdzekļu, kas garantēti Savienības tiesību aktos par personas datu un citu pamattiesību aizsardzību, izmantošana.

- (11) Šai regulai nevajadzētu skart noteikumus par starpnieku pakalpojumu sniedzēju atbildību, kā noteikts Eiropas Parlamenta un Padomes Regulā (ES) 2022/2065 ⁽¹⁵⁾.
- (12) “MI sistēmas” jēdziens šajā regulā būtu skaidri jādefinē un cieši jāsaista ar MI jomas starptautisko organizāciju darbu, lai nodrošinātu juridisko noteiktību, veicinātu starptautisko konvergenci un plašu atzīšanu, vienlaikus nodrošinot elastību, kas vajadzīga, lai pielāgotos tehnoloģiju straujajai attīstībai šajā jomā. Turklāt definīcijas pamatā vajadzētu būt MI sistēmu galvenajām iezīmēm, kas to atšķir no vienkāršākām tradicionālajām programmatūras sistēmām vai programmēšanas pieejām, un tam nebūtu jāattiecas uz sistēmām, kuru pamatā ir tikai fizisku personu definēti noteikumi darbību automātiskai izpildei. MI sistēmu galvenā iezīme ir to spēja izdarīt secinājumus. Šī spēja secināt attiecas uz tādu iznākumu iegūšanas procesu kā prognozes, saturs, ieteikumi vai lēmumi, kas var ietekmēt fizisko un virtuālo vidi, un MI sistēmu spēju atvasināt modeļus vai algoritmus, vai abus, no ievaddatiem vai datiem. Paņēmiens, kas ļauj izdarīt secinājumus, veidojot MI sistēmu, ietver mašīnmācīšanās pieejas, kas mācās no datiem, kā sasniegt konkrētus mērķus, un uz loģiku un zināšanām balstītas pieejas, kas no kodētām zināšanām vai risināmā uzdevuma simboliska atspoguļojuma izdara secinājumus. MI sistēmas spēja izsecināt pārsniedz vienkāršu datu apstrādi, nodrošinot mācīšanās, spriešanas un modelēšanas procesus. Termins “mašīnizēta” nozīmē to, ka MI sistēmas darbina mašīnas. Atsauce uz eksplīcītiem vai implīcītiem mērķiem uzsver, ka MI sistēmas var darboties saskaņā ar eksplīcīti noteiktiem mērķiem vai implīcītiem mērķiem. MI sistēmas mērķi konkrētā kontekstā var atšķirties no MI sistēmas paredzētā nolūka. Šajā regulā vide būtu jāsaprot kā konteksts, kurā MI sistēmas darbojas, savukārt MI sistēmas radītie iznākumi atspoguļo dažādas funkcijas, ko veic MI sistēmas, un ietver prognozes, saturu, ieteikumus vai lēmumus. MI sistēmas ir projektētas darbībai dažādās autonomijas pakāpēs, kas nozīmē, ka tās zināmā mērā darbojas neatkarīgi no cilvēka iesaistīšanās un spēj darboties bez cilvēka iejaukšanās. Pielāgošanās spēja, kāda MI sistēmai varētu būt pēc ieviešanas, attiecas uz pašmācīšanās spējām, kas ļauj sistēmai mainīties lietošanas laikā. MI sistēmas var izmantot kā savrupas sistēmas vai kā produkta sastāvdaļu neatkarīgi no tā, vai sistēma ir fiziski integrēta produktā (iegulta) vai nodrošina produktam funkcionalitāti, nebūdama tajā integrēta (neiegulta).
- (13) Šajā regulā minētais jēdziens “uzturētājs” būtu jāinterpretē kā jebkura fiziska vai juridiska persona, tostarp publiskā sektora iestāde, aģentūra vai cita struktūra, kura lieto MI sistēmu, kas ir tās pārziņā, izņemot gadījumus, kad MI sistēmu lieto personiskas neprofesionālas darbības veikšanai. Atkarībā no MI sistēmas veida sistēmas lietošana var ietekmēt personas, kas nav uzturētājs.
- (14) Šajā regulā izmantotais jēdziens “biometriskie dati” būtu jāinterpretē, ņemot vērā biometrisko datu jēdzienu, kā definēts Regulas (ES) 2016/679 4. panta 14. punktā, Regulas (ES) 2018/1725 3. panta 18. punktā un Direktīvas (ES) 2016/680 3. panta 13. punktā. Biometriskie dati var ļaut autentificēt, identificēt vai kategorizēt fiziskas personas un atpazīt fizisku personu emocijas.
- (15) Šajā regulā minētais jēdziens “biometriskā identifikācija” būtu jādefinē kā cilvēka fizisko, fizioloģisko un uzvedības īpašību, piemēram, sejas, acu kustību, ķermeņa formas, balss, prosodijas, gaitas, stājas, sirdsdarbības ātruma, asinsspiediena, smaržas, taustītāsienu raksturlielumu, automātiska atpazīšana, lai konstatētu personas identitāti, salīdzinot šīs personas biometriskos datus ar atsaucē datubāzē glabātiem personu biometriskajiem datiem, neatkarīgi no tā, vai persona ir devusi piekrišanu vai nav. Tas izslēdz MI sistēmas, kuras paredzēts izmantot biometriskajai verifikācijai, kas ietver autentifikāciju, kuras vienīgais nolūks ir apstiprināt, ka konkrēta fiziska persona ir persona, par ko tā uzdodas, un apstiprināt fiziskas personas identitāti vienīgi nolūkā piekļūt pakalpojumam, atbloķēt ierīci vai iegūt drošības piekļuvi telpām.

⁽¹⁵⁾ Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (OV L 277, 27.10.2022., 1. lpp.).

- (16) Šajā regulā minētais jēdziens “biometriskā kategorizācija” būtu jādefinē kā fizisku personu iedalīšana konkrētās kategorijās, pamatojoties uz viņu biometriskajiem datiem. Šādas konkrētas kategorijas var būt saistītas ar tādiem aspektiem kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, personības iezīmes, valoda, reliģija, piederība nacionālajai minoritātei, seksuālā vai politiskā orientācija. Tas neietver biometriskās kategorizācijas sistēmas, kas ir tikai papildfunkcija, kura ir cieši saistīta ar citu komercpakalpojumu, proti, tas nozīmē, ka objektīvu tehnisku iemeslu dēļ šo funkciju nevar izmantot bez galvenā pakalpojuma, un šīs funkcijas vai funkcionalitātes integrēšana nav līdzeklis, lai apietu šīs regulas noteikumu piemērojamību. Piemēram, filtri, kas kategorizē sejas vai ķermeņa iezīmes un ko izmanto tiešsaistes tirdzniecības vietās, varētu būt šāda papildfunkcija, jo tos var izmantot tikai saistībā ar galveno pakalpojumu – produkta pārdošanu –, dodot patērētājam iespēju pašam redzēt produkta attēlojumu un palīdzot viņam pieņemt lēmumu par pirkumu. Par palīgfunkcijām varētu uzskatīt arī filtrus, ko izmanto tiešsaistes sociālo tīklu pakalpojumos, kuri kategorizē sejas vai ķermeņa iezīmes, lai lietotāji varētu pievienot vai pārveidot attēlus vai videomateriālus, jo šādu filtru nevar izmantot bez sociālā tīkla pakalpojumu galvenā pakalpojuma, kas ietver satura kopīgošanu tiešsaistē.
- (17) Šajā regulā minētais jēdziens “biometriskā tālidentifikācija sistēma” būtu jādefinē funkcionāli kā MI sistēma, kas paredzēta fizisku personu identifikācijai bez to aktīvas iesaistīšanas, parasti no attāluma, salīdzinot personas biometriskos datus ar atsaucē datubāzē esošajiem biometriskajiem datiem, neatkarīgi no konkrētās izmantotās tehnoloģijas, procesa vai biometriskā datu veida. Šādas biometriskās tālidentifikācijas sistēmas parasti izmanto, lai uztvertu vairākas personas vai to uzvedību vienlaikus nolūkā būtiski atvieglot fizisku personu identificēšanu bez to aktīvas iesaistīšanās. Tas izslēdz MI sistēmas, kuras paredzēts izmantot biometriskajai verifikācijai, kas ietver autentifikāciju, kuras vienīgais nolūks ir apstiprināt, ka konkrēta fiziska persona ir persona, par ko tā uzdodas, un apstiprināt fiziskas personas identitāti vienīgi nolūkā piekļūt pakalpojumam, atbloķēt ierīci vai iegūt drošības piekļuvi telpām. Minēto izslēgšanu pamato ar to, ka šādām sistēmām, visticamāk, ir neliela ietekme uz fizisku personu pamattiesībām salīdzinājumā ar biometriskās tālidentifikācijas sistēmām, kuras var izmantot liela skaita personu biometriskā datu apstrādei bez to aktīvas iesaistīšanās. Reāllaika sistēmu gadījumā biometriskā 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 MI sistēmu lietošanu reāllaikā, paredzot nelielas aiztures. Reāllaika sistēmās izmanto “tiešraides” vai “gandrīz tiešraides” materiālu, piemēram, videomateriālu, ko ģenerē kamera vai cita ierīce ar līdzīgu funkcionalitāti. 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 ģenerējušas videonovērošanas sistēmas kameras vai privātas ierīces pirms sistēmas lietošanas attiecībā uz attiecīgajām fiziskajām personām.
- (18) Šajā regulā minētais jēdziens “emociju uztveršanas sistēma” būtu jādefinē kā MI sistēma, kuras mērķis ir identificēt vai izsecināt fizisku personu emocijas vai nodomus, pamatojoties uz viņu biometriskajiem datiem. Šis jēdziens attiecas uz tādām emocijām vai nodomiem kā laime, skumjas, dusmas, pārsteigums, nepatika, apmulsums, satraukums, kauns, nicinājums, gandarījums un bauda. Tas neietver fizisku stāvokli, piemēram, sāpes vai nogurumu; tostarp, piemēram, uz sistēmām, ko izmanto, lai noteiktu profesionālu pilotu vai vadītāju noguruma stāvokli negadījumu novēršanas nolūkā. Tas neattiecas arī uz acīmredzamu izpausmi, žestu vai kustību vienkāršu atpazīšanu, ja vien tos neizmanto emociju identificēšanai vai izsecināšanai. Šis izpausmes var būt vienkāršas sejas izteiksmes, piemēram, saraukta pierē vai smaids, vai žesti, piemēram, plaukstu, roku vai galvas kustība, vai personas balss īpašības, piemēram, pacelta balss vai čuksti.
- (19) Šajā regulā jēdziens “publiski piekļūstama vieta” būtu jāsaprot kā atsaucē uz jebkuru fizisku vietu, kas ir piekļūstama nenoteiktam fizisku personu skaitam neatkarīgi no tā, vai minētā vieta ir publiska vai privāta īpašums, un neatkarīgi no tā, kādām aktivitātēm vietu var izmantot, piemēram, tirdzniecībai (piemēram, veikali, restorāni, kafējnīcas); pakalpojumu sniegšanai, piemēram, bankas, profesionālā darbība, viesmīlība; sportam, piemēram, peldbaseini, sporta zāles, stadioni; transportam, piemēram, autoostas, metro un dzelzceļa stacijas, lidostas, transportlīdzekļi; izklaidei, piemēram, kinoteātri, teātri, muzeji, koncertzāles un konferenču zāles; atpūtai vai citādiem mērķiem, piemēram, koplietošanas ceļi un laukumi, parki, meži, rotaļu laukumi. Vieta būtu jāklasificē kā publiski piekļūstama arī tad, ja – neatkarīgi no potenciālās kapacitātes vai drošības ierobežojumiem – piekļuve ir atkarīga no konkrētiem iepriekš noteiktiem nosacījumiem, kuriem var atbilst nenoteikts personu skaits, piemēram, tās ir iegādājušās biļeti vai transporta lietošanas tiesības, veikušas iepriekšēju reģistrāciju vai sasniegušas konkrētu vecumu. Vietu turpretī nevajadzētu uzskatīt par publiski piekļūstamu, ja piekļuve attiecas tikai uz konkrētām un definētām fiziskām personām, kā noteikts ar Savienības vai valsts tiesību aktiem, kas ir tieši saistīti ar sabiedrības drošumu vai sabiedrisko drošību, vai ja tādu gribu skaidri paudusi persona, kurai ir attiecīgās pilnvaras attiecībā uz konkrēto vietu.

Faktiskā piekļuves iespēja pati par sevi (piemēram, atslēgtas durvis, atvērti vārti nožogojuma vietā) nenozīmē, ka vieta ir publiski piekļūstama, ja ir norādes vai apstākļi, kas liecina par pretējo (piemēram, zīmes, kas aizliedz vai ierobežo piekļuvi). Uzņēmumu un rūpnīcu telpas, kā arī biroji un darba vietas, kurām paredzēts piekļūt tikai attiecīgajiem darbiniekiem un pakalpojumu sniedzējiem, nav publiski piekļūstamas vietas. Cietumi vai robežkontroles zonas nebūtu jāuzskata par publiski piekļūstamām vietām. Dažas citas teritorijas var ietvert gan vietas, kas nav publiski piekļūstamas, gan vietas, kas ir publiski piekļūstamas, piemēram, privātas dzīvojamās ēkas gaitenis, kas nepieciešams, lai piekļūtu ārsta kabinetam, vai lidostu. Arī tiešsaistes vietas nav aptvertas, jo tās nav fiziskas vietas. Tomēr tas, vai konkrēta vieta ir publiski piekļūstama, būtu jānosaka katrā gadījumā atsevišķi, ņemot vērā konkrētās individuālās situācijas specifiku.

- (20) Lai gūtu vislielāko labumu no MI sistēmām, vienlaikus aizsargājot pamattiesības, veselību un drošību, un lai nodrošinātu demokrātisku kontroli, MI pratībai būtu jāsniedz sagādātājiem, uzturētājiem un skartajām personām nepieciešamie jēdzieni, lai tie varētu pieņemt uz informāciju balstītus lēmumus par MI sistēmām. Minētie jēdzieni var atšķirties atkarībā no attiecīgā konteksta, un tie var ietvert izpratni par tehnisko elementu pareizu piemērošanu MI sistēmas izstrādes posmā, pasākumiem, kas piemērojami tās izmantošanas laikā, piemērotiem veidiem, kā interpretēt MI sistēmas iznākumu, un – skarto personu gadījumā – zināšanas, kas vajadzīgas, lai izprastu, kā lēmumi, kas pieņemti ar MI palīdzību, tās ietekmēs. Šīs regulas piemērošanas kontekstā MI pratībai būtu jāsniedz visiem attiecīgajiem MI vērtības ķēdes dalībniekiem zināšanas, kas vajadzīgas, lai nodrošinātu pienācīgu atbilstību un tās pareizu izpildi. Turklāt MI pratības pasākumu plaša īstenošana un atbilstošu turpmāko pasākumu ieviešana varētu palīdzēt uzlabot darba apstākļus un galu galā uzturēt uzticama MI konsolidāciju un inovāciju Savienībā. Eiropas Mākslīgā intelekta padomei (MI padomei) būtu jāatbalsta Komisija MI pratības rīku, sabiedrības informētības un izpratnes veicināšanā par ieguvumiem, riskiem, aizsardzības pasākumiem, tiesībām un pienākumiem saistībā ar MI sistēmu lietošanu. Komisijai un dalībvalstīm sadarbībā ar attiecīgajām ieinteresētajām personām būtu jāveicina brīvprātīgu rīcības kodeksu izstrāde, lai uzlabotu MI pratību to personu vidū, kuras nodarbojas ar MI izstrādi, darbību un lietošanu.
- (21) Lai nodrošinātu vienlīdzīgu konkurences apstākļus un indivīdu tiesību un brīvību efektīvu aizsardzību visā Savienībā, šīs regulas noteikumiem būtu jāattiecas uz MI sistēmu nodrošinātājiem nediskriminējošā veidā neatkarīgi no tā, vai tie iedibināti Savienībā vai trešā valstī, un uz Savienībā iedibinātiem MI sistēmu uzturētājiem.
- (22) Ņemot vērā to digitālo raksturu, šai regulai būtu jāattiecas uz dažām MI sistēmām, pat ja tās nav laistas tirgū, nodotas ekspluatācijā vai izmantotas Savienībā. Tā tas ir, piemēram, ja Savienībā iedibināts operators iepērk dažus pakalpojumus no trešās valstīs iedibināta operatora saistībā ar darbību, ko veic MI sistēma, kura uzskatāma par augsta riska sistēmu. Minētajos apstākļos MI sistēma, ko operators izmanto trešā valstī varētu apstrādāt datus, kas likumīgi savākti Savienībā un nosūtīti no tās, un nodot pakalpojumus iepirkušajam Savienības operatoram minētās MI sistēmas iznākumus, kas izriet no minētās datu apstrādes, minēto MI sistēmu nelaižot tirgū, nenododot ekspluatācijā vai neizmantojot Savienībā. Lai novērstu šīs regulas noteikumu apiešanu un nodrošinātu Savienībā esošo fizisko personu efektīvu aizsardzību, šai regulai būtu jāattiecas arī uz MI sistēmu nodrošinātājiem un uzturētājiem, kuri iedibināti trešā valstī, ciktāl minēto sistēmu radītie iznākumi ir paredzēti izmantošanai Savienībā. Tomēr, lai ņemtu vērā esošo kārtību un īpašu nepieciešamību turpmāk sadarboties ar ārvalstu partneriem, ar kuriem notiek informācijas un pierādījumu apmaiņa, šī regula nebūtu jāpiemēro trešo valstu publiskām iestādēm un starptautiskām organizācijām, ja to darbība notiek sadarbības vai starptautisku nolikumu ietvaros, kas noslēgti Eiropas vai valstu līmenī tiesībaizsardzības un tiesu iestāžu sadarbības nolūkā ar Savienību vai dalībvalstīm, ar noteikumu, ka attiecīgā trešā valsts vai starptautiskā organizācija nodrošina pienācīgus aizsardzības pasākumus attiecībā uz personu pamattiesību un pamatbrīvību aizsardzību. Attiecīgā gadījumā tas var attiekties uz tādu vienību darbībām, kurām trešās valstis uzticējušas veikt konkrētus uzdevumus, atbalstot šādu tiesībaizsardzības un tiesu iestāžu sadarbību. Šāda sadarbības sistēma vai nolīgumi ir izstrādāti divpusēji starp dalībvalstīm un trešām valstīm vai starp Eiropas Savienību, Eiropu un citām Savienības aģentūrām un trešām valstīm un starptautiskām organizācijām. Iestādēm, kuru kompetencē ir tiesībaizsardzības un tiesu iestāžu uzraudzība saskaņā ar šo regulu, būtu jānovērtē, vai minētās sadarbības sistēmas vai starptautiskie nolīgumi ietver pienācīgus aizsardzības pasākumus attiecībā uz personu pamattiesību un pamatbrīvību aizsardzību. Saņēmēju valstu iestādes un Savienības iestādes,

struktūras, biroji un aģentūras, kas izmanto šādus iznākumus Savienībā, joprojām ir atbildīgas par to, lai nodrošinātu, ka to izmantošana atbilst Savienības tiesību aktiem. Kad minētie starptautiskie nolīgumi tiek pārskatīti vai turpmāk tiek noslēgti jauni nolīgumi, līgumslēdzējām pusēm būtu jādara viss iespējamais, lai minētos nolīgumus saskaņotu ar šīs regulas prasībām.

- (23) Šī regula būtu jāpieņem arī Savienības iestādēm, struktūrām, birojiem, un aģentūrām, kad tās rīkojas kā MI sistēmas nodrošinātājs vai uzturētājs.
- (24) Ja un ciktāl MI sistēmas tiek laistas tirgū, nodotas ekspluatācijā vai izmantotas ar šādu sistēmu modifikāciju vai bez tās militārām, aizsardzības vai valsts drošības vajadzībām, tās būtu jāizslēdz no šīs regulas piemērošanas jomas neatkarīgi no tā, kāda veida vienība veic minētās darbības, piemēram, neatkarīgi no tā, vai tā ir publiska vai privāta vienība. Attiecībā uz militāriem un aizsardzības mērķiem šāda izslēgšana ir pamatota gan ar LES 4. panta 2. punktu, gan ar dalībvalstu un Savienības kopējās aizsardzības politikas īpatnībām, ko reglamentē Līguma par Eiropas Savienību (LES) V sadaļas 2. nodaļa un uz ko attiecas starptautiskās publiskās tiesības, kas tādējādi ir piemērotāks tiesiskais regulējums MI sistēmu reglamentēšanai saistībā ar letāla spēka izmantošanu un citu MI sistēmu reglamentēšanai militāro un aizsardzības darbību kontekstā. Attiecībā uz valsts drošības mērķiem izslēgšana ir pamatota gan ar to, ka valsts drošība joprojām ir vienīgi dalībvalstu atbildība saskaņā ar LES 4. panta 2. punktu, gan ar valsts drošības darbību specifisko raksturu un operatīvajām vajadzībām, kā arī ar konkrētiem valsts noteikumiem, kas piemērojami minētajām darbībām. Tomēr, ja MI sistēmu, kas izstrādāta, laista tirgū, nodota ekspluatācijā vai tiek izmantota militāriem, aizsardzības vai valsts drošības mērķiem, uz laiku vai pastāvīgi izmanto citiem mērķiem (piemēram, civiliem vai humanitāriem mērķiem, tiesībaizsardzības vai sabiedriskās drošības mērķiem), šāda sistēma ietilptu šīs regulas piemērošanas jomā. Tādā gadījumā vienībai, kas MI sistēmu izmanto nevis militāriem, aizsardzības vai valsts drošības mērķiem, bet citiem mērķiem, būtu jānodrošina MI sistēmas atbilstība šai regulai, ja vien sistēma tai jau neatbilst. MI sistēmas, kas laistas tirgū vai nodotas ekspluatācijā izslēgtiem mērķiem, t. i., militāriem, aizsardzības vai valsts drošības mērķiem, un vienam vai vairākiem mērķiem, kas nav izslēgti, piemēram, civiliem mērķiem vai tiesībaizsardzībai, ietilpst šīs regulas piemērošanas jomā, un minēto sistēmu nodrošinātājiem būtu jānodrošina atbilstība šai regulai. Minētajos gadījumos tam, ka MI sistēma var ietilpt šīs regulas piemērošanas jomā, nebūtu jāietekmē iespēja vienībām, kas veic valsts drošības, aizsardzības un militārās darbības, – neatkarīgi no vienības, kas veic minētās darbības, veida – lietot tās MI sistēmas valsts drošības, militārajiem un aizsardzības mērķiem, kuru lietošana ir izslēgta no šīs regulas piemērošanas jomas. MI sistēmai, kas laista tirgū civiliem vai tiesībaizsardzības mērķiem un ko ar modifikāciju vai bez tās izmanto militāriem, aizsardzības vai valsts drošības mērķiem, nebūtu jāietilpst šīs regulas piemērošanas jomā neatkarīgi no vienības, kas veic minētās darbības, veida.
- (25) Šai regulai būtu jāatbalsta inovācija un būtu jāievēro zinātnes brīvība, un tai nebūtu jākavē pētniecības un izstrādes darbība. Tāpēc no tās darbības jomas ir jāizslēdz MI sistēmas un modeļi, kas konkrēti izstrādāti un nodoti ekspluatācijā vienīgi zinātniskās pētniecības un izstrādes nolūkā. Turklāt ir jānodrošina, ka šī regula citādi neietekmē zinātniskās pētniecības un izstrādes darbību saistībā ar MI sistēmām vai modeļiem pirms to laišanas tirgū vai nodošanas ekspluatācijā. Šīs regulas noteikumi nebūtu jāpieņem arī uz produktiem orientētai pētniecības, testēšanas un izstrādes darbībai saistībā ar MI sistēmām vai modeļiem pirms minēto sistēmu un modeļu nodošanas ekspluatācijā vai laišanas tirgū. Minētā izslēgšana neskar pienākumu ievērot šo regulu, ja MI sistēma, kas ietilpst šīs regulas darbības jomā, tiek laista tirgū vai nodota ekspluatācijā šādas pētniecības un izstrādes darbības rezultātā, un MI "regulatīvo smilškastu" noteikumu un noteikumu par testēšanu reālos apstākļos piemērošanu. Turklāt, neskarot MI sistēmu izslēgšanu, kuras konkrēti izstrādātas un nodotas ekspluatācijā vienīgi zinātniskās pētniecības un izstrādes nolūkā, uz jebkuru citu MI sistēmu, ko var lietot jebkādu pētniecības un izstrādes darbību veikšanai, arī turpmāk būtu jāattiecinā šīs regulas noteikumi. Jebkurā gadījumā ikviena pētniecības un izstrādes darbība būtu jāveic saskaņā ar atzītiem zinātniskās pētniecības ētikas un profesionālajiem standartiem un saskaņā ar piemērojamiem Savienības tiesību aktiem.
- (26) Lai ieviestu samērīgu un iedarbīgu saistošu noteikumu kopumu MI sistēmām, būtu jāizmanto skaidri noteikta, uz risku balstīta pieeja. Minētajai pieejai šādu noteikumu veids un saturs būtu jāpielāgo MI sistēmu potenciāli radīto risku intensitātei un apmēram. Tāpēc ir jāaizliedz daži nepieņemami MI prakses veidi, jānosaka prasības augsta riska MI sistēmām un pienākumi attiecīgajiem operatoriem un jānosaka pārredzamības pienākumi attiecībā uz dažām MI sistēmām.

- (27) Lai gan uz risku balstītā pieeja ir samērīga un efektīva saistošu noteikumu kopuma pamats, ir svarīgi atgādināt 2019. gada Ētikas vadlīnijas uzticamam mākslīgajam intelektam, kuras izstrādājusi Komisijas ieceltā neatkarīgā *AI HLEG*. Minētajās vadlīnijās *AI ALEG* izstrādāja septiņus nesaistošus ar MI saistītus ētikas principus, kuru mērķis ir palīdzēt nodrošināt, lai MI būtu uzticams un ētiski pamatots. Minētie septiņi principi ietver cilvēka darbības spēju un virsvadību; tehnisko robustumu un drošumu; privātumu un datu pārvaldību; pārredzamību; daudzveidību, nediskriminēšanu un taisnīgumu; sociālo un vides labbūtību un pārskatatbildību. Neskarot šīs regulas un citu piemērojamo Savienības tiesību aktu juridiski saistošās prasības, minētās vadlīnijas palīdz projektēt saskaņotu, uzticamu un uz cilvēku orientētu MI saskaņā ar Hartu un vērtībām, uz kuru pamata ir dibināta Savienība. Saskaņā ar *AI HLEG* vadlīnijām cilvēka darbības spēja un virsvadība nozīmē, ka MI sistēmas tiek projektētas un lietotas kā instruments, kas kalpo cilvēkiem, respektē cilvēka cieņu un personisko autonomiju un darbojas tādā veidā, ko cilvēki var pienācīgi kontrolēt un virsvadīt. Tehniskais robustums un drošums nozīmē, ka MI sistēmas tiek projektētas un lietotas tā, lai nodrošinātu robustumu problēmu gadījumā un noturību pret mēģinājumiem mainīt MI sistēmas lietošanu vai veiktspēju tā, ka trešās personas to var lietot nelikumīgi, un lai līdz minimumam samazinātu neparedzētu kaitējumu. Privātums un datu pārvaldība nozīmē, ka MI sistēmas tiek projektētas un lietotas saskaņā ar privātuma un datu aizsardzības noteikumiem, savukārt datus apstrādā atbilstoši augstiem kvalitātes un integritātes standartiem. Pārredzamība nozīmē, ka MI sistēmas tiek projektētas un lietotas tā, lai būtu iespējama pienācīga izsekojamība un izskaidrojamība un vienlaikus lai cilvēki apzinātos, ka sazinās vai ir saskarē ar MI sistēmu, kā arī lai pienācīgi informētu uzturētājus par MI sistēmas spējām un ierobežojumiem un skartās personas – par to tiesībām. Daudzveidība, nediskriminēšana un taisnīgums nozīmē, ka MI sistēmas tiek projektētas un lietotas tā, lai aptvertu dažādus dalībniekus un veicinātu vienlīdzīgu piekļuvi, dzimumu līdztiesību un kultūru daudzveidību un vienlaikus lai netiktu pieļauta diskriminējoša ietekme un netaisnīgi aizspriedumi, ko aizliedz Savienības vai valsts tiesību akti. Sociālā un vides labbūtība nozīmē, ka MI sistēmas tiek projektētas un lietotas ilgtspējīgā un videi nekaitīgā veidā, kā arī tā, lai ieguvēji būtu visi cilvēki un vienlaikus tiktu uzraudzīta un novērtēta ilgtermiņa ietekme uz indivīdu, sabiedrību un demokrātiju. Minēto principu piemērošana, cik vien iespējams, būtu jāintegrē MI modeļu projektēšanā un lietošanā. Jebkurā gadījumā tiem būtu jākalpo par pamatu šajā regulā noteiktajai rīcības kodeksu izstrādei. Visas ieinteresētās personas, tostarp nozare, akadēmiskā vide, pilsoniskā sabiedrība un standartizācijas organizācijas, tiek mudinātas brīvprātīgas paraugprakses un standartu izstrādē pienācīgi ņemt vērā minētos ētikas principus.
- (28) Līdztekus daudziem lietderīgiem MI lietošanas veidiem to var lietot arī ļaunprātīgi, un tā var sniegt nebijušus un spēcīgus rīkus manipulatīvas, ekspluatatīvas un sociālās kontroles prakses īstenošanai. Šāda prakse ir īpaši kaitējoša un ļaunprātīga un būtu jāaizliedz, jo tā ir pretrunā Savienības vērtībām attiecībā uz cilvēka cieņu, brīvību, līdztiesību, demokrātiju un tiesiskumu un pamattiesībām, kas nostiprinātas Hartā, ieskaitot tiesības uz nediskriminēšanu, datu aizsardzību un privātumu un bērna tiesības.
- (29) MI iespējotas manipulatīvas metodes var izmantot, lai pārliecinātu personas iesaistīties nevēlamā rīcībā vai lai maldinātu tās, vedinot pieņemt lēmumus tādā veidā, kas grauj un vājina to autonomiju, lēmumu pieņemšanu un brīvu izvēli. Tādu konkrētu MI sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana, kuru mērķis vai sekas ir cilvēka uzvedības būtiska iespaidošana, kā dēļ var rasties būtisks kaitējums, jo īpaši pietiekami būtiska nelabvēlīga ietekme uz fizisko un psiholoģisko veselību vai finanšu interesēm, ir īpaši bīstama un tāpēc būtu jāaizliedz. Šādas MI sistēmas izmanto zemapziņai adresētus elementus, piemēram, audio, attēlu vai video stimulus, kuras personas kā tādus nespēj uztvert, jo tie darbojas ārpus cilvēka uztveres, vai citus manipulatīvus vai maldinošus paņēmienus, kas grauj vai vājina personas autonomiju, lēmumu pieņemšanu vai brīvu izvēli tā, ka cilvēki neapzinās minētos paņēmienus vai – pat ja tos apzinās – viņi joprojām var tikt maldināti vai nespēj tos kontrolēt vai tiem pretoties. To varētu veicināt, piemēram, mašīnas–smadzeņu saskarnes vai virtuālā realitāte, jo tās ļauj vairāk kontrolēt to, kādi stimuli personām tiek piedāvāti, ciktāl tās var būtiski iespaidot personu uzvedību tā, ka tiek nodarīts būtisks kaitējums. Turklāt MI sistēmas var arī citādi izmantot kādas personas vai konkrētas personu grupas neaizsargātību to vecuma, invaliditātes Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/882 ⁽¹⁶⁾ nozīmē vai konkrētas sociālas vai ekonomiskas situācijas dēļ, kas var padarīt minētās personas neaizsargātākas pret izmantošanu, piemēram, personas, kas dzīvo galējā nabadzībā, etniskās vai reliģiskās minoritātes. Šādas MI sistēmas var laist tirgū, nodot ekspluatācijā vai lietot ar mērķi vai sekām – būtiska personas uzvedības iespaidošana – un tā, ka tiek nodarīts vai var pamatoti uzskatīt, ka var tikt nodarīts būtisks kaitējums minētajai vai kādai citai personai vai personu grupām, tostarp

⁽¹⁶⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2019/882 (2019. gada 17. aprīlis) par produktu un pakalpojumu piekļūstamības prasībām (OV L 151, 7.6.2019., 70. lpp.).

kaitējums, kas var tikt uzkrāts laika gaitā, un tāpēc tās būtu jāaizliedz. Pieņem, ka nodoms ir iespaidot uzvedību, var būt neiespējami, ja iespaidošana izriet no faktoriem, kas nav saistīti ar MI sistēmu un ir ārpus nodrošinātāja vai uzturētāja kontroles, proti, faktoriem, kurus pamatoti nevar paredzēt un kurus tādēļ MI sistēmas nodrošinātājs vai uzturētājs nevar mazināt. Jebkurā gadījumā nodrošinātājam vai uzturētājam nav noteikti jābūt nodomam radīt būtisku kaitējumu, ar noteikumu, ka šāds kaitējums izriet no manipulatīvas vai ekspluatatīvas MI iespējas prakses. Šādas MI prakses aizliegumi papildina Eiropas Parlamenta un Padomes Direktīvā 2005/29/EK⁽¹⁷⁾ ietvertos noteikumus, jo īpaši to, ka negodīga komercprakse, kas rada ekonomisku vai finansiālu kaitējumu patērētājiem, jebkuros apstākļos ir aizliegta neatkarīgi no tā, vai tā tiek īstenota ar MI sistēmām vai citādi. Šajā regulā noteiktajiem manipulatīvas un ekspluatatīvas prakses aizliegumiem nebūtu jāietekmē likumīga prakse medicīniskās aprūpes kontekstā, piemēram, garīgas slimības psiholoģiska ārstēšana vai fiziska rehabilitācija, ja minētā prakse tiek veikta saskaņā ar piemērojamiem tiesību aktiem un medicīniskajiem standartiem, piemēram, ar personu vai to juridisko pārstāvju nepārprotamu piekrišanu. Turklāt vispārpieņemta un lēģitīma komercprakse, piemēram, reklāmas jomā, kas atbilst piemērojamiem tiesību aktiem, pati par sevi nebūtu jāuzskata par kaitīgu manipulatīvu MI iespējotu praksi.

- (30) Būtu jāaizliedz biometriskās kategorizācijas sistēmas, kuru pamatā ir fizisku personu biometriskie dati, piemēram, personas seja vai pirkstu nospiedumi, lai atvedinātu vai izsecinātu personas politiskos uzskatus, dalību arodbiedrībās, reliģisko vai filozofisko pārliecību, rasi, dzimumdzīvi vai seksuālo orientāciju. Minētajam aizliegumam nebūtu jāattiecas uz tādu biometrisku datu kopu likumīgu marķēšanu, filtrēšanu vai kategorizēšanu, kas iegūtas saskaņā ar Savienības vai valsts tiesību aktiem attiecībā uz biometriskajiem datiem, piemēram, attēlu šķirošanu pēc matu krāsas vai acu krāsas, ko var izmantot, piemēram, tiesībsardzības jomā.
- (31) MI sistēmas, ar ko publiski vai privāti dalībnieki nodrošina fizisko personu sociālo novērtēšanu, var radīt diskriminējošus iznākumus un dažu grupu atstumtību. Tās var pārkāpt tiesības uz cieņu un nediskriminēšanu un līdztiesības un tiesiskuma vērtības. Šādas MI sistēmas izvērtē vai klasificē fiziskas personas vai personu grupas noteiktā laikposmā, pamatojoties uz vairākiem datu punktiem, kas saistīti ar to sociālo uzvedību dažādos kontekstos vai zināmām, izsecinātām vai prognozētām personas vai personības īpašībām. Šādu MI 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 ģenerēti vai savākti, vai kaitējošu attieksmi, kas nav pamatota vai samērīga ar personu sociālās uzvedības "smagumu". Tāpēc MI sistēmas, kas ietver šādu nepieņemamu vērtēšanas praksi un rada šādus kaitīgus vai nelabvēlīgus rezultātus, būtu jāaizliedz. Minētajam aizliegumam nebūtu jāietekmē fizisku personu likumīga novērtēšanas prakse, ko īsteno konkrētā nolūkā saskaņā ar Savienības vai valsts tiesību aktiem.
- (32) MI sistēmu lietošana fizisku personu reāllaika biometriskajai tālidentifikācijai publiski pieklūstamās vietās tiesībsardzības nolūkos ir īpaši aizskarošu attiecībā uz konkrēto personu tiesībām un brīvībām, ciktāl tā var ietekmēt lielas sabiedrības daļas privāto dzīvi, izraisīt pastāvīgas novērošanas sajūtu un netieši atturēt no pulcēšanās brīvības un citu pamattiesību īstenošanas. Fizisku personu biometriskajai tālidentifikācijai paredzētu MI sistēmu tehniskās neprecizitātes var novest pie neobjektīviem rezultātiem un radīt diskriminējošas sekas. Šādi iespējami neobjektīvi rezultāti un diskriminējošas sekas ir īpaši saistīti ar vecumu, etnisko piederību, rasi, dzimumu vai invaliditāti. Turklāt tūlītējā ietekme un ierobežotas iespējas veikt turpmākas pārbaudes vai labojumus attiecībā uz šādu reāllaikā darbojošos sistēmu lietošanu rada pastiprinātu risku attiecīgo personu tiesībām un brīvībām tiesībsardzības darbību vai to ietekmes kontekstā.
- (33) Tāpēc minēto sistēmu izmantošana tiesībsardzības nolūkos būtu jāaizliedz, izņemot izsmeljoši uzskaitītas un šauri definētas situācijas, kurās sistēmu izmantošana ir absolūti nepieciešama tādu būtisku sabiedrības interešu īstenošanai, kuru nozīme atsver riskus. Minētās situācijas ietver konkrētu noziegumus cietušo, tostarp pazudušu personu, meklēšanu; konkrētus draudus fizisku personu dzīvībai vai fiziskajai drošībai vai teroristu uzbrukuma draudus; un šīs regulas pielikumā uzskaitīto noziedzīgo nodarījumu izdarītāju vai aizdomās turēto atrašanās vietas noteikšanu vai identifikāciju, ja par minētajiem noziedzīgajiem nodarījumiem attiecīgajā dalībvalstī saskaņā ar minētās dalībvalsts

⁽¹⁷⁾ Eiropas Parlamenta un Padomes Direktīva 2005/29/EK (2005. gada 11. maijs), kas attiecas uz uzņēmēju negodīgu komercpraksi iekšējā tirgū attiecībā pret patērētājiem un ar ko groza Padomes Direktīvu 84/450/EEK un Eiropas Parlamenta un Padomes Direktīvas 97/7/EK, 98/27/EK un 2002/65/EK un Eiropas Parlamenta un Padomes Regulu (EK) Nr. 2006/2004 ("Negodīgas komercprakses direktīva") (OV L 149, 11.6.2005., 22. lpp.).

tiesību aktiem ir paredzēts brīvības atņemšanas sods vai ar brīvības atņemšanu saistīts drošības līdzeklis, kura maksimālais ilgums ir vismaz četri gadi. Šāda robežvērtība brīvības atņemšanas sodam vai ar brīvības atņemšanu saistītam drošības līdzeklim saskaņā ar valsts tiesību aktiem palīdz nodrošināt to, ka noziedzīgajam nodarījumam vajadzētu būt pietiekami smagam, lai potenciāli pamatotu reāllaika biometriskās tālidentifikācijas sistēmas lietošanu. Turklāt noziedzīgo nodarījumu, kas paredzēti šīs regulas pielikumā, pamatā ir 32 Padomes Pamatlēmumā 2002/584/TI⁽¹⁸⁾ uzskaitīti noziedzīgi nodarījumi, ņemot vērā, ka daži no minētajiem nodarījumiem praksē, iespējams, būs būtiskāki nekā citi, proti, paredzams, ka reāllaika biometriskās tālidentifikācijas sistēmas lietošana varētu būt nepieciešama un samērīga ļoti atšķirīgā pakāpē atkarībā no praktiskajām darbībām dažādo uzskaitīto noziedzīgo nodarījumu izdarītāja vai aizdomās turētā atrašanās vietas noteikšanai vai identificēšanai, ņemot vērā iespējamās atšķirības kaitējuma smaguma, iespējamības un apmēra vai iespējamo negatīvo seku ziņā. Nenovēršamus draudus fizisku personu dzīvībai vai fiziskajai drošībai varētu radīt arī Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2557⁽¹⁹⁾ 2. panta 4. punktā definētās kritiskās infrastruktūras nopietni traucējumi, ja šādas kritiskās infrastruktūras traucējumu vai iznīcināšanas rezultātā nenovēršami tiktu apdraudēta personas dzīvība vai fiziskā drošība, tostarp, nopietni kaitējot pamatapgādes nodrošināšanai iedzīvotājiem vai valsts pamatfunkciju īstenošanai. Papildus tam šajā regulā būtu jāsaģlabā tiesībaizsardzības, robežkontroles, imigrācijas vai patvēruma iestādēm iespēja attiecīgās personas klātbūtnē veikt identitātes pārbaudes saskaņā ar nosacījumiem, kas attiecībā uz šādām pārbaudēm paredzēti Savienības un valsts tiesību aktos. Jo īpaši tiesībaizsardzības, robežkontroles, imigrācijas vai patvēruma iestādēm vajadzētu būt iespējai lietot informācijas sistēmas saskaņā ar Savienības vai valsts tiesību aktiem, lai identificētu personas, kuras identitātes pārbaudes laikā vai nu atsakās tikt identificētas, vai nespēj norādīt vai apliecināt savu identitāti, un šajā regulā tām nebūtu jāparedz prasība saņemt iepriekšēju atļauju. Tā varētu būt, piemēram, noziedzīgā nodarījumā iesaistīta persona, kas nevēlas atklāt savu identitāti tiesībaizsardzības iestādēm vai to nespēj negadījuma vai medicīniska stāvokļa dēļ.

- (34) Lai nodrošinātu, ka minētās sistēmas tiek lietotas atbildīgi un samērīgi, ir svarīgi arī noteikt, ka katrā no izsmeljoši uzskaitītajām un šauri definētajām situācijām būtu jāņem vērā daži elementi, it īpaši situācijas raksturs, kurš pamato sistēmas lietošanu, lietošanas ietekme uz visu attiecīgo personu tiesībām un brīvībām, un saistībā ar lietošanu paredzētie aizsardzības pasākumi un nosacījumi. Turklāt reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski piekļūstamās vietās tiesībaizsardzības nolūkos būtu jāizvērs tikai, lai apstiprinātu konkrētas personas identitāti, un tai būtu jānotiek tikai tiktāl, cik tas ir absolūti nepieciešams laikposma, kā arī ģeogrāfiskā un personiskā tvēruma ziņā, jo īpaši, ņemot vērā pierādījumus vai norādes par draudiem, cietušajiem vai nodarījuma izdarītāju. Reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski piekļūstamās vietās būtu jāatļauj vienīgi tad, ja attiecīgā tiesībaizsardzības iestāde ir pabeigusi novērtējumu par ietekmi uz pamattiesībām un, ja vien šajā regulā nav paredzēts citādi, ir reģistrējusi sistēmu datubāzē, kā noteikts šajā regulā. Personu atsaucē datubāzei vajadzētu būt piemērotai katram lietošanas gadījumam katrā no iepriekš minētajām situācijām.

- (35) Katram reāllaika biometriskās tālidentifikācijas sistēmas lietošanas gadījumam publiski piekļūstamās vietās tiesībaizsardzības nolūkos vajadzētu saņemt skaidru un konkrētu atļauju no tiesu iestādes vai dalībvalsts neatkarīgas administratīvās iestādes, kuras lēmums ir saistošs. Šāda atļauja principā būtu jāsaņem pirms MI sistēmas lietošanas personas vai personu identificēšanai. Izņēmumi no minētā noteikuma būtu pieļaujami pienācīgi pamatotās situācijās steidzamu iemeslu dēļ, proti, situācijās, kurās nepieciešamība lietot attiecīgās sistēmas padara atļaujas iegūšanu pirms MI sistēmas lietošanas sākšanas faktiski un objektīvi neiespējamu. Šādās steidzamās situācijās MI sistēmas lietošanai būtu jāaprobežojas ar absolūti nepieciešamo minimumu un uz to būtu jāattiecinā pienācīgi aizsardzības pasākumi un nosacījumi, kā to nosaka valsts tiesību akti un katra atsevišķa steidzamas lietošanas gadījuma kontekstā precīzē pati tiesībaizsardzības iestāde. Turklāt tiesībaizsardzības iestādei šādās situācijās bez liekas kavēšanās un ne vēlāk kā 24 stundu laikā būtu jāpieprasa šāda atļauja, vienlaikus norādot iemeslus, kāpēc tā nav varējusi to pieprasīt agrāk. Ja šāda atļauja tiek noraidīta, būtu nekavējoties jāpārtrauc lietot reāllaika biometriskās identifikācijas sistēmas, kas saistītas ar minēto atļauju, un visi dati, kas saistīti ar šādu lietošanu, būtu jāatmet un jādzēš. Šādi dati ietver ievades

⁽¹⁸⁾ 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.).

⁽¹⁹⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un Padomes Direktīvas 2008/114/EK atcelšanu (OV L 333, 27.12.2022., 164. lpp.).

datu, ko MI sistēma tieši ieguvusi šādas sistēmas lietošanas gaitā, kā arī ar minēto atļauju saistītās lietošanas rezultātus un iznākumus. Tam nebūtu jāiekļauj ievades dati, kas likumīgi iegūti saskaņā ar citiem Savienības vai valsts tiesību aktiem. Jebkurā gadījumā nevienš lēmums, kas personai rada nelabvēlīgas tiesiskas sekas, nebūtu jāpieņem, balstoties vienīgi uz biometriskās tālidentifikācijas sistēmas iznākumu.

- (36) Lai attiecīgā tirgus uzraudzības iestāde un valstu datu aizsardzības iestāde varētu pildīt savus uzdevumus saskaņā ar šajā regulā un valsts noteikumos paredzētajām prasībām, tās būtu jāinformē par katru reāllaika biometriskās identifikācijas sistēmas lietošanas gadījumu. Valstu tirgus uzraudzības iestādēm un valsts datu aizsardzības iestādēm, kuras ir informētas, būtu jāiesniedz Komisijai gada ziņojums par reāllaika biometriskās identifikācijas sistēmu lietošanu.
- (37) Turklāt šīs regulas izveidotajā izsmelšajā regulējumā ir lietderīgi noteikt, ka minētajai lietošanai dalībvalsts teritorijā saskaņā ar šo regulu vajadzētu būt iespējai tikai, ja un ciktāl attiecīgā dalībvalsts ir nolēmusi savos sīki izstrādātajos valsts tiesību aktu noteikumos skaidri paredzēt iespēju atļaut šādu lietošanu. Tādējādi šī regula dalībvalstīm ļauj neparedzēt šādu iespēju nemaz vai paredzēt to tikai attiecībā uz dažiem mērķiem, ar kuriem var pamatot šajā regulā noteikto atļauto lietošanu. Šādi valsts noteikumi būtu jāpaziņo Komisijai 30 dienu laikā pēc to pieņemšanas.
- (38) MI sistēmu lietošana fizisku personu reāllaika biometriskajai tālidentifikācijai publiski pieklūstamās vietās tiesībaizsardzības nolūkos neizbēgami ietver biometrisku datu apstrādi. Šīs regulas noteikumi, kas aizliedz (ar dažiem izņēmumiem) šādu lietošanu un pamatojas uz LESD 16. pantu, būtu jāpieņem kā *lex specialis* attiecībā uz Direktīvas (ES) 2016/680 10. panta noteikumiem par biometrisku datu apstrādi, tādējādi izsmelši regulējot šādu lietošanu un ar to saistīto biometrisku datu apstrādi. Tāpēc šādai lietošanai un datu apstrādei vajadzētu būt iespējai tikai, ciktāl tā ir saderīga ar šajā regulā noteikto satvaru, bez darbības jomas ārpus minētā satvara, kurā kompetentās iestādes, rīkojoties tiesībaizsardzības nolūkā, varētu lietot šādas sistēmas un apstrādāt šādus datus saistībā ar tām, pamatojoties uz Direktīvas (ES) 2016/680 10. pantā uzskaitītajiem iemesliem. Minētajā kontekstā šī regula nav paredzēta juridiskā pamata nodrošināšanai Direktīvas (ES) 2016/680 8. pantā noteiktajai personas datu apstrādei. Tomēr reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski pieklūstamās vietās nolūkos, kas nav tiesībaizsardzība, tostarp no kompetento iestāžu puses, nebūtu jāiekļauj šajā regulā noteiktajā konkrētajā regulējumā attiecībā uz šādu lietošanu tiesībaizsardzības nolūkos. Tāpēc šajā regulā noteiktā prasība saņemt atļauju un piemērojamie sīki izstrādātie valsts tiesību aktu noteikumi, kas minēto atļauju var ieviest, nebūtu jāattiecinā uz šādu lietošanu nolūkos, kas nav tiesībaizsardzība.
- (39) Biometrisku datu un citu personas datu apstrādei saistībā ar MI sistēmu lietošanu biometriskajai identifikācijai, kas nav saistīta ar reāllaika biometriskās tālidentifikācijas sistēmu lietošanu publiski pieklūstamās vietās tiesībaizsardzības nolūkos, kā to reglamentē šī regula, arī turpmāk būtu jāatbilst visām prasībām, kas izriet no Direktīvas (ES) 2016/680 10. panta. Nolūkos, kas nav tiesībaizsardzība, Regulas (ES) 2016/679 9. panta 1. punkts un Regulas (ES) 2018/1725 10. panta 1. punkts aizliedz biometrisku datu apstrādi, ievērojot minētajos pantos paredzētos ierobežotos izņēmumus. Piemērojot Regulas (ES) 2016/679 9. panta 1. punktu, uz biometriskās tālidentifikācijas lietošanu nolūkos, kas nav tiesībaizsardzība, jau attiecas valsts datu aizsardzības iestāžu lēmumi par aizliegšanu.
- (40) Saskaņā ar 6.a pantu LES un LESD pievienotajā Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu Īrijai nav saistoši noteikumi, kas paredzēti šīs regulas 5. panta 1. punkta pirmās daļas g) apakšpunktā, ciktāl to piemēro biometriskās kategorizācijas sistēmu lietošanai saistībā ar darbībām policijas un tiesu iestāžu sadarbībā krimināllietās, 5. panta 1. punkta pirmās daļas d) apakšpunktā, ciktāl tos piemēro MI sistēmu lietošanai, uz ko minētais noteikums attiecas, 5. panta 1. punkta pirmās daļas h) apakšpunktā, 5. panta 2. līdz 6. punktā un 26. panta 10. punktā un kas pieņemti, pamatojoties uz Līguma par Eiropas Savienības darbību 16. pantu, un skar personas datu apstrādi dalībvalstīs, veicot darbības, uz ko attiecas LESD Trešās daļas V sadaļas 4. vai 5. nodaļas darbības joma, ja Īrijai nav saistoši noteikumi, ar ko reglamentē veidus tiesu iestāžu sadarbībai krimināllietās vai policijas sadarbības veidus, sakarā ar kuriem ir jāievēro noteikumi, kas paredzēti, pamatojoties uz LESD 16. pantu.
- (41) Saskaņā ar 2. un 2.a pantu LES un LESD pievienotajā Protokolā Nr. 22 par Dānijas nostāju Dānijai nav saistoši un nav jāpieņem noteikumi, kas paredzēti šīs regulas 5. panta 1. punkta pirmās daļas g) apakšpunktā, ciktāl to piemēro biometriskās kategorizācijas sistēmu lietošanai saistībā ar darbībām policijas un tiesu iestāžu sadarbībā krimināllietās, 5. panta 1. punkta pirmās daļas d) apakšpunktā, ciktāl tos piemēro MI sistēmu lietošanai, uz ko

minētais noteikums attiecas, 5. panta 1. punkta pirmās daļas h) apakšpunktā, 2. līdz 6. punktā un 26. panta 10. punktā un kas pieņemti, pamatojoties uz Līguma par Eiropas Savienības darbību 16. pantu, un skar personas datu apstrādi dalībvalstīs, veicot darbības, uz ko attiecas LESD Trešās daļas V sadaļas 4. vai 5. nodaļas darbības joma.

- (42) Saskaņā ar nevainīguma prezumpciju fiziskas personas Savienībā vienmēr būtu jāvērtē pēc to faktiskās uzvedības. Fiziskas personas nekad nevajadzētu vērtēt pēc MI prognozētas uzvedības, pamatojoties tikai uz to profilēšanu, personiskajām īpašībām vai rakstura iezīmēm, piemēram, valstspiederību, dzimšanas vietu, dzīvesvietu, bērnu skaitu, parāda līmeni vai automobiļa veidu, ja, balstoties uz objektīviem pārbaudāmiem faktiem, nav pamatotu aizdomu par personas iesaistīšanos noziedzīgā darbībā un ja nav cilvēka veikta novērtējuma par to. Tāpēc būtu jāaizliedz riska novērtējumi, ko veic attiecībā uz fiziskām personām, lai novērtētu to nodarījuma izdarīšanas risku vai lai prognozētu faktiska vai iespējama noziedzīga nodarījuma notikšanu, pamatojoties tikai uz personu profilēšanu vai novērtējot to personiskās īpašības un rakstura iezīmes. Jebkurā gadījumā minētais aizliegums neattiecas uz riska analīzi, kas nav balstīta uz personu profilēšanu vai to personiskajām īpašībām un rakstura iezīmēm, piemēram, MI sistēmām, kas izmanto riska analīzi, lai novērtētu uzņēmumu īstenotas finanšu krāpšanas iespējamību, pamatojoties uz aizdomīgiem darījumiem, vai riska analīzes rīkus, lai prognozētu iespējamību, ka muitas dienesti, piemēram, pamatojoties uz zināmiem tirdzniecības maršrutiem, nosaka narkotiku vai nelikumīgu preču atrašanās vietu.
- (43) Tādu MI sistēmu laišana tirgū, nodošana ekspluatācijā minētajam konkrētajam mērķim vai lietošana, kuras izveido vai paplašina sejas atpazīšanas datubāzes, nemērķorientēti rasmojot sejas attēlus no interneta vai videonovērošanas sistēmu video, būtu jāaizliedz, jo minētā prakse pastiprina masveida novērošanas sajūtu un var izraisīt rupjus pamattiesību, tostarp tiesību uz privātumu, pārkāpumus.
- (44) Ir nopietnas bažas par tādu MI sistēmu zinātnisko pamatojumu, kuru mērķis ir identificēt vai izsecināt emocijas, jo īpaši tāpēc, ka emociju izpausmes dažādās kultūrās un situācijās un pat vienas personas gadījumā ievērojami atšķiras. Šādu sistēmu galvenie trūkumi ir ierobežotā uzticamība, specifiskuma trūkums un ierobežotā vispārināmība. Tāpēc MI sistēmas, kas identificē vai izsecina fizisku personu emocijas vai nodomus, pamatojoties uz to biometriskajiem datiem, var radīt diskriminējošus rezultātus un var aizskart attiecīgo personu tiesības un brīvības. Ņemot vērā nevienlīdzīgo spēku samēru darba vai izglītības jomā un to, ka šīs sistēmas pēc būtības ir aizskarošas, šādas sistēmas varētu izraisīt kaitējošu vai nelabvēlīgu attieksmi pret konkrētām fiziskām personām vai to grupām. Tāpēc būtu jāaizliedz tādu MI sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana, kuras paredzēts lietot, lai noteiktu personu emocionālo stāvokli situācijās, kas saistītas ar darba vietu un izglītību. Minētajam aizliegumam nebūtu jāattiecas uz MI sistēmām, kas laistas tirgū tikai un vienīgi medicīnisku vai drošības iemeslu dēļ, piemēram, uz sistēmām, kas paredzētas lietošanai terapeitiskos nolūkos.
- (45) Šai regulai nevajadzētu ietekmēt praksi, kas ir aizliegta ar Savienības tiesību aktiem, tostarp tiesību aktiem datu aizsardzības, diskriminācijas novēršanas, patērētāju tiesību aizsardzības un konkurences jomā.
- (46) Augsta riska MI sistēmas būtu jālaiž Savienības tirgū, jānodod ekspluatācijā vai jālieto tikai tad, ja tās atbilst konkrētām obligātām prasībām. Minētajām prasībām būtu jānodrošina, ka augsta riska MI sistēmas, kuras pieejamas Savienībā vai kuru iznākumus citādā veidā izmanto Savienībā, nerada nepieņemamus riskus svarīgām Savienības sabiedrības interesēm, kas ir atzītas un aizsargātas Savienības tiesību aktos. Pamatojoties uz jauno tiesisko regulējumu, kas precizēts Komisijas paziņojumā “Zilā rokasgrāmata” par ES produktu noteikumu īstenošanu 2022. gadā⁽²⁰⁾, vispārējais noteikums ir tāds, ka vairāk nekā vienu Savienības saskaņošanas tiesību aktu, piemēram, Eiropas Parlamenta un Padomes Regulu (ES) 2017/745⁽²¹⁾ un (ES) 2017/746⁽²²⁾ vai Eiropas Parlamenta un Padomes Direktīvu 2006/42/EK⁽²³⁾, var piemērot vienam produktam, jo darīt pieejamu vai nodot ekspluatācijā to var tikai tad, ja produkts atbilst visiem piemērojamiem Savienības saskaņošanas tiesību aktiem. Lai nodrošinātu

⁽²⁰⁾ OV C 247, 29.6.2022., 1. lpp.

⁽²¹⁾ 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.).

⁽²²⁾ 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.).

⁽²³⁾ Eiropas Parlamenta un Padomes Direktīva 2006/42/EK (2006. gada 17. maijs) par mašīnām, un ar kuru groza Direktīvu 95/16/EK (OV L 157, 9.6.2006., 24. lpp.).

konsekvenci un izvairītos no nevajadzīga administratīvā sloga vai izmaksām, tāda produkta nodrošinātājiem, kas ietver vienu vai vairākas augsta riska MI sistēmas, uz kurām attiecas šīs regulas vai šīs regulas pielikumā uzskaitīto Savienības saskaņošanas tiesību aktu prasības, vajadzētu būt elastīgiem attiecībā uz operatīviem lēmumiem par to, kā optimāli nodrošināt produkta, kas ietver vienu vai vairākas MI sistēmas, atbilstību visām piemērojamām Savienības saskaņošanas tiesību aktu prasībām. Kā augsta riska sistēmas būtu jāidentificē tikai tās MI sistēmas, kurām ir ievērojama kaitējoša ietekme uz personu veselību, drošību un pamattiesībām Savienībā, un šādam ierobežojumam būtu jāsamazina jebkādu iespējamu starptautiskās tirdzniecības ierobežojumu rašanos.

- (47) MI sistēmas varētu negatīvi ietekmēt personu veselību un drošību, jo īpaši, ja šādas sistēmas darbojas kā produktu drošības 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 MI 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 veselības aprūpes nozarē, kur runa ir par veselību un dzīvību, arvien sarežģītākām diagnostikas sistēmām un cilvēka lēmumus atbalstošām sistēmām vajadzētu būt uzticamām un pareizām.
- (48) Tas, cik liela ir MI sistēmas izraisītā kaitējošā ietekme uz Hartā aizsargātajām pamattiesībām, ir īpaši svarīgi, klasificējot MI sistēmu kā augsta riska. Minētās tiesības ietver tiesības uz cilvēka cieņu, privātās un ģimenes dzīves neaizskaramību, personas datu aizsardzību, vārda un informācijas brīvību, pulcēšanās un biedrošanās brīvību, diskriminācijas aizliegumu, tiesības uz izglītību, patērētāju tiesību aizsardzību, darba ņēmēju tiesības, personu ar invaliditāti tiesības, dzimumu līdztiesību, intelektuālā īpašuma tiesības, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, tiesības uz aizstāvību un nevainīguma prezumpciju, kā arī tiesības uz labu pārvaldību. Papildus minētajām tiesībām ir svarīgi uzsvērt, ka bērniem ir konkrētas tiesības, kas noteiktas Hartas 24. pantā un ANO Konvencijā par bērna tiesībām, kuras pilnveidotas minētās ANO konvencijas Vispārējā komentārā Nr. 25 par digitālo vidi; abos dokumentos ir noteikts, ka ir jāņem vērā bērnu neaizsargātība un jānodrošina viņu labklājībai nepieciešamā aizsardzība un gādība. Novērtējot kaitējuma smagumu, ko MI sistēma var nodarīt, arī attiecībā uz personu veselību un drošību, būtu jāņem vērā arī pamattiesības uz augstu vides aizsardzības līmeni, kuras ir nostiprinātas Hartā un īstenotas Savienības politikā.
- (49) Attiecībā uz augsta riska MI sistēmām, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas, uz ko attiecas Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008⁽²⁴⁾, Eiropas Parlamenta un Padomes Regula (ES) Nr. 167/2013⁽²⁵⁾, Eiropas Parlamenta un Padomes Regula (ES) Nr. 168/2013⁽²⁶⁾, Eiropas Parlamenta un Padomes Direktīva 2014/90/ES⁽²⁷⁾, Eiropas Parlamenta un Padomes Direktīva (ES) 2016/797⁽²⁸⁾, Eiropas Parlamenta un Padomes Regula (ES) 2018/858⁽²⁹⁾, Eiropas Parlamenta un Padomes Regula (ES) 2018/1139⁽³⁰⁾ un Eiropas Parlamenta un Padomes Regula (ES) 2019/2144⁽³¹⁾, ir lietderīgi grozīt minētos aktus,
- (²⁴) 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.).
- (²⁵) 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.).
- (²⁶) 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.).
- (²⁷) 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.).
- (²⁸) 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.).
- (²⁹) 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.).
- (³⁰) 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.).
- (³¹) 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, (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.).

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

- (50) Attiecībā uz augsta riska MI sistēmām, kuras ir produktu drošības sastāvdaļas vai pašas ir produkti, uz ko attiecas daži Savienības saskaņošanas tiesību akti, kas uzskaitīti šīs regulas pielikumā, ir lietderīgi tās klasificēt kā augsta riska sistēmas, kā paredzēts šajā regulā, ja attiecīgajam produktam piemēro atbilstības novērtēšanas struktūras, kas ir trešā persona, veiktu atbilstības novērtēšanas procedūru, ievērojot attiecīgos Savienības saskaņošanas tiesību aktus. 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, gāzveida kurināmā iekārtas, medicīniskās ierīces, *in vitro* diagnostikas medicīniskās ierīces, pašgājēji un aviācija.
- (51) Tam, ka MI sistēmu klasificē kā augsta riska sistēmu, ievērojot šo regulu, nebūtu obligāti jānozīmē, ka produktu, kura drošības sastāvdaļa ir attiecīgā MI sistēma, vai pašu MI sistēmu kā produktu uzskata par augsta riska saskaņā ar kritērijiem, kas noteikti attiecīgajos Savienības saskaņošanas tiesību aktos, kurus piemēro minētajam produktam. Tas jo īpaši attiecas uz Regulām (ES) 2017/745 un (ES) 2017/746, kurās paredzēta trešās personas veikta atbilstības novērtēšana vidēja riska un augsta riska produktiem.
- (52) Savrupas MI sistēmas, proti, augsta riska MI 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 tā iespējamību, un ja tās lieto vairākās iepriekš konkrēti noteiktās jomās, kā precizēts šajā regulā. Minēto sistēmu identifikācija pamatojas uz tādu pašu metodiku un kritērijiem, kādi paredzēti arī jebkādiem turpmākiem augsta riska MI sistēmu saraksta grozījumiem, kurus Komisija būtu jāpildinvaro pieņemt ar deleģētajiem aktiem, lai ņemtu vērā tehnoloģiju attīstības straujo tempu, kā arī iespējamās izmaiņas MI sistēmu lietošanā.
- (53) Ir arī svarīgi precizēt, ka var būt konkrēti gadījumi, kad MI sistēmas, kas attiecas uz iepriekš noteiktām jomām, kuras norādītas šajā regulā, nerada būtisku kaitējuma risku minētajās jomās aizsargātajām juridiskajām interesēm, jo būtiski neietekmē lēmumu pieņemšanu vai būtiski nekaitē minētajām interesēm. Šīs regulas nolūkos ar MI sistēmu, kas būtiski neietekmē lēmumu pieņemšanas iznākumu, būtu jāsaprot MI sistēma, kas neietekmē cilvēka vai automatizētas lēmumu pieņemšanas būtību un līdz ar to arī tās iznākumu. MI sistēma, kas būtiski neietekmē lēmumu pieņemšanas iznākumu, varētu ietvert situācijas, kurās ir izpildīts viens vai vairāki turpmāk minētie nosacījumi. Pirmajam šādam nosacījumam vajadzētu būt, ka MI sistēma ir paredzēta šaura procedūras uzdevuma veikšanai, piemēram, MI sistēma, kas nestrukturētus datus pārveido strukturētos datos, MI sistēma, kas ienākošos dokumentus klasificē kategorijās, vai MI sistēma, ko lieto, lai plašajā pieteikumu klāstā atklātu dublikātus. Minētie uzdevumi ir tik šauri un ierobežoti, ka tie rada tikai ierobežotus riskus, kurus nepaaugstina MI sistēmu lietošana kādā no kontekstiem, kas šīs regulas pielikumā ir uzskaitīti kā augsta riska lietošanas gadījumi. Otrajam nosacījumam vajadzētu būt tādam, ka MI sistēmas uzdevums ir uzlabot iepriekš pabeigtas cilvēka darbības rezultātu,

kam var būt nozīme šīs regulas pielikumā uzskaitīto augsta riska lietošanas gadījumu uzskaitījuma nolūkos. Ņemot vērā minētās iezīmes, MI sistēma nodrošina tikai papildu slāni cilvēka darbībai ar attiecīgi zemāku risku. Minētais nosacījums attiektos, piemēram, uz MI sistēmām, kuru mērķis ir uzlabot valodu, kas lietota iepriekš sagatavotos dokumentos, piemēram, piešķirt profesionālu toni, izmantot akadēmisku valodas stilu vai tekstu pielāgot vēstījumiem, kas saistīti ar kādu noteiktu zīmolu. Trešajam nosacījumam vajadzētu būt tādam, ka MI sistēma ir paredzēta tam, lai atklātu lēmumu pieņemšanas modeļus vai novirzes no iepriekšējiem lēmumu pieņemšanas modeļiem. Risks būtu mazāks, jo MI sistēmas lietošana notiek pēc iepriekš pabeigta novērtējuma, ko veicis cilvēks, un tā nav paredzēta, lai šo novērtējumu aizstātu vai ietekmētu, bez pienācīgas cilvēka veiktas pārskatīšanas. Šādas MI sistēmas ietver, piemēram, sistēmas, ko, ņemot vērā konkrētu skolotāja klasifikācijas modeli, var izmantot, lai *ex post* pārbaudītu, vai skolotājs varētu būt novirzījies no attiecīgā klasifikācijas modeļa, un lai tādējādi norādītu uz iespējamām neatbilstībām vai anomālijām. Ceturtajam nosacījumam vajadzētu būt tādam, ka MI sistēma ir paredzēta tikai sagatavošanās uzdevuma veikšanai saistībā ar novērtējumu, kam ir nozīme šīs regulas pielikumā uzskaitīto MI sistēmu nolūkos, tādējādi panākot, ka sistēmas iznākuma iespējamā ietekme rada ļoti mazu risku novērtējumam, kas pēc tam tiek veikts. Minētais nosacījums cita starpā attiecas uz viediem lietu apstrādes risinājumiem, kas ietver dažādas funkcijas, sākot ar indeksēšanu, meklēšanu, teksta un runas apstrādi vai datu sasaisti ar citiem datu avotiem, vai MI sistēmas, ko lieto sākotnējo dokumentu tulkošanai. Jebkurā gadījumā būtu jāuzskata, ka MI sistēmas, kas tiek lietotas augsta riska gadījumos, kas uzskaitīti šīs regulas pielikumā, rada būtiskus kaitējuma riskus veselībai, drošībai vai pamattiesībām, ja MI sistēma ietver profilēšanu Regulas (ES) 2016/679 4. panta 4. punkta vai Direktīvas (ES) 2016/680 3. panta 4. punkta, vai Regulas (ES) 2018/1725 3. panta 5. punkta nozīmē. Lai nodrošinātu izsekojamību un pārredzamību, nodrošinātājam, kurš uzskata, ka MI sistēma, pamatojoties uz iepriekš minētajiem nosacījumiem, nav augsta riska sistēma, būtu jā sagatavo novērtējuma dokumentācija pirms minētās sistēmas laišanas tirgū vai nodošanas ekspluatācijā un pēc pieprasījuma šī dokumentācija būtu jāiesniedz valsts kompetentajām iestādēm. Šādam nodrošinātājam vajadzētu būt pienākamam reģistrēt MI sistēmu ES datubāzē, kas izveidota saskaņā ar šo regulu. Lai sniegtu turpmākus norādījumus par to nosacījumu praktisko īstenošanu, saskaņā ar kuriem MI sistēmas, kas uzskaitītas šīs regulas pielikumā, izpēruma kārtā nav augsta riska sistēmas, Komisijai pēc apspriešanās ar padomi būtu jāsniedz pamatnostādnes, kurās precizē minēto praktisko īstenošanu, pievienojot visaptverošu sarakstu ar praktiskiem piemēriem, kas parāda augsta riska MI sistēmu lietošanas gadījumus un tādus gadījumus, kas nav.

- (54) Tā kā biometriskie dati ir īpaša personas datu kategorija, ir lietderīgi vairākus biometrisku sistēmu kritiskās lietošanas gadījumus klasificēt kā augsta riska gadījumus, ciktāl šo sistēmu lietošana ir atļauta saskaņā ar attiecīgajiem Savienības un valsts tiesību aktiem. Fizisku personu biometriskajai tālidentifikācijai paredzētu MI sistēmu tehniskās neprecizitātes var novest pie neobjektīviem rezultātiem un radīt diskriminējošas sekas. Šādu neobjektīvu rezultātu risks un diskriminējošas sekas ir īpaši saistītas ar vecumu, etnisko piederību, rasi, dzimumu vai invaliditāti. Tāpēc, ņemot vērā biometriskās tālidentifikācijas sistēmu radītos riskus, tās būtu jāklasificē kā augsta riska sistēmas. Šāda klasifikācija izslēdz MI sistēmas, kuras paredzēts lietot biometriskajai verifikācijai, tostarp autentifikācijai, kuras vienīgais nolūks ir apstiprināt, ka konkrēta fiziska persona ir persona, par ko tā uzdodas, un apstiprināt fiziskas personas identitāti vienīgi nolūkā piekļūt pakalpojumam, atbloķēt ierīci vai iegūt drošības piekļuvi telpām. Turklāt MI sistēmas, ko paredzēts lietot biometriskajai kategorizācijai pēc sensitīviem atribūtiem vai raksturlielumiem, ko aizsargā atbilstīgi Regulas (ES) 2016/679 9. panta 1. punktam, pamatojoties uz biometriskajiem datiem, ciktāl tās nav aizliegtas šajā regulā, un emociju atpazīšanas sistēmas, kas nav aizliegtas šajā regulā, būtu jāklasificē kā augsta riska sistēmas. Biometriskās sistēmas, ko paredzēts lietot tikai kibernetikas un personas datu aizsardzības pasākumu nodrošināšanai, nebūtu jāuzskata par augsta riska MI sistēmām.

- (55) Attiecībā uz kritiskās infrastruktūras pārvaldību un darbību ir lietderīgi kā augsta riska sistēmas klasificēt tās MI sistēmas, kuras paredzēts lietot kā drošības sastāvdaļas Direktīvas (ES) 2022/2557 pielikuma 8. punktā uzskaitītās kritiskās digitālās infrastruktūras pārvaldībā un darbībā, ceļu satiksmē, 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. Kritiskās infrastruktūras, tostarp kritiskās digitālās infrastruktūras, drošības sastāvdaļas ir sistēmas, ko lieto, lai tieši aizsargātu kritiskās infrastruktūras fizisko integritāti vai cilvēku veselību un drošību un mantas drošību, bet kas nav

nepieciešamas sistēmas darbībai. Šādu sastāvdaļu atteice vai darbības traucējumi var tieši radīt riskus kritiskās infrastruktūras fiziskajai integritātei un tādējādi riskus cilvēku veselībai un drošībai un mantas drošībai. Sastāvdaļas, ko paredzēts lietot tikai kibernetikas nolūkos, nebūtu uzskatāmas par drošības sastāvdaļām. Šādas kritiskās infrastruktūras drošības sastāvdaļu piemēri var būt sistēmas ūdens spiediena uzraudzībai vai ugunsgrēka signalizācijas sistēmas mākonādošanas Centros.

- (56) MI sistēmu ieviešana izglītībā ir svarīga, lai veicinātu kvalitatīvu digitālo izglītību un apmācību un lai visi izglītojamie un skolotāji varētu apgūt un kopīgot nepieciešamās digitālās prasmes un kompetences, tostarp medijpratību un kritisko domāšanu, lai aktīvi piedalītos ekonomikas, sabiedrības un demokrātiskajos procesos. Tomēr MI sistēmas, ko lieto izglītībā un arodmācībā, jo īpaši, lai noteiktu personu piekļuvi izglītības un arodmācību iestādēm vai programmām visos līmeņos vai lai izlemtu par personu iestāšanos tajās, lai personas tajās uzņemtu, lai izvērtētu personu mācīšanās rezultātus, lai novērtētu attiecīgo personas izglītības līmeni un būtiski ietekmētu tās izglītības un apmācības līmeni, ko personas saņem vai kam tās spēj piekļūt, vai lai pārbaudījumu laikā uzraudzītu un konstatētu audzēkņu neatļautu uzvedību, būtu jāklasificē kā augsta riska MI sistēmas, jo tās var noteikt izglītības vai profesionālo ievirzi personas dzīvē un tādējādi varētu ietekmēt minētās personas spēju nodrošināt sev iztiku. Ja šādas sistēmas ir nepareizi projektētas un tiek neatbilstīgi lietotas, tās var būt īpaši aizskarošas un var pārkāpt tiesības uz izglītību un apmācību, kā arī tiesības uz nediskrimināšanu un nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, pret sievietēm, noteiktām vecuma grupām, personām ar invaliditāti vai personām ar noteiktu rases vai etnisko izcelsmi vai dzimumorientāciju.
- (57) MI sistēmas, kuras lieto nodarbinātībā, darba ņēmēju pārvaldībā un piekļuvē pašnodarbinātībai, jo īpaši personu darbā līgšanā un atlasē, lēmumu pieņemšanā, kas skar darba attiecību, paaugstināšanas amatā un darba līgumattiecību izbeigšanas kārtību, uzdevumu sadalē, pamatojoties uz individuālo uzvedību vai personības iezīmēm vai īpašībām, un darba līgumattiecībās esošu personu pārraudzībā vai izvērtēšanā, arī būtu jāklasificē kā augsta riska sistēmas, jo minētās sistēmas var ievērojami ietekmēt karjeras iespējas nākotnē, minēto personu labklājību un darba ņēmēju tiesības. Attiecīgajām darba līgumattiecībām būtu jāpilnībā jāietver darba ņēmēji un personas, kuras sniedz pakalpojumus, izmantojot platformas, kā norādīts Komisijas darba programmā 2021. gadam. Darbā līgšanas procesā un izvērtēšanas, paaugstināšanas amatā vai darba līgumattiecību uzturēšanas ietvaros minētās sistēmas var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, attiecībā uz sievietēm, dažām vecuma grupām, personām ar invaliditāti vai personām ar noteiktu etnisko vai rasisko piederību vai seksuālo orientāciju. MI sistēmas, ko lieto šādu personu snieguma un uzvedības pārraudzībai, var arī apdraudēt viņu pamattiesības uz datu aizsardzību un privātumu.
- (58) Cita joma, kurā MI sistēmu lietošanai ir jāpievērš īpaša uzmanība, ir piekļuve dažiem 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. Jo īpaši fiziskas personas, kuras piesakās pamata sociālās palīdzības pabalstiem un pakalpojumiem vai saņem tos no publiskām iestādēm, proti, veselības aprūpes pakalpojumus, sociālās nodrošināšanas pabalstus, sociālos pakalpojumus, kas nodrošina aizsardzību tādos gadījumos kā maternitāte, slimība, nelaimes gadījumi darbā, atrašanās apgādībā vai vecums un darba zaudēšana, kā arī sociālā palīdzība un palīdzība mājokļa jomā, parasti ir atkarīgas no minētajiem pabalstiem un pakalpojumiem un atrodas neaizsargātā pozīcijā attiecībā pret atbildīgajām iestādēm. Ja MI sistēmas lieto, lai noteiktu, vai iestādēm šādi pabalsti un pakalpojumi būtu jāpiešķir, jāatsaka, jāsamazina, jāatsauc vai jāatgūst, tostarp, lai noteiktu, vai labuma guvējiem ir likumīgas tiesības uz šādiem pabalstiem vai pakalpojumiem, minētajām sistēmām var būt ievērojama ietekme uz personu iztiku, un tās var pārkāpt tādas personu pamattiesības kā tiesības uz sociālo aizsardzību, nediskrimināšanu, cilvēka cieņu vai efektīvu tiesību aizsardzību, un tāpēc tās 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 MI sistēmu plašākas lietošanas ar noteikumu, ka minētās sistēmas nerada augstu risku fiziskām un juridiskām personām. Turklāt MI sistēmas, ko lieto fizisku personu kredītnovērtējuma vai kredītpējas izvērtēšanai, būtu jāklasificē kā augsta riska MI sistēmas, jo tās nosaka minēto personu piekļuvi finanšu resursiem vai tādiem būtiskiem pakalpojumiem kā mājoklis, elektroenerģija un telesakaru pakalpojumi. Minētajiem nolūkiem lietotās MI sistēmas var izraisīt diskrimināciju starp personām vai grupām un var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, pamatojoties uz rasisko vai etnisko izcelsmi, dzimumu, invaliditāti, vecumu vai seksuālo orientāciju, vai var radīt jaunus diskriminējošas ietekmes veidus. Tomēr MI sistēmas, kas Savienības tiesību aktos paredzētas, lai atklātu krāpšanu finanšu pakalpojumu piedāvāšanā un prudenciālos nolūkos aprēķinātu kredītiestāžu un apdrošināšanas sabiedrību kapitāla prasības, nebūtu jāuzskata par augsta riska sistēmām saskaņā ar šo regulu. Turklāt MI sistēmas, ko paredzēts lietot riska novērtēšanai un cenu

noteikšanai saistībā ar fiziskām personām veselības un dzīvības apdrošināšanas gadījumā, var būt ievērojama ietekme uz personu iztiku un, ja tās netiek pienācīgi projektētas, izstrādātas un lietotas, var pārkāpt viņu pamattiesības un radīt nopietnas sekas cilvēku dzīvībai un veselībai, tostarp finansiālu atstumtību un diskrimināciju. Visbeidzot, MI sistēmas, ko lieto fizisku personu ārkārtas palīdzības izsaukumu novērtēšanai un klasificēšanai vai ārkārtas pirmās reaģēšanas dienestu, tostarp policijas, ugunsdzēsēju un medicīniskās palīdzības sniedzēju, nosūtīšanai vai nosūtīšanas prioritāšu noteikšanai, kā arī neatliekamās medicīniskās aprūpes pacientu triāžas sistēmām, arī būtu jāklasificē kā augsta riska sistēmas, jo tās pieņem lēmumus personu veselībai un dzīvībai un to īpašumam izšķirīgi svarīgās situācijās.

- (59) Ņemot vērā tiesībaizsardzības iestāžu lomu un atbildību, to darbībām, kuras ietver dažus MI sistēmu lietošanas veidus, ir raksturīga ievērojama varas nesamērība, un to rezultāts var būt fiziskas personas novērošana, aizturēšana vai tās brīvības atņemšana, kā arī cita veida nelabvēlīga ietekme uz Hartā garantētajām pamattiesībām. Proti, ja MI sistēma nav apmācīta ar augstas kvalitātes datiem, neatbilst attiecīgām veikspējas, precizitātes vai robustuma prasībām vai nav pienācīgi projektēta un testēta pirms laišanas tirgū vai citādas nodošanas ekspluatācijā, tā var norādīt uz cilvēkiem diskriminējošu vai kā citādi nekorektu vai netaisnīgu veidu. Turklāt 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 šādas MI sistēmas nav pietiekami pārredzamas, izskaidrojamas un dokumentētas. Tāpēc ir lietderīgi klasificēt kā augsta riska sistēmas, ciktāl to lietošanu atļauj attiecīgie Savienības vai valsts tiesību akti, vairākas MI 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 MI sistēmām jo īpaši būtu jāpieskaita MI sistēmas, ko tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, lai novērtētu risku, ka fiziska persona varētu kļūt par cietušo personu noziedzīgos nodarījumos, paredzēts lietot kā melu detektorus vai līdzīgus rīkus, pierādījumu uzticamības izvērtēšanai noziedzīgu nodarījumu izmeklēšanas vai kriminālvajāšanas gaitā un, ciktāl to neaizliedz šī regula, lai novērtētu risku, ka fiziska persona varētu izdarīt vai atkārtoti izdarīt nodarījumu, pamatojoties ne tikai uz fizisku personu profilēšanu vai novērtējot personiskās īpašības un rakstura iezīmes vai iepriekšēju noziedzīgu rīcību, profilēšanai noziedzīgu nodarījumu atklāšanas, izmeklēšanas vai kriminālvajāšanas gaitā. MI sistēmas, kuras konkrēti paredzētas lietošanai administratīvajā procesā nodokļu un muitas iestādēs, kā arī finanšu ziņu vākšanas vienībās, kas veic administratīvus uzdevumus informācijas analizēšanai, ievērojot Savienības tiesību aktus nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas jomā, nebūtu jāklasificē kā augsta riska MI sistēma, ko tiesībaizsardzības iestādes lieto noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai un kriminālvajāšanai par tiem. MI rīku lietošanai tiesībaizsardzības un citās attiecīgās iestādēs nevajadzētu kļūt par nevienlīdzības vai atstumtības faktoru. MI rīku lietošanas ietekme uz aizdomās turētu personu tiesībām uz aizstāvību nebūtu jāignorē, jo īpaši grūtības iegūt jēgpilnu informāciju par minēto sistēmu darbību un no tā izrietošās grūtības apstrīdēt to rezultātus tiesā, jo īpaši fiziskām personām, par kurām tika veikta izmeklēšana.
- (60) Migrācijas un patvēruma jomā un robežkontroles pārvaldībā lietotās MI sistēmas ietekmē personas, kuri bieži ir īpaši neaizsargātā pozīcijā un ir atkarīgi no kompetento publisko iestāžu darbības rezultāta. Tāpēc minētajos kontekstos lietoto MI sistēmu precizitāte, nediskriminējošais raksturs un pārredzamība ir īpaši svarīga skarto personu pamattiesību ievērošanas garantēšanai, jo īpaši viņu tiesību brīvi pārvietoties, tiesību uz nediskriminēšanu, privātuma un personas datu aizsardzību, starptautisko aizsardzību un labu pārvaldību īstenošanai. Tāpēc ir lietderīgi klasificēt kā augsta riska sistēmas, ciktāl to lietošanu atļauj attiecīgie Savienības vai valsts tiesību akti, MI sistēmas, ko kompetentajās publiskajās iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kurām uzticēti pienākumi migrācijas, patvēruma un robežkontroles pārvaldības jomā, paredzēts lietot kā melu detektorus un līdzīgus rīkus, lai novērtētu dažus riskus, kurus rada fiziskas personas, kas ieceļo dalībvalsts teritorijā vai piesakās vīzai vai patvērumam, sniegtu palīdzību kompetentām publiskām iestādēm, tostarp, veicot saistītu pierādījumu patiesuma novērtēšanu, patvēruma, vīzu un uzturēšanās atļauju pieteikumu un saistīto sūdzību izskatīšanā ar mērķi noteikt fizisku personu, kuras piesakās uz kādu statusu, atbilstību kritērijiem, nolūkā atklāt, apazīt vai identificēt fiziskas personas saistībā ar migrācijas, patvēruma vai robežkontroles pārvaldību, izņemot ceļošanas dokumentu verifikāciju. MI sistēmām migrācijas, patvēruma un robežkontroles pārvaldības jomā, uz kurām attiecas šī regula, būtu jāatbilst attiecīgajām procesuālajām prasībām, kas noteiktas Eiropas Parlamenta un Padomes Regulā (EK)

Nr. 810/2009 ⁽³²⁾, Eiropas Parlamenta un Padomes Direktīvā 2013/32/ES ⁽³³⁾ un citos attiecīgajos Savienības tiesību aktos. Dalībvalstīm vai Savienības iestādēm, struktūrām, birojiem vai aģentūrām nekādā gadījumā nebūtu jālieto MI sistēmas migrācijas, patvēruma un robežkontroles pārvaldībā kā līdzekli, lai apietu savas starptautiskās saistības saskaņā ar 1951. gada 28. jūlijā Ženēvā parakstīto ANO Konvenciju par bēgļa statusu, kas grozīta ar 1967. gada 31. janvāra protokolu. Tās arī nebūtu jālieto, lai jebkādā veidā pārkāptu neizraidīšanas principu vai liegtu drošas un efektīvas likumīgas iespējas iekļūt Savienības teritorijā, tostarp tiesības uz starptautisko aizsardzību.

- (61) Dažas MI 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. Jo īpaši, lai mazinātu potenciālu neobjektivitātes, kļūdu un nepārredzamības risku, ir lietderīgi kvalificēt par augsta riska sistēmām tās MI sistēmas, kuras paredzēts lietot tiesu iestādē vai tās vārdā, lai palīdzētu tiesu iestādēm fakti un tiesību normu interpretēšanā un tiesību normu piemērošanā konkrētam fakti kopumam. MI sistēmas, ko minētajos nolūkos paredzēts lietot strīdu izšķiršanas ārpustiesas kārtībā struktūrās, arī būtu jāuzskata par augsta riska sistēmām, ja strīdu izšķiršanas ārpustiesas kārtībā izskatīšanas iznākums pusēm rada tiesiskas sekas. MI rīku lietošana var atbalstīt tiesnešu lēmumu pieņemšanas pilnvaras vai tiesu neatkarību, bet tai nevajadzētu to aizstāt: galīgajai lēmumu pieņemšanai arī turpmāk jābūt cilvēka virzītai darbībai. Tomēr MI sistēmu klasificēšana par augsta riska sistēmām nebūtu jāattiecinā uz MI sistēmām, kuras paredzētas tikai tādu administratīvu papilddarbību veikšanai, kam nav ietekmes uz faktiski tiesvedību atsevišķās lietās, piemēram, tiesas nolēmumu, dokumentu vai datu anonimizācijai vai pseidonimizācijai, saziņai starp darbiniekiem un administratīvu uzdevumu veikšanai.
- (62) Neskarot Eiropas Parlamenta un Padomes Regulā (ES) 2024/900 ⁽³⁴⁾ paredzētos noteikumus un lai novērstu riskus, kas saistīti ar nepamatotu ārēju iejaukšanos Hartas 39. pantā nostiprinātajās tiesībās balsot un nelabvēlīgu ietekmi uz demokrātiju un tiesiskumu, MI sistēmas, ko paredzēts lietot, lai ietekmētu vēlēšanu vai referenduma rezultātus vai fizisku personu balsošanas uzvedību, kad tās piedalās vēlēšanās vai referendumos, būtu jāklasificē kā augsta riska MI sistēmas, izņemot MI sistēmas, kuru iznākuma fiziskas personas nav tieši pakļautas to ietekmei, piemēram, rīki, ko lieto, lai organizētu, optimizētu un strukturētu politiskās kampaņas no administratīvā un loģistikas viedokļa.
- (63) Fakts, ka MI sistēma saskaņā ar šo regulu ir klasificēta kā augsta riska MI sistēma, nebūtu jāinterpretē kā norāde, ka sistēmas lietošana ir likumīga citu Savienības tiesību aktu vai ar tiem saderīgu valsts tiesību aktu ietvaros, piemēram, attiecībā uz personas datu aizsardzību, melu detektoru un tamlīdzīgu rīku vai citu sistēmu lietošanu fizisku personu emocionālā stāvokļa noteikšanai. Šāda lietošana būtu jāturpina tikai saskaņā ar piemērojamajām prasībām, kas izriet no Hartas un no attiecīgajiem Savienības sekundārajiem tiesību aktiem un dalībvalstu tiesību aktiem. Nebūtu jāuzskata, ka šī regula nodrošina juridisko pamatu personas datu, tostarp – attiecīgā gadījumā – īpašu kategoriju personas datu, apstrādei, ja vien šajā regulā nav konkrēti noteikts citādi.
- (64) Lai mazinātu tirgū laisto vai ekspluatācijā nodoto augsta riska MI sistēmu radītos riskus un nodrošinātu augstu uzticamības līmeni, augsta riska MI sistēmām būtu jāpiemēro dažas obligātas prasības, ņemot vērā paredzēto MI sistēmas lietošanas nolūku un saskaņā ar riska pārvaldības sistēmu, kura nodrošinātajam jāizveido. Pasākumos, ko nodrošinātāji pieņemusi, lai izpildītu šīs regulas obligātās prasības, būtu jāņem vērā vispārārstītie jaunākie sasniegumi MI jomā, tiem vajadzētu būt samērīgiem un efektīviem, lai sasniegtu šīs regulas mērķus. Pamatojoties uz Jauno tiesisko regulējumu, kā precizēts Komisijas paziņojumā “Zilā rokasgrāmata” par ES produktu noteikumu īstenošanu 2022. gadā, vispārējais noteikums ir tāds, ka vairāk nekā vienu Savienības saskaņošanas tiesību aktu var piemērot vienam produktam, jo to darīt pieejamu vai nodot ekspluatācijā var tikai tad, ja produkts atbilst visiem piemērojamiem Savienības saskaņošanas tiesību aktiem. MI sistēmu apdraudējumi, uz kuriem attiecas šīs regulas prasības, attiecas uz citiem aspektiem, nevis spēkā esošajiem Savienības saskaņošanas tiesību aktiem, un tāpēc šīs regulas prasības papildinātu esošo Savienības saskaņošanas aktu struktūru. Piemēram, mašīnas vai medicīniskās ierīces, kas ietver MI sistēmu, varētu radīt riskus, uz kuriem neattiecas būtiskās veselības un drošības prasības, kas noteiktas attiecīgajos Savienības saskaņošanas tiesību aktos, jo minētie nozaru tiesību akti neattiecas uz MI sistēmām

⁽³²⁾ 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.).

⁽³³⁾ 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.).

⁽³⁴⁾ Eiropas Parlamenta un Padomes Regula (ES) 2024/900 (2024. gada 13. marts) par politiskās reklāmas pārredzamību un mērķorientēšanu (OV L, 2024/900, 20.3.2024., ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

raksturīgiem riskiem. Tāpēc vienlaikus un papildinoši ir jāpiemēro dažādi tiesību akti. Lai nodrošinātu konsekvenci un izvairītos no nevajadzīga administratīvā sloga un nevajadzīgām izmaksām, tāda produkta nodrošinātājiem, kas ietver vienu vai vairākas augsta riska MI sistēmas, uz kurām attiecas šīs regulas un šīs regulas pielikumā uzskaitīto Savienības saskaņošanas tiesību aktu, kuru pamatā ir Jaunais tiesiskais regulējums, prasības, vajadzētu būt elastīgiem attiecībā uz operatīviem lēmumiem par to, kā optimāli nodrošināt produkta, kas ietver vienu vai vairākas MI sistēmas, atbilstību visām piemērojamām minēto Savienības saskaņoto tiesību aktu prasībām. Minētā elastība varētu nozīmēt, piemēram, nodrošinātāja lēmumu daļu no nepieciešamajiem testēšanas un ziņošanas procesiem, šajā regulā prasīto informāciju un dokumentāciju integrēt jau esošā dokumentācijā un procedūrās, kas prasītas saskaņā ar šīs regulas pielikumā uzskaitītajiem esošajiem Savienības saskaņošanas tiesību aktiem, kuru pamatā ir Jaunais tiesiskais regulējums. Tam nekādā veidā nevajadzētu ietekmēt nodrošinātāja pienākumu ievērot visas piemērojamās prasības.

- (65) Riska pārvaldības sistēmu būtu jāveido nepārtrauktam iteratīvam procesam, ko plāno un kas norit visā augsta riska MI sistēmas darbībā. Minētā procesa mērķim vajadzētu būt identificēt un mazināt MI sistēmu attiecīgos riskus veselībai, drošībai un pamattiesībām. Riska pārvaldības sistēma būtu regulāri jāpārskata un jāatjaunina, lai nodrošinātu tās pastāvīgu efektivitāti, kā arī visu nozīmīgo lēmumu un darbību, kas veiktas, ievērojot šo regulu, pamatotību un dokumentāciju. Šim procesam būtu jānodrošina, ka nodrošinātājs identificē riskus vai nelabvēlīgu ietekmi un īsteno riska mazināšanas pasākumus attiecībā uz MI sistēmu zināmajiem un saprātīgi paredzamajiem riskiem veselībai, drošībai un pamattiesībām, ņemot vērā to paredzēto nolūku un saprātīgi paredzamu nepareizu lietošanu, tostarp iespējamos riskus, ko rada mijiedarbība starp MI sistēmu un vidi, kurā tā darbojas. Riska pārvaldības sistēmai būtu jāpieņem vispiemērotākie riska pārvaldības pasākumi, ņemot vērā jaunākos sasniegumus MI jomā. Identificējot vispiemērotākos riska pārvaldības pasākumus, nodrošinātājam būtu jādokumentē un jāizskaidro izdarītās izvēles un attiecīgā gadījumā jāiesaista eksperti un ārējās ieinteresētās personas. Identificējot augsta riska MI sistēmu saprātīgi paredzamu nepareizu lietošanu, nodrošinātājam būtu jāaptver tādi MI sistēmu lietojumi, kuri nav tieši saistīti ar paredzēto nolūku un kuri ir paredzēti lietošanas instrukcijā, tomēr var saprātīgi sagaidīt, ka tie izrietēs no viegli paredzamas cilvēka uzvedības konkrētas MI sistēmas konkrēto īpašību un lietojuma kontekstā. Visi zināmie vai paredzamie apstākļi, kas saistīti ar augsta riska MI sistēmas lietošanu atbilstoši tai paredzētajam nolūkam vai saprātīgi paredzamas nepareizas lietošanas apstākļos un kas var radīt risku veselībai un drošībai vai pamattiesībām, būtu jāiekļauj nodrošinātāja sniegtajās lietošanas instrukcijās. Tas ir vajadzīgs, lai nodrošinātu, ka uzturētājs ir informēts un ņem tās vērā, izmantojot augsta riska MI sistēmu. Lai identificētu un īstenotu riska mazināšanas pasākumus paredzamai nepareizai lietošanai saskaņā ar šo regulu, nodrošinātājam, lai novērstu paredzamu nepareizu lietošanu, nebūtu vajadzīgi īpaša papildu apmācība augsta riska MI sistēmai. Tomēr nodrošinātāji tiek mudināti apsvērt šādus papildu apmācības pasākumus, lai mazinātu saprātīgi paredzamu nepareizu lietošanu, ja tie ir nepieciešami un piemēroti.
- (66) Prasībām būtu jāattiecas uz augsta riska MI sistēmām saistībā ar riska pārvaldību, izmantoto datu kopu kvalitāti un nozīmīgumu, tehnisko dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu uzturētājiem, cilvēka virsvadību un robustumu, precizitāti un kiberdrošību. Minētās prasības ir nepieciešamas, lai efektīvi mazinātu riskus veselībai, drošībai un pamattiesībām. Ņemot vērā to, ka citi tirdzniecību mazāk ierobežojoši pasākumi nav saprātīgi pieejami, minētās prasības nav nepamatoti tirdzniecības ierobežojumi.
- (67) Augstas kvalitātes datiem un piekļuvei augstas kvalitātes datiem ir būtiska loma daudzu MI sistēmu struktūras nodrošināšanā un veikspējas nodrošināšanā, jo īpaši, ja tiek izmantotas metodes, kas ietver modeļu apmācīšanu, ar mērķi nodrošināt, ka augsta riska MI sistēma darbojas, kā paredzēts, un droši un ka tā nekļūst par Savienības tiesību aktos aizliegtas diskriminācijas avotu. Lai nodrošinātu augstas kvalitātes datu kopas apmācībai, validēšanai un testēšanai, ir jāīsteno atbilstoša datu pārvaldība un pārvaldības prakse. Apmācības, validēšanas un testēšanas datu kopām, tostarp marķējumiem, vajadzētu būt atbilstošām, pietiekami reprezentatīvām un, cik vien iespējams, bez kļūdām un pilnīgām, ņemot vērā sistēmas paredzēto nolūku. Lai veicinātu atbilstību Savienības datu aizsardzības tiesību aktiem, piemēram, Regulai (ES) 2016/679, datu pārvaldībā un pārvaldības praksē – personas datu gadījumā – būtu jāietver pārredzamība attiecībā uz datu vākšanas sākotnējo nolūku. Datu kopām vajadzētu būt arī atbilstošiem statistiskajiem raksturlielumiem, tostarp attiecībā uz personām vai personu grupām, attiecībā uz kurām ir paredzēts lietot augsta riska MI sistēmu, īpašu uzmanību pievēršot tādas iespējamās neobjektivitātes mazināšanai datu kopās, kura varētu ietekmēt personu veselību un drošību, kurai varētu būt negatīva ietekme uz pamattiesībām vai kura varētu izraisīt diskrimināciju, kas ir aizliegta Savienības tiesību aktos, jo īpaši, ja izvaddati ievaddatus

turpmākām darbībām (atgriezeniskās saites cilpas). Neobjektivitāte, piemēram, var būt raksturīga pamatā esošajām datu kopām, jo īpaši tad, ja tiek izmantoti vēsturiski dati, vai radīta tad, kad sistēmas tiek izmantotas reālās pasaules apstākļos. MI sistēmu sniegtos rezultātus varētu ietekmēt šāda raksturīga neobjektivitāte, kas tiecas pakāpeniski palielināties un tādējādi turpināt un pastiprināt esošo diskrimināciju, jo īpaši attiecībā uz personām, kas pieder pie dažām neaizsargātām grupām, tostarp rasiskām vai etniskām grupām. Prasībai par to, ka datu kopām jābūt pēc iespējas pilnīgām un bez kļūdām, nebūtu jāietekmē privātumu aizsargājošu metožu izmantošana MI sistēmu izstrādes un testēšanas kontekstā. Jo īpaši datu kopās, ciktāl to nosaka to paredzētais nolūks, būtu jāņem vērā iezīmes, raksturlielumi vai elementi, kas raksturīgi konkrētajai ģeogrāfiskajai, kontekstuālajai, uzvedības vai funkcionālajai videi, kurā MI sistēmu paredzēts lietot. Ar datu pārvaldību saistītās prasības var izpildīt, izmantojot trešās personas, kas piedāvā sertificētus atbilstības pakalpojumus, tostarp datu pārvaldības, datu kopu integritātes un datu apmācības, validēšanas un testēšanas prakses verifikāciju, ciktāl tiek nodrošināta atbilstība šīs regulas datu prasībām.

- (68) Augsta riska MI sistēmu izstrādes un novērtēšanas nolūkā dažiem dalībniekiem, piemēram, nodrošinātajiem, paziņotajām struktūrām un citām attiecīgajām struktūrām, piemēram, Eiropas digitālās inovācijas centriem, testēšanas un eksperimentēšanas struktūrām un pētniekiem, būtu jāvar piekļūt augstas kvalitātes datu kopām un izmantot tās minēto dalībnieku darbības jomās, kas ir saistītas ar šo regulu. Komisijas izveidotās Eiropas vienotās datu telpas un datu kopīgošanas atvieglošana uzņēmumu starpā un ar valdības iestādēm sabiedrības interešu labā būs ļoti būtiska, lai nodrošinātu uzticēšanos raisošu, pārskatāmu un nediskriminējošu piekļuvi augstas kvalitātes datiem MI sistēmu apmācībai, validēšanai un testēšanai. Piemēram, veselības jomā Eiropas veselības datu telpa veicinās nediskriminējošu piekļuvi veselības jomas datiem un MI algoritmu apmācībai minētajās datu kopās privātumu saglabājošā, drošā, savlaicīgā, pārredzamā un uzticamā veidā ar pienācīgu institucionālo pārvaldi. Arī attiecīgās kompetentās iestādes, tostarp nozaru iestādes, nodrošinot vai atbalstot piekļuvi datiem, var atbalstīt augstas kvalitātes datu piegādāšanu MI sistēmu apmācībai, validēšanai un testēšanai.
- (69) Tiesības uz privātumu un personas datu aizsardzību ir jāgarantē visā MI sistēmas darbmūžā. Šajā sakarā personas datu apstrādes gadījumā ir piemērojami datu minimizēšanas, integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principi, kā noteikts Savienības datu aizsardzības tiesību aktos. Neskarot šajā regulā paredzētās datu pārvaldības prasības, nodrošinātāju veiktie pasākumi, lai nodrošinātu atbilstību minētajiem principiem, var ietvert ne tikai anonimizāciju un šifrēšanu, bet arī tādas tehnoloģijas lietošanu, kas ļauj algoritmus ievadīt datus un ļauj apmācīt MI sistēmas, nepārsūtot starp pusēm vai nekopējot pašus neapstrādātos vai strukturētos datus.
- (70) Lai citu tiesības aizsargātu pret diskrimināciju, kas varētu izrietēt no MI sistēmu neobjektivitātes, nodrošinātajiem izņēmuma kārtā, ciktāl tas ir absolūti nepieciešams, lai nodrošinātu neobjektivitātes atklāšanu un labošanu saistībā ar augsta riska MI sistēmām, ievērojot atbilstošus fizisku personu pamattiesību un pamatbrīvību aizsardzības pasākumus un pēc visu šajā regulā paredzēto piemērojamo nosacījumu piemērošanas papildus Regulās (ES) 2016/679 un (ES) 2018/1725 un Direktīvā (ES) 2016/680 paredzētajiem nosacījumiem, būtu jāvar apstrādāt arī īpašu kategoriju personas datus svarīgās sabiedrības interesēs Regulas (ES) (ES) 2016/679 9. panta 2. punkta g) apakšpunkta un Regulas (ES) 2018/1725 10. panta 2. punkta g) apakšpunkta nozīmē.
- (71) Saprotama informācija par to, kā izstrādātas augsta riska MI sistēmas un kā tās darbojas visā savā darbmūžā, ir ļoti būtiska, lai nodrošinātu minēto sistēmu ietekmējamību, pārbaudītu atbilstību šajā regulā noteiktajām prasībām, kā arī veiktu darbības pārraudzību un pēctirgus pārraudzību. Tam nepieciešama uzskaitē un tādas tehniskās dokumentācijas pieejamība, kura ietver informāciju, kas nepieciešama, lai novērtētu MI sistēmas atbilstību attiecīgajām prasībām un atvieglotu pēctirgus pārraudzību. 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, un tai vajadzētu būt sagatavotai skaidrā un visaptverošā veidā. Tehniskā dokumentācija būtu pienācīgi jāaktualizē visā MI sistēmas darbmūžā. Turklāt augsta riska MI sistēmām būtu tehniski jāļauj automātiski reģistrēt notikumus, izmantojot "žurnāldatnes", visā sistēmas darbmūža laikā.

- (72) Lai kļiedētu bažas, kas saistītas ar dažu MI sistēmu nepārredzamību un sarežģītību, un palīdzētu uzturētājiem izpildīt savus pienākumus saskaņā ar šo regulu, pirms augsta riska MI sistēmu laišanas tirgū vai nodošanas ekspluatācijā būtu jānodrošina to pārredzamība. Augsta riska MI sistēmas būtu jāprojektē tā, lai uzturētāji varētu saprast, kā MI sistēma darbojas, izvērtēt tās funkcionalitāti un izprast tās stiprās puses un ierobežojumus. Augsta riska MI sistēmām būtu jāpievieno atbilstoša informācija lietošanas instrukcijas veidā. Šādai informācijai būtu jāietver MI sistēmas raksturlielumi, spējas un veikspējas ierobežojumi. Minētie elementi ietvertu informāciju par iespējamām zināmām un paredzamiem apstākļiem, kuri saistīti ar augsta riska MI sistēmas lietošanu, tostarp uzturētāja darbību, kas var ietekmēt sistēmas uzvedību un veikspēju, un kuros MI sistēma var radīt riskus veselībai, drošībai un pamattiesībām, par izmaiņām, kuras nodrošinātājs ir iepriekš noteicis un novērtējis attiecībā uz atbilstību, un par attiecīgajiem cilvēka virsvadības pasākumiem, tostarp pasākumiem, ar kuriem uzturētājiem palīdz interpretēt MI sistēmas iznākumus. Pārredzamībai, tostarp pievienotajai lietošanas instrukcijai, būtu jāpalīdz uzturētājiem sistēmas lietošanā un būtu jāatbalsta, ka tie pieņem informētus lēmumus. Uzturētājiem cita starpā vajadzētu būt labākām iespējām pareizi izvēlēties sistēmu, ko tie plāno lietot, ņemot vērā pienākumus, kas uz tiem attiecas, tiem vajadzētu būt izglītotiem par paredzētajiem un aizliegtajiem lietojumiem, un tiem būtu MI sistēma jālieto pareizi un atbilstoši. Lai uzlabotu lietošanas instrukcijā iekļautās informācijas skaidrību un pieklūstamību, attiecīgā gadījumā būtu jāiekļauj ilustratīvi piemēri, piemēram, par ierobežojumiem un par paredzētajiem un aizliegtajiem MI sistēmas lietojumiem. Nodrošinātājiem būtu jānodrošina, ka visa dokumentācija, tostarp lietošanas instrukcija, ietver jēgpilnu, visaptverošu, pieejamu un saprotamu informāciju, ņemot vērā mērķēto uzturētāju vajadzības un paredzamās zināšanas. Lietošanas instrukcijām vajadzētu būt pieejamām mērķētajiem uzturētājiem viegli saprotamā valodā, kā noteikusi attiecīgā dalībvalsts.
- (73) Augsta riska MI sistēmas būtu jāprojektē un jāizstrādā tā, lai fiziskas personas varētu virsvadīt to funkcionēšanu, nodrošināt, ka tās tiek lietotas, kā paredzēts, un ka to ietekmei pievēršas visā sistēmas darbībā. Šajā nolūkā sistēmas nodrošinātājam pirms sistēmas laišanas tirgū vai nodošanas ekspluatācijā būtu jānosaka piemēroti cilvēka virsvadības pasākumi. Jo īpaši, attiecīgā gadījumā šādiem pasākumiem būtu jāgarantē, ka sistēmai ir iebūvēti operacionāli ierobežojumi, kurus pati sistēma nevar neievērot, un ka tā reaģē uz cilvēka-operatora virsvadību un ka fiziskām personām, kurām uzticēta šī virsvadība, ir uzdevuma veikšanai nepieciešamā kompetence, apmācība un pilnvaras. Attiecīgā gadījumā ir arī būtiski nodrošināt, ka augsta riska MI sistēmas ietver mehānismus, kas ievirza un informē fizisku personu, kurai ir uzticēta cilvēka virsvadība, lai tā pieņemtu informētus lēmumus par to, vai, kad un kā iejaukties, lai izvairītos no negatīvām sekām vai riskiem, vai apturētu sistēmu, ja tā nedarbojas, kā paredzēts. Ņemot vērā būtiskās sekas personām, ja dažas biometriskās identifikācijas sistēmas uzrādītu nepareizu atbilstību, ir lietderīgi attiecībā uz minētajām sistēmām paredzēt pastiprinātas cilvēka virsvadības prasību, lai uzturētājs, pamatojoties uz identifikāciju, kas izriet no sistēmas, nevarētu veikt nekādas darbības vai pieņemt lēmumu, ja vien to nav atsevišķi pārbaudījušas un apstiprinājušas vismaz divas fiziskas personas. Minētās personas varētu būt no vienas vai vairākām vienībām, tostarp persona, kas darbina vai izmanto sistēmu. Šai prasībai nevajadzētu radīt nevajadzīgu slogu vai kavēšanos, un varētu pietikt ar to, ka sistēmas ģenerētajās žurnāldatnēs tiek automātiski reģistrētas dažādu personu veiktās atsevišķās verifikācijas. Ņemot vērā tiesībaizsardzības, migrācijas, robežkontroles un patvēruma jomu specifiku, šī prasība nebūtu jāpiemēro, ja Savienības vai valsts tiesību aktos minētās prasības piemērošana tiek uzskatīta par nesamērīgu.
- (74) Augsta riska MI sistēmām jādarbojas konsekventi visā to darbībā un jānodrošina atbilstošs precizitātes, robustuma un kiberdrošības līmenis, ņemot vērā to paredzēto nolūku un saskaņā ar vispārāzīto tehnoloģiju attīstības līmeni. Komisija un attiecīgās organizācijas un ieinteresētās personas tiek mudinātas pienācīgi ņemt vērā MI sistēmas risku un negatīvās ietekmes mazināšanu. Paredzamais veikspējas rādītāju līmenis būtu jānorāda pievienotajā lietošanas instrukcijā. Nodrošinātāji tiek mudināti minēto informāciju paziņot uzturētājiem skaidrā un viegli saprotamā veidā, bez pārpratumiem vai maldinošiem paziņojumiem. Savienības tiesību aktu par reglamentēto metroloģiju, tostarp Eiropas Parlamenta un Padomes Direktīvu 2014/31/ES⁽³⁵⁾ un 2014/32/ES⁽³⁶⁾, mērķis ir nodrošināt mērījumu precizitāti un veicināt komercdarījumu pārredzamību un taisnīgumu. Minētajā sakarā sadarbībā ar attiecīgajām ieinteresētajām personām un organizācijām, piemēram, metroloģijas un salīdzinošās vērtēšanas iestādēm, Komisijai attiecīgā gadījumā būtu jāveicina MI sistēmu etalonrādītāju un mērījumu metodiku izstrāde. To darot, Komisijai būtu jāņem vērā starptautiskie partneri, kas strādā metroloģijas un attiecīgo ar MI saistīto mērījumu rādītāju jomā, un jāsadarbības ar tiem.

⁽³⁵⁾ Eiropas Parlamenta un Padomes Direktīva 2014/31/ES (2014. gada 26. februāris) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz neautomātisko svaru pieejamību tirgū (OV L 96, 29.3.2014., 107. lpp.).

⁽³⁶⁾ Eiropas Parlamenta un Padomes Direktīva 2014/32/ES (2014. gada 26. februāris) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz mērinstrumentu pieejamību tirgū (OV L 96, 29.3.2014., 149. lpp.).

- (75) Tehniskais robustums ir viena no galvenajām prasībām augsta riska MI sistēmām. Tām vajadzētu būt noturīgām pret kaitīgu vai citādi nevēlamu uzvedību, ko var izraisīt ierobežojumi sistēmās vai vidē, kurā sistēmas darbojas (piemēram, kļūdas, defekti, neatbilstības, negaidītas situācijas). Tāpēc būtu jāveic tehniski un organizatoriski pasākumi, lai nodrošinātu augsta riska MI sistēmu robustumu, piemēram, projektējot un izstrādājot piemērotus tehniskus risinājumus, lai novērstu vai līdz minimumam samazinātu kaitīgu vai citādi nevēlamu uzvedību. Minētie tehniskie risinājumi var ietvert, piemēram, mehānismus, kas ļauj sistēmai droši pārtraukt savu darbību (drošatteices plāni) dažu noviržu gadījumā vai tad, ja darbība notiek ārpus konkrētām iepriekš noteiktām robežām. Nespēja aizsargāt pret šiem riskiem varētu ietekmēt drošību vai negatīvi ietekmēt pamattiesības, piemēram, MI sistēmas ģenerētu kļūdainu lēmumu vai nepareizu vai neobjektīvu iznākumu dēļ.
- (76) Kiberdrošībai ir būtiska loma, nodrošinot, ka MI sistēmas ir noturīgas pret mēģinājumiem mainīt to lietojumu, uzvedību, veikspēju vai apdraudēt to drošības iezīmes, ļaunprātīgām trešām personām izmantojot sistēmas vājās vietas. Kiberuzbrukumi MI sistēmām var izmantot MI konkrētos aktīvus, piemēram, apmācībā izmantotās datu kopas (piemēram, datu saindēšana) vai apmācītos modeļus (piemēram, pretnieciskie uzbrukumi vai dalības inference), vai ekspluatēt MI sistēmas digitālo aktīvu vai pamatā esošās IKT infrastruktūras vājās vietas. Lai nodrošinātu riskiem atbilstošu kiberdrošības līmeni, augsta riska MI sistēmu nodrošinātājiem būtu jāveic piemēroti pasākumi, piemēram, drošības kontroles, attiecīgi ņemot vērā arī pamatā esošo IKT infrastruktūru.
- (77) Neskarot šajā regulā noteiktās prasības attiecībā uz robustumu un precizitāti, augsta riska MI sistēmas, kas ietilpst Eiropas Parlamenta un Padomes Regulas par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem darbības jomā, saskaņā ar minēto regulu var apliecināt atbilstību šīs regulas kiberdrošības prasībām, izpildot minētajā regulā noteiktās kiberdrošības pamatprasības. Ja augsta riska MI sistēmas atbilst Regulas par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem pamatprasībām, tās būtu jāuzskata par atbilstošām šajā regulā noteiktajām kiberdrošības prasībām, ciktāl minēto prasību izpilde ir apliecināta saskaņā ar minēto regulu izdotā ES atbilstības deklarācijā vai tās daļās. Šajā nolūkā saskaņā ar Regulu par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem veiktā tādu kiberdrošības risku novērtējumā, kuri saistīti ar produktu ar digitāliem elementiem, kas saskaņā ar šo regulu klasificēti kā augsta riska MI sistēma, būtu jāņem vērā MI sistēmas kiberneturības riski attiecībā uz nepilnvarotu trešo personu mēģinājumiem mainīt tās lietojumu, uzvedību vai veikspēju, tostarp MI konkrētā ietekmējamība, piemēram, datu saindēšana vai pretnieciskie uzbrukumi, kā arī attiecīgā gadījumā riski pamattiesībām, kā noteikts šajā regulā.
- (78) Šajā regulā paredzētā atbilstības novērtēšanas procedūra būtu jāpiemēro attiecībā uz kiberdrošības pamatprasībām produktam ar digitāliem elementiem, uz ko attiecas Regula par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un kas saskaņā ar šo regulu klasificēti kā augsta riska MI sistēma. Tomēr šā noteikuma piemērošanai nevajadzētu samazināt nepieciešamo uzticamības līmeni kritiski svarīgiem produktiem ar digitāliem elementiem, uz kuriem attiecas Regula par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem. Tāpēc, atkāpjoties no šā noteikuma, augsta riska MI sistēmām, kuras ir šīs regulas darbības jomā un ir arī kvalificētas kā svarīgi un kritiski svarīgi produkti ar digitāliem elementiem, ievērojot Regulu par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem, un uz kurām attiecas šīs regulas pielikumā izklāstītā atbilstības novērtēšanas procedūra, kā pamatā ir iekšējā kontrole, piemēro Regulas par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem atbilstības novērtēšanas noteikumus, ciktāl tie attiecas uz minētās regulas kiberdrošības pamatprasībām. Šajā gadījumā visiem pārējiem aspektiem, uz kuriem attiecas šī regula, būtu jāpiemēro attiecīgie noteikumi par atbilstības novērtēšanu, pamatojoties uz iekšējo kontroli, kas izklāstīti šīs regulas pielikumā. Pamatojoties uz ENISA zināšanām un lietpratību par kiberdrošības politiku un uzdevumiem, kas ENISA uzticēti saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 ⁽³⁷⁾, Komisijai būtu jāsadarbības ar ENISA jautājumos, kas saistīti ar MI sistēmu kiberdrošību.

⁽³⁷⁾ 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., 15. lpp.).

- (79) Ir lietderīgi, ka konkrēta fiziska vai juridiska persona, kas definēta kā nodrošinātājs, uzņemas atbildību par augsta riska MI sistēmas laišanu tirgū vai nodošanu ekspluatācijā, neatkarīgi no tā, vai minētā fiziskā vai juridiskā persona ir tā persona, kas sistēmu projektējusi vai izstrādājusi.
- (80) Savienībai un dalībvalstīm kā Apvienoto Nāciju Organizācijas Konvencijas par personu ar invaliditāti tiesībām parakstītājām ir juridisks pienākums aizsargāt personas ar invaliditāti pret diskrimināciju un veicināt viņu līdztiesību, nodrošināt, ka personām ar invaliditāti ir tāda pati piekļuve informācijas un komunikācijas tehnoloģijām un sistēmām kā citiem, un nodrošināt personu ar invaliditāti privātuma ievērošanu. Ņemot vērā MI sistēmu pieaugošo nozīmi un lietošanu, universālā dizaina principu piemērošanai visām jaunajām tehnoloģijām un pakalpojumiem būtu jānodrošina pilnīga un vienlīdzīga piekļuve visiem, kurus potenciāli skar MI tehnoloģijas vai kuri tās izmanto, tostarp personām ar invaliditāti, tādā veidā, ka tiek pilnībā ievērota minēto personu cieņa un daudzveidība. Tāpēc ir būtiski, ka nodrošinātāji nodrošina pilnīgu atbilstību piekļūstamības prasībām, tostarp Eiropas Parlamenta un Padomes Direktīvai (ES) 2016/2102⁽³⁸⁾ un Direktīvai (ES) 2019/882. Nodrošinātājiem būtu jānodrošina integrēta atbilstība šīm prasībām. Tāpēc nepieciešamie pasākumi būtu pēc iespējas jāintegrē augsta riska MI sistēmas projektēšanā.
- (81) Nodrošinātājam būtu jāizveido stabila kvalitātes vadības sistēma, jānodrošina nepieciešamās atbilstības novērtēšanas procedūras pabeigšana, jāizstrādā attiecīgā dokumentācija un jāizveido spēcīga pēctirgus pārraudzības sistēma. Augsta riska MI sistēmu nodrošinātājiem, uz kuriem attiecas pienākumi attiecībā uz kvalitātes pārvaldības sistēmām saskaņā ar attiecīgajiem Savienības nozaru tiesību aktiem, vajadzētu būt iespējai šajā regulā paredzētās kvalitātes pārvaldības sistēmas elementus iekļaut esošajā kvalitātes pārvaldības sistēmā, kas paredzēta minētajos citos Savienības nozaru tiesību aktos. Turpmākajās standartizācijas darbībās vai Komisijas pieņemtajos norādījumos būtu jāņem vērā arī papildināmība starp šo regulu un spēkā esošajiem Savienības nozaru tiesību aktiem. Publiskas iestādes, kuras nodod ekspluatācijā augsta riska MI sistēmu pašu lietošanai, var pieņemt un īstenot kvalitātes vadības sistēmas noteikumus valsts vai reģionālā līmenī pieņemtas kvalitātes vadības sistēmas ietvaros, attiecīgi ņemot vērā nozares īpatnības un attiecīgās publiskās iestādes kompetences un struktūru.
- (82) Lai nodrošinātu šīs regulas izpildi un radītu vienlīdzīgus konkurences apstākļus operatoriem un ņemot vērā dažādos veidus, kā digitālos produktus var darīt pieejamus, ir svarīgi nodrošināt, ka Savienībā iedibināta persona jebkuros apstākļos var iestādēm sniegt visu nepieciešamo informāciju par MI sistēmas atbilstību. Tāpēc nodrošinātājiem, kas iedibināti trešās valstīs, pirms savas MI sistēmas dara pieejamas Savienībā, ar rakstisku pilnvaru būtu jāieceļ Savienībā iedibinātu pilnvarotu pārstāvi. Šim pilnvarotajam pārstāvim ir būtiska loma tādu augsta riska MI sistēmu atbilstības nodrošināšanā, kuras Savienībā laiž tirgū vai nodod ekspluatācijā nodrošinātāji, kas nav iedibināti Savienībā, un tas darbojas kā šo nodrošinātāju kontaktpersona, kas iedibināta Savienībā.
- (83) Ņemot vērā MI sistēmu vērtības ķēdes raksturu un sarežģītību un saskaņā ar Jauno tiesisko regulējumu, ir būtiski nodrošināt juridisko noteiktību un veicināt atbilstību šai regulai. Tāpēc ir jāprecizē to attiecīgo operatoru, piemēram, importētāju un izplatītāju, loma un konkrētie pienākumi visā vērtības ķēdē, kuri var veicināt MI sistēmu izstrādi. Dažās situācijās minētie operatori varētu vienlaikus pildīt vairāk nekā vienu funkciju, un tāpēc tiem būtu kumulatīvi jāizpilda visi attiecīgie pienākumi, kas saistīti ar minētajām funkcijām. Piemēram, operators varētu darboties vienlaikus kā izplatītājs un importētājs.
- (84) Lai nodrošinātu juridisko noteiktību, ir jāprecizē, ka saskaņā ar dažiem konkrētiem nosacījumiem jebkurš uzturētājs, importētājs, ieviešējs vai cita trešā persona būtu jāuzskata par augsta riska MI sistēmas nodrošinātāju un tādēļ tam būtu jāuzņemas visi attiecīgie pienākumi. Tā tas būtu gadījumā, ja minētā persona uzliek savu nosaukumu/vārdu vai preču zīmi augsta riska MI sistēmai, kas jau ir laista tirgū vai nodota ekspluatācijā, neskarot līgumiskas vienošanās, kas paredz, ka pienākumi tiek sadalīti citādi. Tā tas būtu arī gadījumā, ja minētā persona veic būtisku modifikāciju augsta riska MI sistēmā, kura jau ir laista tirgū vai jau ir nodota ekspluatācijā, tādā veidā, ka tā joprojām paliek augsta riska MI sistēma, ievērojot šo regulu, vai ja tā veic modifikāciju MI sistēmai paredzētajā nolūkā, tostarp vispārīga lietojuma MI sistēmai, kas nav klasificēta kā augsta riska sistēma un kas jau ir laista tirgū vai nodota ekspluatācijā, tādā veidā, ka attiecīgā MI sistēma kļūst par augsta riska MI sistēmu saskaņā ar šo regulu. Minētie noteikumi būtu jāpiemēro, neskarot konkrētākus noteikumus, kas paredzēti dažos Savienības saskaņošanas tiesību aktos, kuru pamatā ir Jaunais tiesiskais regulējums, kopā ar kuru būtu jāpiemēro šī regula. Piemēram, Regulas (ES) 2017/745

⁽³⁸⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/2102 (2016. gada 26. oktobris) par publiskā sektora struktūru tīmekļvietņu un mobilo lietotņu piekļūstamību (OV L 327, 2.12.2016., 1. lpp.).

16. panta 2. punktu, kurā noteikts, ka dažas izmaiņas nebūtu jāuzskata par tādām ierīces modifikācijām, kas varētu ietekmēt tās atbilstību piemērojamajām prasībām, būtu jāturpina piemērot augsta riska MI sistēmām, kuras ir medicīniskas ierīces minētās regulas nozīmē.

- (85) Vispārīga lietojuma MI sistēmas var lietot kā augsta riska MI sistēmas pašas par sevi vai kā citu augsta riska MI sistēmu sastāvdaļas. Tāpēc, ņemot vērā šādu sistēmu īpašo raksturu un lai nodrošinātu taisnīgu atbildības sadali visā MI vērtības ķēdē, šādu sistēmu nodrošinātājiem – neatkarīgi no tā, vai citi nodrošinātāji tās var lietot kā augsta riska MI sistēmas pašas par sevi vai kā augsta riska MI sistēmu sastāvdaļas, un ja šajā regulā nav noteikts citādi, – būtu cieši jāsadarbojas ar attiecīgo augsta riska MI sistēmu nodrošinātājiem, lai nodrošinātu atbilstību attiecīgajiem šajā regulā noteiktajiem pienākumiem, un ar kompetentajām iestādēm, kas izveidotas šajā regulā.
- (86) Ja saskaņā ar šajā regulā paredzētajiem nosacījumiem nodrošinātājs, kas sākotnēji laidis tirgū vai nodevis ekspluatācijā MI sistēmu, vairs nebūtu uzskatāms par nodrošinātāju šīs regulas nozīmē un ja minētais nodrošinātājs nav skaidri izslēdzis MI sistēmas pārveidošanu par augsta riska MI sistēmu, iepriekšējam nodrošinātājam tomēr būtu cieši jāsadarbojas un jādara pieejama nepieciešamā informācija, un jāsniedz saprātīgi sagaidāma tehniskā piekļuve un cita palīdzība, kas vajadzīga šajā regulā noteikto pienākumu izpildei, jo īpaši attiecībā uz atbilstību augsta riska MI sistēmu atbilstības novērtējumam.
- (87) Turklāt, ja augsta riska MI sistēma, kas ir drošības sastāvdaļa kādā produktā, uz kuru attiecas Jaunajā tiesiskajā regulējumā balstīto Savienības saskaņošanas tiesību aktu piemērošanas joma, nav laista tirgū vai nodota ekspluatācijā neatkarīgi no produkta, produkta ražotājam, kas definēts minētajos tiesību aktos, būtu jāizpilda šajā regulā noteiktie nodrošinātāja pienākumi un jo īpaši būtu jānodrošina, ka gatavajā produktā iegultā MI sistēma atbilst šīs regulas prasībām.
- (88) MI vērtības ķēdē daudzas puses bieži piegādā MI sistēmas, rīkus un pakalpojumus, bet arī sastāvdaļas vai procesus, ko nodrošinātājs integrē MI sistēmā ar dažādiem mērķiem, tostarp saistībā ar modeļu apmācību, modeļu pārmācību, modeļu testēšanu un izvērtēšanu, integrēšanu programmatūrā vai citiem modeļu izstrādes aspektiem. Minētajām pusēm ir svarīga loma vērtības ķēdē attiecībā uz tādās augsta riska MI sistēmas nodrošinātāju, kurā ir integrētas to MI sistēmas, rīki, pakalpojumi, sastāvdaļas vai procesi, un tām ar rakstisku piekrišanu būtu jāsniedz šim nodrošinātājam nepieciešamā informācija, spējas, tehniskā piekļuve un cita palīdzība, pamatojoties uz vispārārstītiem jaunākajiem sasniegumiem, lai nodrošinātājs varētu pilnībā izpildīt šajā regulā noteiktos pienākumus, neskarot savas intelektuālā īpašuma tiesības vai komercnoslēpumus.
- (89) Trešām personām, kas dara piekļūstamus publiskus rīkus, pakalpojumus, procesus vai MI sastāvdaļas, kas nav vispārīga lietojuma MI modeļi, nevajadzētu būt pienākumam izpildīt prasības, kas vērstas uz pienākumiem MI vērtības ķēdē, jo īpaši pret nodrošinātāju, kurš tos ir izmantojis vai integrējis, ja minētie rīki, pakalpojumi, procesi vai MI sastāvdaļas tiek darīti piekļūstami saskaņā ar bezmaksas un atvērta piekļuves licenci. Brīvā un atvērtā pirmkoda rīku, pakalpojumu, procesu vai MI sastāvdaļu, kas nav vispārīga lietojuma MI modeļi, izstrādātāji būtu jāmodina īstenot plaši pieņemtu dokumentēšanas praksi, piemēram, modeļu kartes un datu lapas, lai paātrinātu informācijas apmaiņu visā MI vērtības ķēdē, ļaujot veicināt uzticamas MI sistēmas Savienībā.
- (90) Komisija varētu izstrādāt un ieteikt brīvprātīgus līguma paraugnoteikumus starp augsta riska MI sistēmu nodrošinātājiem un trešām personām, kuras piegādā rīkus, pakalpojumus, sastāvdaļas vai procesus, ko izmanto vai integrē augsta riska MI sistēmās, lai veicinātu sadarbību vērtības ķēdē. Izstrādājot brīvprātīgus līguma paraugnoteikumus, Komisijai būtu arī jāņem vērā iespējamās līgumiskās prasības, kas piemērojamas konkrētās nozarēs vai uzņēmējdarbības gadījumos.
- (91) Ņemot vērā MI sistēmu raksturu un iespējamās riskus drošībai un pamattiesībām, kas saistīti ar to lietošanu, tostarp attiecībā uz nepieciešamību nodrošināt MI sistēmas veiktspējas reālos apstākļos pienācīgu pārraudzību, ir lietderīgi noteikt konkrētus pienākumus uzturētājiem. Uzturētājiem būtu jo īpaši jāveic pienācīgi tehniski un organizatoriski pasākumi, lai nodrošinātu, ka augsta riska MI sistēmas tie lieto saskaņā ar lietošanas instrukcijām, un būtu jānosaka daži citi pienākumi attiecībā uz MI sistēmu funkcionēšanas pārraudzību un uzskaiti vajadzības gadījumā. Turklāt

uzturētājiem būtu jānodrošina, ka personām, kurām uzdots īstenot šajā regulā noteiktās lietošanas instrukcijas un cilvēka virsvadību, ir vajadzīgā kompetence, jo īpaši pienācīga līmeņa MI pratība, apmācība un pilnvaras minēto uzdevumu pienācīgai izpildei. Minētajiem pienākumiem nebūtu jāskar citi uzturētāja pienākumi attiecībā uz augsta riska MI sistēmām saskaņā ar Savienības vai valsts tiesību aktiem.

- (92) Šī regula neskar darba devēju pienākumus informēt darba ņēmējus vai informēt un uzklaut darba ņēmējus vai viņu pārstāvjus saskaņā ar Savienības vai valsts tiesību aktiem un praksi, tostarp Eiropas Parlamenta un Padomes Direktīvu 2002/14/EK⁽³⁹⁾, par lēmumiem nodot ekspluatācijā vai izmantot MI sistēmas. Joprojām ir nepieciešams nodrošināt darba ņēmēju un viņu pārstāvju informēšanu par augsta riska MI sistēmu plānoto ieviešanu darbavietā, ja nav izpildīti citos juridiskajos instrumentos paredzētie nosacījumi attiecībā uz minēto informāciju vai informēšanas un uzklautāšanas pienākumiem. Turklāt šādas tiesības uz informāciju ir papildinošas un nepieciešamas, lai sasniegtu mērķi aizsargāt pamattiesības, kas ir šīs regulas pamatā. Tāpēc šajā regulā būtu jānosaka informēšanas prasība, neskarot darba ņēmēju spēkā esošās tiesības.
- (93) Lai gan riski, kas saistīti ar MI sistēmām, var rasties no šādu sistēmu uzbūves, riskus var radīt arī veids, kā šādas MI sistēmas tiek lietotas. Tāpēc augsta riska MI sistēmas uzturētājiem ir būtiska nozīme pamattiesību aizsardzības nodrošināšanā, papildinot nodrošinātāja pienākumus MI sistēmu izstrādē. Uzturētājiem ir vislabākās iespējas izprast, kā tieši tiks lietota augsta riska MI sistēma, un tādēļ, pateicoties precīzākām zināšanām par lietošanas kontekstu, personām vai personu grupām, kuras varētu tikt skartas, tostarp neaizsargātām grupām, tie var identificēt iespējamus būtiskos riskus, kas nebija paredzēti izstrādes posmā. Šīs regulas pielikumā uzskaitīto augsta riska MI sistēmu uzturētājiem ir arī būtiska loma fizisku personu informēšanā, un, pieņemot lēmumus vai palīdzot pieņemt lēmumus saistībā ar fiziskām personām, tiem attiecīgā gadījumā būtu jāinformē fiziskās personas par to, ka uz tām attiecas augsta riska MI sistēmas lietošana. Šai informācijai būtu jāietver paredzētais nolūks un pieņemto lēmumu veids. Uzturētājam būtu arī jāinformē fiziskās personas par to šajā regulā paredzētajām tiesībām saņemt paskaidrojumu. Attiecībā uz augsta riska MI sistēmām, ko lieto tiesībaizsardzības nolūkos, minētais pienākums būtu jāīsteno saskaņā ar Direktīvas (ES) 2016/680 13. pantu.
- (94) Jebkādai biometrisku datu apstrādei, kas saistīta ar MI sistēmu lietošanu biometriskajai identifikācijai tiesībaizsardzības nolūkos, ir jāatbilst Direktīvas (ES) 2016/680 10. pantam, kas atļauj šādu apstrādi tikai tad, ja tas ir absolūti nepieciešams, uz to attiecas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām un ja tas ir atļauts Savienības vai dalībvalsts tiesībās. Šādā lietošanā, ja tā ir atļauta, ir jāievēro arī Direktīvas (ES) 2016/680 4. panta 1. punktā noteiktie principi, tostarp likumība, godprātība un pārredzamība, mērķa ierobežojums, precizitāte un glabāšanas ierobežojums.
- (95) Neskarot piemērojamos Savienības tiesību aktus, jo īpaši Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680, tā kā vēlāklaika biometriskās tālidentifikācijas sistēmas pēc būtības ir aizskarošas, vēlāklaika biometriskās tālidentifikācijas sistēmu lietošanai būtu jāpiemēro aizsardzības pasākumi. Vēlāklaika biometriskās tālidentifikācijas sistēmas vienmēr būtu jālieto samērīgi, legītimi un tad, ja tas ir absolūti nepieciešams, un tādējādi tās būtu jāorientē uz identificējamām personām, atrašanās vietu, darbības laiku un pamatojoties uz slēgtu datu kopu, ko veido likumīgi iegūti videomateriāli. Jebkurā gadījumā vēlāklaika biometriskās tālidentifikācijas sistēmas nebūtu jālieto tiesībaizsardzības sistēmā, kas radītu nediferencētu uzraudzību. Vēlāklaika biometriskās tālidentifikācijas nosacījumiem nekādā gadījumā nevajadzētu būt par pamatu, lai apietu aizlieguma nosacījumus un stingrus izņēmumus attiecībā uz reāllaika biometrisku tālidentifikāciju.
- (96) Lai efektīvi nodrošinātu pamattiesību aizsardzību, augsta riska MI sistēmu uzturētājiem, kas ir publisko tiesību subjekti, vai privātām vienībām, kas sniedz sabiedriskos pakalpojumus, un konkrētu šīs regulas pielikumā uzskaitītu augsta riska MI sistēmu uzturētājiem, piemēram, banku vai apdrošināšanas vienībām, pirms nodošanas ekspluatācijā būtu jāveic novērtējums par ietekmi uz pamattiesībām. Sabiedriska rakstura pakalpojumus, kas ir svarīgi privātpersonām, var sniegt arī privātas vienības. Privātas vienības, kas sniedz šādus sabiedriskus pakalpojumus, ir saistīti ar uzdevumiem sabiedrības interesēs, piemēram, izglītības, veselības aprūpes, sociālo pakalpojumu, mājokļa, tiesvedības jomā. Novērtējuma par ietekmi uz pamattiesībām mērķis ir panākt, lai uzturētājs identificētu konkrētos riskus to personu vai personu grupu tiesībām, kas varētu tikt skartas, un identificētu pasākumus, kas jāveic minētā

⁽³⁹⁾ Eiropas Parlamenta un Padomes Direktīva 2002/14/EK (2002. gada 11. marts), ar ko izveido vispārēju sistēmu darbinieku informēšanai un uzklautāšanai Eiropas (OV L 80, 23.3.2002., 29. lpp.).

riska iestāšanās gadījumā. Ietekmes novērtējums būtu jāpiemēro augsta riska MI sistēmas pirmajai lietošanai, un tas būtu jāatjaunina, ja uzturētājs uzskata, ka kāds no būtiskajiem faktoriem ir mainījies. Ietekmes novērtējumā būtu jāidentificē uzturētāja attiecīgie procesi, kuros augsta riska MI sistēma tiks lietota saskaņā ar tai paredzēto nolūku, un tajā būtu jāietver apraksts par sistēmas paredzētās lietošanas laikposmu un biežumu, kā arī par konkrētām fizisku personu un grupu kategorijām, kuras varētu tikt skartas konkrētajā lietošanas kontekstā. Novērtējumā būtu arī jāidentificē konkrēti kaitējuma riski, kas varētu ietekmēt minēto personu vai grupu pamattiesības. Veicot šo novērtējumu, uzturētājam būtu jāņem vērā informācija, kas ir būtiska ietekmes pienācīgam novērtējumam, tostarp, bet ne tikai, informācija, ko augsta riska MI sistēmas nodrošinātājs sniedzis lietošanas instrukcijā. Ņemot vērā identificētos riskus, uzturētājiem būtu jānosaka pasākumi, kas jāveic minēto risku iestāšanās gadījumā, tostarp, piemēram, pārvaldības kārtība konkrētajā lietošanas kontekstā, piemēram, cilvēka virsvadības kārtība saskaņā ar lietošanas instrukciju, vai sūdzību izskatīšanas un tiesiskās aizsardzības procedūras, jo tās varētu būt noderīgas risku pamattiesībām mazināšanā konkrētos lietošanas gadījumos. Pēc minētā ietekmes novērtējuma veikšanas uzturētājam par to būtu jāpaziņo attiecīgajai tirgus uzraudzības iestādei. Attiecīgā gadījumā, lai vāktu attiecīgo informāciju, kas nepieciešama ietekmes novērtējuma veikšanai, augsta riska MI sistēmas uzturētāji, jo īpaši tad, ja MI sistēmas izmanto publiskajā sektorā, varētu iesaistīt attiecīgās ieinteresētās personas, tostarp to personu grupu pārstāvjus, kuras MI sistēma varētu skart, neatkarīgus ekspertus un pilsoniskās sabiedrības organizācijas šādu ietekmes novērtējumu veikšanā un tādu pasākumu izstrādē, kas jāveic risku iestāšanās gadījumā. Eiropas Mākslīgā intelekta birojam (MI birojs) būtu jāizstrādā anketas veidne, lai atvieglotu atbilstību un samazinātu administratīvo slogu uzturētājiem.

- (97) Lai nodrošinātu juridisko noteiktību, vispārīga lietojuma MI modeļu jēdziens būtu skaidri jādefinē un jānošķir no MI sistēmu jēdziena. Definīcijas pamatā vajadzētu būt vispārīga lietojuma MI modeļa galvenajām funkcionālajām iezīmēm, jo īpaši vispārīgumam un spējai kompetenti veikt plašu atšķirīgu uzdevumu klāstu. Šie modeļi parasti tiek apmācīti par lielu datu apjomu, izmantojot dažādas metodes, piemēram, pašuzraudzītu, neuzraudzītu vai stimulētu mācīšanos. Vispārīga lietojuma MI modeļus var laist tirgū dažādos veidos, tostarp ar bibliotēku, lietojumprogrammu saskarpi (API) starpniecību, kā tiešu lejupielādi vai kā fizisku kopiju. Šos modeļus var vēl vairāk modificēt vai pilnveidot, pārveidojot par jauniem modeļiem. Lai gan MI modeļi ir būtiskas MI sistēmu sastāvdaļas, tie paši par sevi nav MI sistēmas. MI modeļiem – lai tie kļūtu par MI sistēmām – ir jāpievieno vēl citas sastāvdaļas, piemēram, lietotāja saskarne. MI modeļi parasti ir integrēti MI sistēmās un ir to daļa. Šī regula paredz tāds konkrēts noteikums vispārīga lietojuma MI modeļiem un vispārīga lietojuma MI modeļiem, kuri rada sistēmiskus riskus, kas būtu jāpiemēro arī tad, ja šie modeļi ir integrēti vai daļa no MI sistēmas. Būtu jāsaprot, ka vispārīga lietojuma MI modeļu nodrošinātāju pienākumi būtu jāpiemēro tad, kad vispārīga lietojuma MI modeļi ir laisti tirgū. Ja vispārīga lietojuma MI modeļa nodrošinātājs integrē savu modeli savā MI sistēmā, kas ir darīta pieejama tirgū vai nodota ekspluatācijā, būtu jāuzskata, ka minētais modelis ir laists tirgū, un tāpēc šajā regulā noteiktie pienākumi attiecībā uz modeļiem būtu jāturpina piemērot papildus tiem, kas attiecas uz MI sistēmām. Jebkurā gadījumā modeļiem paredzētie pienākumi nebūtu jāpiemēro, ja savu modeli izmanto tikai iekšējiem procesiem, kas nav būtiski produkta vai pakalpojuma piedāvāšanai trešām personām, un netiek skartas fizisku personu tiesības. Ņemot vērā to iespējamo būtiski negatīvo ietekmi, uz vispārīga lietojuma MI modeļiem ar sistēmisku risku vienmēr būtu jāattiecinā attiecīgie šajā regulā paredzētie pienākumi. Definīcijai nebūtu jāattiecas uz MI modeļiem, ko pirms to laišanas tirgū izmanto vienīgi pētniecības, izstrādes un prototipu izstrādes darbību vajadzībām. Tas neskar pienākumu ievērot šo regulu, ja pēc šādām darbībām modelis tiek laists tirgū.
- (98) Tā kā modeļa vispārīgumu cita starpā varētu noteikt arī ar vairākiem parametriem, būtu jāuzskata, ka modeļi, kam ir vismaz miljards parametru un kas ir apmācīti ar lielu datu apjomu, izmantojot pašuzraudzību plašā mērogā, uzrāda būtisku vispārīgumu un ir kompetenti veikt plašu atšķirīgu uzdevumu klāstu.
- (99) Lieli ģeneratīvi MI modeļi ir tipisks vispārīga lietojuma MI piemērs, ņemot vērā, ka tie ļauj elastīgi radīt saturu, piemēram, teksta, audio, attēlu vai video formātā, kas var viegli veikt plašu atšķirīgu uzdevumu klāstu.
- (100) Ja vispārīga lietojuma MI modelis ir integrēts MI sistēmā vai ir tās daļa, šī sistēma būtu jāuzskata par vispārīga lietojuma MI sistēmu, ja šīs integrācijas dēļ šī sistēma spēj kalpot dažādiem nolūkiem. Vispārīga lietojuma MI sistēmu var lietot tieši vai integrēt citās MI sistēmās.

- (101) Vispārīga lietojuma MI modeļu nodrošinātājiem ir īpaša loma un atbildība visā MI vērtības ķēdē, jo to nodrošinātie modeļi var veidot pamatu virknei lejasposma sistēmu, ko bieži nodrošina lejasposma nodrošinātāji, kuriem ir vajadzīga laba izpratne par modeļiem un to spējām, lai tie šādus modeļus varētu integrēt savos produktos un arī lai varētu izpildīt savus šajā vai citās regulās noteiktos pienākumus. Tāpēc būtu jānosaka samērīgi pārredzamības pasākumi, tostarp dokumentācijas izstrāde un atjaunināšana un informācijas sniegšana par vispārīga lietojuma MI modeļiem, lai to varētu izmantot lejasposma nodrošinātāji. Vispārīga lietojuma MI modeļa nodrošinātājam būtu jā sagatavo un jāatjaunina tehniskā dokumentācija, lai to pēc pieprasījuma darītu pieejamu MI birojam un valstu kompetentajām iestādēm. Minimālais elementu kopums, kas jāiekļauj šādā dokumentācijā, būtu jānosaka konkrētos šīs regulas pielikumos. Komisija būtu jāpilnvaro grozīt minētos pielikumus ar deleģētajiem aktiem, ņemot vērā tehnoloģiju attīstību.
- (102) Programmatūra un dati, tostarp modeļi, kas tiek laisti apgrozībā ar bezmaksas un atvērtā pirmkoda licenci, kas ļauj tos atklāti kopīgot un saskaņā ar ko lietotāji var brīvi piekļūt tiem vai to modificētām versijām, tos lietot, modificēt un pārdalīt, var veicināt pētniecību un inovāciju tirgū un sniegt ievērojamas izaugsmes iespējas Savienības ekonomikai. Būtu jānosaka, ka vispārīga lietojuma MI modeļi, kas tiek laisti apgrozībā ar bezmaksas un atvērtā pirmkoda licencēm, nodrošina augstu pārredzamības un atvērtības līmeni, ja to parametri, tostarp svāri, informācija par modeļa arhitektūru un informācija par modeļu lietošanu ir darīti publiski pieejami. Licence būtu jānosaka par brīvu un atvērtu pirmavotu arī tad, ja tā ļauj lietotājiem vadīt, kopēt, izplatīt, pētīt, mainīt un uzlabot programmatūru un datus, tostarp modeļus, ar nosacījumu, ka tiek atzīts modeļa sākotnējais nodrošinātājs un tiek ievēroti identiski vai salīdzināmi izplatīšanas noteikumi.
- (103) Bezmaksas un atvērtā pirmkoda MI sastāvdaļas aptver MI sistēmas programmatūru un datus, tostarp modeļus un vispārīga lietojuma MI modeļus, rīkus, pakalpojumus vai procesus. Bezmaksas un atvērtā pirmkoda MI sastāvdaļas var nodrošināt, izmantojot dažādus kanālus, tostarp to izstrādi atvērtos repozitorijos. Šajā regulā MI sastāvdaļām, kas tiek nodrošinātas par noteiktu cenu vai citādi monetizētas, tostarp, sniedzot tehnisko atbalstu vai citus pakalpojumus, tostarp, izmantojot programmatūras platformu, kas saistīta ar MI sastāvdaļu, vai izmantojot personas datu citu iemeslu dēļ, nevis tikai programmatūras drošības, saderības vai sadarbības uzlabošanai, izņemot darījumus starp mikrouzņēmumiem, nebūtu jāgūst labums no uzņēmumiem, kas paredzēti bezmaksas un atvērtā pirmkoda MI sastāvdaļām. Tas, ka MI sastāvdaļas tiek darītas pieejamas, izmantojot atvērtos repozitorijos, pats par sevi nebūtu jānosaka par monetizāciju.
- (104) Tādu vispārīga lietojuma MI modeļu nodrošinātājiem, kuri tiek laisti apgrozībā ar bezmaksas un atvērtā pirmkoda licenci un kuru parametri, tostarp svāri, informācija par modeļa arhitektūru un informācija par modeļu lietošanu, ir darīti publiski pieejami, būtu jāpiemēro uzņēmumi attiecībā uz prasībām, kas saistītas ar pārredzamību un kas noteiktas vispārīga lietojuma MI modeļiem, izņemot gadījumus, kad tos var uzskatīt par tādiem, kas rada sistēmisku risku, un tādā gadījumā apstāklis, ka modelis ir pārredzams un tam ir pievienota atvērtā pirmkoda licence, nebūtu jānosaka par pietiekamu iemeslu, lai izslēgtu atbilstību šajā regulā noteiktajiem pienākumiem. Jebkurā gadījumā, ņemot vērā to, ka vispārīga lietojuma MI modeļu laišana apgrozībā ar bezmaksas un atvērtā pirmkoda licenci ne vienmēr atklāj būtisku informāciju par modeļa apmācībai vai pilnveidošanai izmantoto datu kopu un par to, kā šajā procesā tika nodrošināta atbilstība tiesību aktiem autortiesību jomā, vispārīga lietojuma MI modeļiem paredzētajam uzņēmumam attiecībā uz atbilstību ar pārredzamību saistītajām prasībām nebūtu jāattiecas uz pienākumu sagatavot kopsavilkumu par saturu, ko izmanto modeļu apmācībā, un pienākumu ieviest politiku, ar ko nodrošina atbilstību Savienības tiesību aktiem autortiesību jomā, jo īpaši, lai identificētu un nodrošinātu tiesību rezervāciju, ievērojot Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/790⁽⁴⁰⁾ 4. panta 3. punktu.
- (105) Vispārīga lietojuma modeļi, jo īpaši lieli ģeneratīvi modeļi, kas spēj ģenerēt tekstu, attēlus un citu saturu, sniedz unikālas inovācijas iespējas, taču arī rada izaicinājumus māksliniekiem, autoriem un citiem satura veidotājiem un tam, kā tiek radīts, izplatīts, lietots un patērēts radošais saturs. Šādu modeļu izstrādei un apmācībai ir vajadzīga piekļuve liela teksta, attēlu, video un citu datu apjomam. Tekstizrašanas un datizrašanas metodes šajā kontekstā var plaši izmantot, lai izgūtu un analizētu šādu saturu, ko var aizsargāt autortiesības un blakustiesības. Jebkādai ar autortiesībām aizsargāta satura izmantošanai ir vajadzīga attiecīgā tiesību subjekta atļauja, ja vien netiek piemēroti attiecīgie autortiesību izņēmumi un ierobežojumi. Ar Direktīvu (ES) 2019/790 tika ieviesti izņēmumi un ierobežojumi, kas pieļauj – ar konkrētiem nosacījumiem – reproducēšanu un ekstrahēšanu attiecībā uz darbiem vai

⁽⁴⁰⁾ Eiropas Parlamenta un Padomes Regula (ES) 2019/790 (2019. gada 17. aprīlis) par autortiesībām un blakustiesībām digitālajā vienotajā tirgū un ar ko groza Direktīvas 96/9/EK un 2001/29/EK (OV L 130, 17.5.2019., 92. lpp.).

citiem blakustiesību objektiem tekstizraces un datizraces nolūkā. Saskaņā ar šiem noteikumiem tiesību subjekti var izvēlēties rezervēt tiesības uz saviem darbiem vai citiem blakustiesību objektiem, lai nepieļautu tekstizraci un datizraci, ja vien tas netiek darīts zinātniskās pētniecības nolūkos. Ja tiesības atteiktas ir skaidri rezervētas piemērotā veidā, vispārīga lietojuma MI modeļu nodrošinātājiem ir jāsaņem atļauja no tiesību subjektiem, ja tie vēlas veikt tekstizraci un datizraci šādos darbos.

- (106) Nodrošinātājiem, kas Savienības tirgū laiž vispārīga lietojuma MI modeļus, būtu jānodrošina atbilstība attiecīgajiem šajā regulā noteiktajiem pienākumiem. Šajā nolūkā vispārīga lietojuma MI modeļu nodrošinātājiem būtu jāievieš politika, lai nodrošinātu atbilstību Savienības tiesību aktiem autortiesību un blakustiesību jomā, jo īpaši, lai identificētu un ievērotu tiesību rezervācijas, ko pauduši tiesību subjekti, ievērojot Direktīvas (ES) 2019/790 4. panta 3. punktu. Jebkuram nodrošinātājam, kas Savienības tirgū laiž vispārīga lietojuma MI modeli, šis pienākums būtu jāievēro neatkarīgi no jurisdikcijas, kurā notiek ar autortiesībām saistītās darbības, kas ir minēto vispārīga lietojuma MI modeļu apmācības pamatā. Tas ir nepieciešams, lai nodrošinātu vienlīdzīgus konkurences apstākļus vispārīga lietojuma MI modeļu nodrošinātājiem, proti, nevienam nodrošinātājam nevajadzētu spēt gūt konkurences priekšrocības Savienības tirgū, piemērojot zemākus autortiesību standartus nekā Savienībā noteiktie.
- (107) Lai palielinātu pārredzamību attiecībā uz datiem, ko izmanto vispārīga lietojuma MI modeļu iepriekšējā apmācībā un apmācībā, tostarp attiecībā uz tekstu un datiem, ko aizsargā tiesību akti autortiesību jomā, ir piemēroti, ka šādu modeļu nodrošinātāji izstrādā un dara publiski pieejamu pietiekami detalizētu kopsavilkumu par saturu, ko izmanto vispārīga lietojuma MI modeļa apmācībā. Pienācīgi ņemot vērā nepieciešamību aizsargāt komercnoslēpumus un konfidencialu uzņēmējdarbības informāciju, šā kopsavilkuma tvērumam vajadzētu būt kopumā visaptverošam, nevis tehniski detalizētam, lai pusēm ar leģitīmām interesēm, tostarp autortiesību īpašniekiem, atvieglotu savu Savienības tiesību aktos paredzēto tiesību izmantošanu un īstenošanu, piemēram, uzskaitot galvenos modeļa apmācībā izmantotos datu apkopojumus vai datu kopas, piemēram, lielas privātas vai publiskas datubāzes vai datu arhīvi, un sniedzot aprakstošu skaidrojumu par citiem izmantotajiem datu avotiem. Ir lietderīgi, ka MI birojs nodrošina kopsavilkuma veidni, kam vajadzētu būt vienkāršam un efektīvam un kas ļautu nodrošinātājam sniegt prasīto kopsavilkumu aprakstošā veidā.
- (108) Attiecībā uz vispārīga lietojuma MI modeļu nodrošinātājiem uzliktajiem pienākumiem ieviest politiku, ar ko nodrošina atbilstību Savienības tiesību aktiem autortiesību jomā, un darīt publiski pieejamu apmācībā izmantotā satura kopsavilkumu MI birojam būtu jāpārtrauga, vai nodrošinātājs ir izpildījis minētos pienākumus, neveicot pārbaudi vai nevērtējot apmācības datus par katru atsevišķu darbu attiecībā uz atbilstību tiesību aktiem autortiesību jomā. Šī regula neietekmē Savienības tiesību aktos paredzēto noteikumu autortiesību jomā izpildi.
- (109) Vispārīga lietojuma MI modeļu nodrošinātājiem piemērojamo pienākumu izpildei vajadzētu būt samērīgai un proporcionālai modeļa nodrošinātāja veidam, izņemot nepieciešamību atbilstību nodrošināt personām, kuras izstrādā vai lieto modeļus neprofesionālos vai zinātniskās pētniecības nolūkos, bet kuras tomēr būtu jānodrošina brīvprātīgi ievērot šīs prasības. Neskarot Savienības tiesību aktus autortiesību jomā, minēto pienākumu izpildē būtu pienācīgi jāņem vērā nodrošinātāja lielums un jāļauj MVU, tostarp jaunuzņēmumiem, izmantot vienkāršotus atbilstības nodrošināšanas veidus, kuriem nebūtu jārada pārmērīgas izmaksas un jāattur no šādu modeļu izmantošanas. Modeļa modifikācijas vai pilnveidošanas gadījumā vispārīga lietojuma MI modeļu nodrošinātāju pienākumi būtu jāattiecinā tikai uz minēto modifikāciju vai pilnveidošanu, piemēram, papildinot jau esošo tehnisko dokumentāciju ar informāciju par modifikācijām, tostarp jauniem apmācības datu avotiem, lai izpildītu šajā regulā noteiktos pienākumus saistībā ar vērtības ķēdi.
- (110) Vispārīga lietojuma MI modeļi varētu radīt sistēmiskus riskus, kas cita starpā ietver jebkādu faktisku vai pamatoti paredzamu negatīvu ietekmi saistībā ar smagiem negadījumiem, kritisko nozaru darbības traucējumiem un nopietnām sekām sabiedrības veselībai un drošībai; jebkādu faktisku vai pamatoti paredzamu negatīvu ietekmi uz demokrātiskajiem procesiem, sabiedrības un ekonomikas drošību; nelikumīga, nepatiesa vai diskriminējoša satura izplatīšanu. Sistēmiskie riski būtu jāsaprot kā tādi, kas palielinās līdz ar modeļa spējam un modeļa tvērumu, var rasties visā modeļa dzīves ciklā un ko ietekmē ļaunprātīgas izmantošanas apstākļi, modeļa uzticamība, modeļa taisnīgums un modeļa drošība, modeļa autonomijas pakāpe, tā piekļuve rīkiem, nebijušas vai kombinētas modalitātes, laišanas apgrozībā un izplatīšanas stratēģijas, aizsargmehānismu likvidēšanas potenciāls un citi faktori. Jo īpaši starptautiskajās pieejās līdz šim ir konstatēta vajadzība pievērst uzmanību riskiem, ko rada potenciāli tīša ļaunprātīga izmantošana vai neparedzētas kontroles problēmas saistībā ar saskaņošanu ar cilvēka nolūku; ķīmiskiem, bioloģiskiem, radioloģiskiem riskiem un kodolriskiem, piemēram, veidiem, kā samazināt iekļūšanas šķēršļus, tostarp

attiecībā uz ieroču izstrādi, projektēšanu iegādi vai izmantošanu; ofensīvām kiberspējām, piemēram, neaizsargātības atklāšanas, izmantošanas vai operatīvas izmantošanas veidiem; rīku mijiedarbības un izmantošanas ietekmei, tostarp, piemēram, spējai kontrolēt fiziskās sistēmas un ietekmēt kritisko infrastruktūru; riskiem, ko rada modeļi, kas paši sevi kopē, ir "pašreplīcējoši" vai apmāca citus modeļus; veidiem, kā modeļi var veicināt kaitējošus aizspriedumus un diskrimināciju, rados riskus personām, kopienām vai sabiedrībai; dezinformācijas veicināšanai vai privātuma aizskārumiem, kas apdraud demokrātiskās vērtības un cilvēktiesības; riskam, ka konkrēts notikums varētu izraisīt ķēdes reakciju ar ievērojamu negatīvu ietekmi, kas varētu skart veselu pilsētu, veselās jomas darbību vai veselu kopienu.

- (111) Ir lietderīgi izveidot metodoloģiju vispārīga lietojuma MI modeļu klasificēšanai par vispārīga lietojuma MI modeļiem ar sistēmiskiem riskiem. Tā kā sistēmiskie riski izriet no īpaši augstām spējām, būtu jānoskaidro, ka vispārīga lietojuma MI modeļi rada sistēmiskus riskus, ja tam ir augstas ietekmes spējas, kas novērtētas, pamatojoties uz piemērotiem tehniskiem rīkiem un metodēm, vai būtiska ietekme uz iekšējo tirgu tā tvēruma dēļ. Augstas ietekmes spējas vispārīga lietojuma MI modeļos ir spējas, kas atbilst vai pārsniedz spējas, kuras ir iekļautas modernākajos vispārīga lietojuma MI modeļos. Visu modeļa spēju klāstu varētu labāk izprast pēc tā laišanas tirgū vai tad, kad uzturētāji mijiedarbojas ar modeli. Saskaņā ar jaunākajiem sasniegumiem šīs regulas spēkā stāšanās brīdī vispārīga lietojuma MI modeļa apmācībā izmantotais kumulatīvais skaitļošanas resursu apjoms, mērīts peldošā punkta operācijās, ir viens no attiecīgajiem modeļa spēju tuvināšanas faktoriem. Apmācībai izmantotais kumulatīvais skaitļošanas resursu apjoms ietver skaitļošanas resursus, ko izmanto visām darbībām, un metodes, kas paredzētas, lai uzlabotu modeļa spējas pirms ieviešanas, piemēram, iepriekšēju apmācību, sintētisko datu ģenerēšanu un pilnveidošanu. Tāpēc būtu jānosaka sākotnējā peldošā punkta operāciju robežvērtība, kas, ja to sasniedz ar vispārīga lietojuma MI modeli, rada pieņēmumu, ka modeļi ir vispārīga lietojuma MI modeļi ar sistēmiskiem riskiem. Šī robežvērtība laika gaitā būtu jāpielāgo, lai atspoguļotu tehnoloģiskās un rūpnieciskās pārmaiņas, piemēram, algoritmiskos uzlabojumus vai uzlabotu aparātūras efektivitāti, un tā būtu jāpapildina ar modeļa spējas kritērijiem un rādītājiem. Informācijas ieguves nolūkā MI birojam būtu jāsadarbojas ar zinātnieku aprindām, nozari, pilsonisko sabiedrību un citiem ekspertiem. Robežvērtībām, kā arī rīkiem un kritērijiem augstas ietekmes spēju novērtēšanai vajadzētu būt spēcīgiem vispārīguma, spēju un vispārīga lietojuma MI modeļu saistītā sistēmiskā riska prognozētājiem, un tajos varētu ņemt vērā veidu, kādā modeļi tiks laisti tirgū, vai to lietotāju skaitu, ko modeļi var ietekmēt. Lai papildinātu šo sistēmu, Komisijai vajadzētu būt iespējai pieņemt atsevišķus lēmumus, ar kuriem vispārīga lietojuma MI modeļi izraugās par vispārīga lietojuma MI modeļi ar sistēmisku risku, ja tiek konstatēts, ka šādam modeļim ir spējas vai ietekme, kas ir līdzvērtīga tām, kuras aptver noteiktā robežvērtība. Minētais lēmums būtu jāpieņem, pamatojoties uz tādu šīs regulas pielikumā izklāstīto vispārīga lietojuma MI modeļu ar sistēmisku risku izraudzīšanās kritēriju vispārēju novērtējumu kā, piemēram, apmācības datu kopas kvalitāte vai lielums, komerciālo lietotāju un galalietotāju skaits, to ievades un izvades modalitātes, autonomijas pakāpe un mērogojamība vai rīki, kuriem tiem ir piekļuve. Pēc nodrošinātāja, kura modeļi ir atzīti par vispārīga lietojuma MI modeļi ar sistēmisku risku, pamatota pieprasījuma Komisijai pieprasījums būtu jāņem vērā, un tā var lemt atkārtoti vērtēt, vai joprojām var uzskatīt, ka vispārīga lietojuma MI modeļi rada sistēmiskus riskus.
- (112) Ir arī jāprecizē vispārīga lietojuma MI modeļu ar sistēmiskiem riskiem klasificēšanas procedūra. Vispārīga lietojuma MI modeļi, kas atbilst piemērojamai robežvērtībai attiecībā uz augstas ietekmes spējām, būtu jānoskaidro par vispārīga lietojuma MI modeļi ar sistēmisku risku. Nodrošinātājam par to būtu jāpaziņo MI birojam ne vēlāk kā divas nedēļas pēc tam, kad ir izpildītas prasības vai kļūst zināms, ka vispārīga lietojuma MI modeļi atbildīs prasībām, kas ir pieņēmuma pamatā. Tas ir īpaši svarīgi attiecībā uz peldošā punkta operāciju robežvērtību, jo vispārīga lietojuma MI modeļu apmācībai ir vajadzīga ievērojama plānošana, kas ietver skaitļošanas resursu sākotnējo iedalīšanu, un tāpēc vispārīga lietojuma MI modeļu nodrošinātāji var zināt, vai viņu modeļi atbilstu robežvērtībai pirms apmācības pabeigšanas. Minētā paziņojuma kontekstā nodrošinātājam būtu jāspēj pierādīt, ka vispārīga lietojuma MI modeļi tā specifisko iezīmju dēļ izņēmuma kārtā nerada sistēmiskus riskus un ka tādējādi to nevajadzētu klasificēt kā vispārīga lietojuma MI modeļi ar sistēmiskiem riskiem. Minētā informācija ir MI birojam noderīga, lai prognozētu vispārīga

lietojuma MI modeļu ar sistēmiskiem riskiem laišanu tirgū, un nodrošinātāji jau agrīnā posmā var sākt sadarboties ar MI biroju. Minētā informācija ir īpaši svarīga attiecībā uz vispārīga lietojuma MI modeļiem, kurus plānots laist apgrozībā kā atvērtā pirmkoda modeļus, ņemot vērā to, ka pēc atvērtā pirmkoda modeļa laišanas apgrozībā var būt grūtāk īstenot pasākumus, kas vajadzīgi, lai nodrošinātu atbilstību šajā regulā paredzētajiem pienākumiem.

- (113) Ja Komisijai kļūst zināms, ka vispārīga lietojuma MI modelis atbilst prasībām, lai to klasificētu kā vispārīga lietojuma MI modeli ar sistēmisku risku, par ko iepriekš nebija zināms vai par ko attiecīgais nodrošinātājs nav paziņojis Komisijai, Komisijai vajadzētu būt pilnvarotai to noteikt par tādu. Kvalificētu brīdinājumu sistēmai būtu jānodrošina, ka zinātniskā grupa informē MI biroju par tādiem vispārīga lietojuma MI modeļiem, kas, iespējams, būtu jāklasificē kā vispārīga lietojuma MI modeļi ar sistēmisku risku – papildus MI biroja pārraudzības darbībām.
- (114) Uz tādu vispārīga lietojuma MI modeļu, kas rada sistēmiskus riskus, nodrošinātājiem – papildus vispārīga lietojuma MI modeļu nodrošinātājiem noteiktajiem pienākumiem – būtu jāattiecinā pienākumi, kuru mērķis ir identificēt un mazināt minētos riskus un nodrošināt pienācīgu kiberdrošības aizsardzības līmeni neatkarīgi no tā, vai tas tiek nodrošināts kā savrups modelis vai tiek iegulsts kādā MI sistēmā vai produktā. Lai sasniegtu minētos mērķus, ar šo regulu nodrošinātājiem būtu jāprasa veikt vajadzīgos modeļu novērtējumus, jo īpaši pirms to pirmās laišanas tirgū, tostarp veikt un dokumentēt modeļu pretiniecko testēšanu, attiecīgā gadījumā izmantojot arī iekšējo vai neatkarīgu ārējo testēšanu. Turklāt vispārīga lietojuma MI modeļu ar sistēmiskiem riskiem nodrošinātājiem būtu pastāvīgi jānovērtē un jāmazina sistēmiskie riski, tostarp, piemēram, ieviešot riska pārvaldības politiku, piemēram, pārskatatbildības un pārvaldības procesus, īstenojot pētījumus pārraudzību, veicot atbilstošus pasākumus visā modeļa dzīves ciklā un sadarbojoties ar attiecīgajiem MI vērtības ķēdes dalībniekiem.
- (115) Vispārīga lietojuma MI modeļu ar sistēmiskiem riskiem nodrošinātājiem būtu jānovērtē un jāmazina iespējamie sistēmiskie riski. Ja, neraugoties uz centieniem identificēt un novērst riskus, kas saistīti ar vispārīga lietojuma MI modeli, kurš var radīt sistēmiskus riskus, modeļa izstrāde vai lietošana izraisa nopietnu incidentu, vispārīga lietojuma MI modeļa nodrošinātājam bez liekas kavēšanās būtu jāveic incidenta uzskaitē un jāpaziņo Komisijai un valstu kompetentajām iestādēm visa attiecīgā informācija un iespējamie korektīvie pasākumi. Turklāt nodrošinātājiem attiecīgā gadījumā visā modeļa dzīves ciklā būtu jānodrošina pienācīga līmeņa kiberdrošības aizsardzība modelim un tā fiziskajai infrastruktūrai. Kiberdrošības aizsardzībā tādu sistēmisku risku kontekstā, kuri saistīti ar ļaunprātīgu modeļa izmantošanu vai uzbrukumiem, būtu pienācīgi jāņem vērā nejauša modeļa noplūde, neatļauta laišana apgrozībā, drošības pasākumu apiešana, kā arī aizsardzība pret kiberuzbrukumiem, neatļauta piekļuve vai modeļa zādzība. Minēto aizsardzību varētu sekmēt, nodrošinot modeļu svarus, algoritmus, serverus un datu kopas, piemēram, izmantojot operatīvus drošības pasākumus informācijas drošībai, specifisku kiberdrošības politiku, pienācīgus tehniskus un iedibinātus risinājumus un kiberpiekļuves un fiziskās piekļuves kontroles, kas atbilst attiecīgajiem apstākļiem un saistītajiem riskiem.
- (116) MI birojam būtu jāveicina un jāatvieglo prakses kodeksu izstrāde, pārskatīšana un pielāgošana, ņemot vērā starptautiskās pieejas. Piedalīties varētu uzaicināt visus vispārīga lietojuma MI modeļu nodrošinātājus. Lai nodrošinātu, ka prakses kodeksi atspoguļo jaunākos sasniegumus un pienācīgi ņem vērā dažādu perspektīvu kopumu, MI birojam būtu jāsadarbojas ar attiecīgajām valstu kompetentajām iestādēm un attiecīgā gadījumā šādu kodeksu izstrādes nolūkā tas varētu apspriesties ar pilsoniskās sabiedrības organizācijām un citām attiecīgajām ieinteresētajām personām un ekspertiem, tostarp ar zinātnisko grupu. Prakses kodeksiem būtu jāaptver vispārīga lietojuma MI modeļu un vispārīga lietojuma MI modeļu, kuri rada sistēmiskus riskus, nodrošinātāju pienākumi. Turklāt attiecībā uz sistēmiskiem riskiem ar prakses kodeksiem būtu jāpalīdz izveidot riska taksonomiju, kas raksturo Savienības līmeņa sistēmisko risku veidu un raksturu, tostarp to avotus. Prakses kodeksos uzmanība būtu jāpievērš arī konkrētiem riska novērtēšanas un mazināšanas pasākumiem.
- (117) Prakses kodeksiem vajadzētu būt centrālām rīkam, ar ko vispārīga lietojuma MI modeļu nodrošinātāji nodrošina šajā regulā paredzēto pienākumu pienācīgu izpildi. Pienākumu izpildes pierādīšanas nolūkā nodrošinātājiem vajadzētu spēt paļauties uz prakses kodeksiem. Ar īstenošanas aktiem Komisija var nolemt apstiprināt prakses kodeksu un piešķirt tam vispārēju spēkā esību Savienībā vai – alternatīvi – paredzēt kopīgus noteikumus attiecīgo pienākumu īstenošanai, ja līdz brīdim, kad šī regula kļūst piemērojama, nav iespējams pabeigt prakses kodeksa izstrādi vai MI birojs to neuzskata par piemērotu. Tiklīdz saskaņots standarts ir publicēts, un MI birojs ir novērtējis, ka tas ir

piemērots, lai aptvertu attiecīgos pienākumus, atbilstībai Eiropas saskaņotajam standartam būtu jānodrošina nodrošinātājiem pieņemums par atbilstību. Turklāt vispārīga lietojuma MI modeļu nodrošinātājiem vajadzētu spēt pierādīt atbilstību, izmantojot alternatīvus piemērotus līdzekļus, ja nav pieejami prakses kodeksi vai saskaņoti standarti vai ja nodrošinātāji izvēlas uz tiem nepaļauties.

- (118) Šī regula reglamentē MI sistēmas un MI modeļus, nosakot konkrētas prasības un pienākumus attiecīgajiem tirgus dalībniekiem, kas tos laiž tirgū, nodod ekspluatācijā vai lieto Savienībā, un tādējādi papildinot pienākumus, kas noteikti starpniecības pakalpojumu nodrošinātājiem, kuri šādas sistēmas vai modeļus iegulst savos pakalpojumos, ko reglamentē Regula (ES) 2022/2065. Ciktāl šādas sistēmas vai modeļi ir iegulti izraudzītās ļoti lielās tiešsaistes platformās vai ļoti lielās tiešsaistes meklētājprogrammās, uz tiem attiecas Regulā (ES) 2022/2065 paredzētā riska pārvaldības sistēma. Līdz ar to būtu jāuzskata, ka attiecīgie šajā regulā noteiktie pienākumi ir izpildīti, ja vien šādos modeļos nerodas un netiek identificēti būtiski sistēmiski riski, uz kuriem neattiecas Regula (ES) 2022/2065. Šajā kontekstā ļoti lielu tiešsaistes platformu un ļoti lielu tiešsaistes meklētājprogrammu nodrošinātājiem ir pienākums novērtēt iespējamās sistēmiskās riskus, kas izriet no to pakalpojumu izstrādes, darbības un izmantošanas, tostarp to, kā pakalpojumā izmantoto algoritmisko sistēmu izstrāde var veicināt šādus riskus, kā arī sistēmiskos riskus, kas izriet no iespējamās ļaunprātīgas izmantošanas. Minētajiem nodrošinātājiem ir arī pienākums veikt atbilstošus riska mazināšanas pasākumus, ievērojot pamattiesības.
- (119) Ņemot vērā digitālo pakalpojumu inovācijas straujo tempu un tehnoloģisko attīstību dažādu Savienības tiesību instrumentu piemērošanas jomā, jo īpaši paturot prātā, kā šos pakalpojumus lieto un uztver to saņēmēji, MI sistēmas, uz kurām attiecas šī regula, var nodrošināt kā starpniecības pakalpojumus vai to daļas Regulas (ES) 2022/2065 nozīmē, kas būtu jāinterpretē tehnoloģiski neitrālā veidā. Piemēram, MI sistēmas var lietot tiešsaistes meklētājprogrammu nodrošināšanai, jo īpaši tādā mērā, kādā MI sistēma, piemēram, tiešsaistes sarunbots, principā veic meklēšanu visās tīmekļa vietnēs, pēc tam iekļauj rezultātus savās esošajās zināšanās un pielieto atjauninātās zināšanas, lai generētu vienu iznākumu, kas apvieno dažādus informācijas avotus.
- (120) Turklāt pienākumi, kas šajā regulā noteikti dažu MI sistēmu nodrošinātājiem un uzturētājiem, lai varētu atklāt un izpaust, ka minēto sistēmu iznākumi ir mākslīgi ģenerēti vai manipulēti, ir īpaši būtiski nolūkā veicināt Regulas (ES) 2022/2065 efektīvu īstenošanu. Tas jo īpaši attiecas uz ļoti lielu tiešsaistes platformu vai ļoti lielu tiešsaistes meklētājprogrammu nodrošinātāju pienākumiem identificēt un mazināt sistēmiskos riskus, kas var rasties no mākslīgi ģenerēta vai manipulēta satura izplatīšanas, jo īpaši risku, ka radīsies faktiska vai paredzama negatīva ietekme uz demokrātiskajiem procesiem, pilsonisko diskursu un vēlēšanu procesiem, tostarp izplatot dezinformāciju.
- (121) Standartizācijai vajadzētu būt ļoti būtiskai tādu tehnisko risinājumu nodrošināšanā, kas nodrošinātājiem atbilstoši jaunākajiem sasniegumiem ļautu panākt atbilstību šīs regulas noteikumiem, veicināt inovāciju, kā arī konkurētspēju un izaugsmi vienotajā tirgū. Atbilstībai Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012⁽⁴¹⁾ 2. panta 1. punkta c) apakšpunktā noteiktajiem saskaņotajiem standartiem, kuros – kā lielākoties sagaidāms – ir atspoguļoti jaunākie sasniegumi, vajadzētu būt veidam, kā nodrošinātāji var apliecināt atbilstību šīs regulas prasībām. Tāpēc būtu jāveicina līdzsvarota interešu pārstāvība, saskaņā ar Regulas (ES) Nr. 1025/2012 5. un 6. pantu standartu izstrādē iesaistot visas attiecīgās ieinteresētās personas, jo īpaši MVU, patērētāju organizācijas un vides un sociālās jomas ieinteresētās personas. Lai veicinātu atbilstību, Komisijai standartizācijas pieprasījumi būtu jāizdod bez liekas kavēšanās. Sagatavojot standartizācijas pieprasījumu, Komisijai būtu jāapspriežas ar konsultatīvo forumu un MI padomi, lai apkopotu attiecīgās speciālās zināšanas. Tomēr, ja nav attiecīgu atsauču uz saskaņotajiem standartiem, Komisijai vajadzētu būt iespējai ar īstenošanas aktiem un pēc apspriešanās ar konsultatīvo forumu noteikt kopīgas specifikācijas dažām šajā regulā paredzētajām prasībām. Kopīgajai specifikācijai vajadzētu būt izņēmuma alternatīvam risinājumam, lai nodrošinātājam atvieglotu pienākumu izpildīt šīs regulas prasības, ja neviena no Eiropas standartizācijas organizācijām nav akceptējusi standartizācijas pieprasījumu vai ja attiecīgajos saskaņotajos

⁽⁴¹⁾ 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.).

standartos nav pietiekami ņemti vērā pamattiesību jautājumi, vai ja saskaņotie standarti neatbilst pieprasījumam, vai ja atbilstoša saskaņota standarta pieņemšana kavējas. Ja šāda kavēšanās saskaņota standarta pieņemšanā ir saistīta ar minētā standarta tehnisko sarežģītību, Komisijai tas būtu jāņem vērā, pirms tiek apsvērta kopīgu specifikāciju izstrāde. Izstrādājot kopīgas specifikācijas, Komisija ir mudināta sadarboties ar starptautiskiem partneriem un starptautiskām standartizācijas iestādēm.

- (122) Neskarot saskaņoto standartu un kopīgo specifikāciju izmantošanu, būtu lietderīgi pieņemt, ka tādas augsta riska MI sistēmas nodrošinātāji, kura ir apmācīta un pārbaudīta ar datiem, kas atspoguļo konkrēto ģeogrāfisko, uzvedības, kontekstuālo vai funkcionālo vidi, kurā MI sistēmu ir paredzēts lietot, atbilst attiecīgajam pasākumam, kas paredzēts saskaņā ar šajā regulā noteikto datu pārvaldības prasību. Neskarot šajā regulā noteiktās prasības attiecībā uz robustumu un precizitāti, saskaņā ar Regulas (ES) 2019/881 54. panta 3. punktu būtu jāpieņem, ka augsta riska MI sistēmas, kuras, ievērojot minēto regulu, ir sertificētas vai kurām saskaņā ar kiberdrošības shēmu ir izsniegts atbilstības apliecinājums, un uz to atsaucies ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, atbilst šīs regulas kiberdrošības prasībai, ciktāl kiberdrošības sertifikāts vai atbilstības apliecinājums vai tā daļas attiecas uz šīs regulas kiberdrošības prasību. Tas neskar minētās kiberdrošības shēmas brīvprātīgo raksturu.
- (123) Lai nodrošinātu augsta riska MI sistēmu augstu uzticamības līmeni, būtu jāveic minēto sistēmu atbilstības novērtēšana pirms to laišanas tirgū vai nodošanas ekspluatācijā.
- (124) Lai mazinātu slogu uz operatoriem un novērstu iespējamu dublēšanos, attiecībā uz augsta riska MI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas esošie Savienības saskaņošanas tiesību akti, kuru pamatā ir Jaunais tiesiskais regulējums, būtu lietderīgi minēto MI sistēmu atbilstību šīs regulas prasībām novērtēt minētajos tiesību aktos jau paredzētās atbilstības novērtēšanas ietvaros. Tādējādi šīs regulas prasību piemērojamībai nevajadzētu ietekmēt attiecīgajos Savienības saskaņošanas tiesību aktos paredzētās atbilstības novērtēšanas īpašo loģiku, metodiku vai vispārīgo struktūru.
- (125) Ņemot vērā augsta riska MI sistēmu sarežģītību un ar tām saistītos riskus, ir svarīgi izstrādāt pienācīgas atbilstības novērtēšanas procedūras augsta riska MI sistēmām, iesaistot paziņotās struktūras, tā saukto trešās personas veiktu atbilstības novērtēšanu. Tomēr, ņemot vērā pašreizējo produktu drošuma jomā gūto pieredzi, kas ir profesionāliem sertificētājiem, kuri darbojas pirmstirdzniecības posmā, 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 MI sistēmām, kuras nav saistītas ar produktiem. Tāpēc šādu sistēmu atbilstības novērtēšana parasti būtu jāveic nodrošinātājam uz savu atbildību, izņemot vienīgi MI sistēmas, kuras paredzēts izmantot biometrijas vajadzībām.
- (126) Lai īstenotu trešās personas veiktus atbilstības novērtējumus, kad tas ir prasīts, valstu kompetentajām iestādēm saskaņā ar šo regulu būtu jāpaziņo paziņotās struktūras ar noteikumu, ka tās atbilst prasību kopumam, it īpaši neatkarības, kompetences, interešu konflikta neesības un piemērotu kiberdrošības prasību ziņā. Valstu kompetentajām iestādēm paziņojums par minētajām struktūrām būtu jānosūta Komisijai un pārējām dalībvalstīm, izmantojot elektronisko paziņošanas rīku, ko Komisija izveidojusi un pārvalda, ievērojot Lēmuma Nr. 768/2008/EK I pielikuma R23. pantu.
- (127) Atbilstoši Savienības saistībām saskaņā ar Pasaules Tirdzniecības organizācijas Nolīgumu par tehniskajiem šķēršļiem tirdzniecībā, ir lietderīgi veicināt to atbilstības novērtēšanas rezultātu savstarpēju atzīšanu, kurus sagatavojušas kompetentās atbilstības novērtēšanas struktūras neatkarīgi no teritorijas, kurā tās ir iedibinātas, ar noteikumu, ka tādas atbilstības novērtēšanas struktūras, kas iedibinātas saskaņā ar kādas trešās valsts tiesību aktiem, atbilst šīs regulas piemērojamajām prasībām un Savienība šajā sakarā ir noslēgusi nolīgumu. Šajā kontekstā Komisijai būtu aktīvi jāizpēta iespējamie starptautiskie instrumenti šādā nolūkā un jo īpaši būtu jācenšas panākt savstarpējas atzīšanas nolīgumu noslēgšana ar trešām valstīm.
- (128) Saskaņā ar vispārātzīto būtisku modifikāciju jēdzienu, ko attiecinā uz Savienības saskaņošanas tiesību aktu regulētajiem produktiem, ir lietderīgi, ka ikreiz, kad notikušas izmaiņas, kas var ietekmēt augsta riska MI sistēmas atbilstību šīs regulas noteikumiem (piemēram, operētājsistēmas vai programmatūras arhitektūras izmaiņas), vai kad mainījies sistēmas paredzētais nolūks, MI sistēma būtu jāuzskata par jaunu MI sistēmu, kurai būtu jāveic jauns atbilstības novērtējums. Tomēr izmaiņas tādu MI sistēmu algoritmā un veikspējā, kuras turpina "mācīties" pēc to laišanas tirgū vai nodošanas ekspluatācijā, proti, automātiski pielāgojot veidu, kādā tās veic funkcijas, nebūtu uzskatāmas par būtisku modifikāciju, ar noteikumu, ka nodrošinātājs minētās izmaiņas ir iepriekš noteicis un novērtējis atbilstības novērtēšanas brīdī.

- (129) Augsta riska MI sistēmām vajadzētu būt marķētām ar CE zīmi, kas norādītu uz to atbilstību šīs regulas noteikumiem, ļaujot tām būt brīvā apritē iekšējā tirgū. Produktā iegultām augsta riska MI sistēmām būtu jāpiestiprina fiziska CE zīme, kuru var papildināt ar digitālu CE zīmi. Augsta riska MI sistēmām, kas tiek nodrošinātas tikai digitāli, būtu jāizmanto digitāla CE zīme. Dalībvalstīm nevajadzētu radīt nepamatotus šķēršļus tādu augsta riska MI sistēmu laišānai tirgū vai nodošanai ekspluatācijā, kuras atbilst šajā regulā noteiktajām prasībām un ir marķētas ar CE zīmi.
- (130) Dažos apstākļos ātra inovatīvu tehnoloģiju pieejamība var būt ļoti svarīga personu veselībai un drošumam, vides aizsardzībai un klimata pārmaiņu mazināšanas nolūkos, kā arī sabiedrībai kopumā. Līdz ar to ir lietderīgi, ka ar sabiedrisko drošību vai fizisku personu dzīvības un veselības aizsardzību, vides aizsardzību un svarīgu rūpniecības un infrastruktūras aktīvu aizsardzību saistītos ārkārtas apstākļos tirgus uzraudzības iestādes varētu atļaut laist tirgū vai nodot ekspluatācijā MI sistēmas, kurām nav veikta atbilstības novērtēšana. Pienācīgi pamatotos gadījumos, kā paredzēts šajā regulā, tiesībaizsardzības iestādes vai civilās aizsardzības iestādes var konkrētu augsta riska MI sistēmu nodot ekspluatācijā bez tirgus uzraudzības iestādes atļaujas ar noteikumu, ka šāda atļauja, lieki nekavējoties, tiek pieprasīta lietošanas laikā vai pēc tās.
- (131) Lai veicinātu Komisijas un dalībvalstu darbu MI jomā, kā arī lai vairotu pārredzamību sabiedrībai, būtu jānosaka prasība tādu augsta riska MI sistēmu nodrošinātājiem, kuras nav saistītas ar produktiem, uz kuriem attiecas esošie Savienības saskaņošanas tiesību akti, kā arī nodrošinātājiem, kuri uzskata, ka MI sistēma, kas uzskaitīta šīs regulas pielikumā augsta riska lietošanas gadījumos, nav augsta riska MI sistēma, pamatojoties uz atkāpi, reģistrēties pašiem un reģistrēt informāciju par savu MI sistēmu ES datubāzē, ko izveidos un pārvaldīs Komisija. Pirms MI sistēmu, kas uzskaitīta šīs regulas pielikumā augsta riska lietošanas gadījumos, tiek lietota, augsta riska MI sistēmu uzturētāji, kas ir publiskas iestādes, aģentūras vai struktūras, paši reģistrējas šādā datubāzē un izvēlas sistēmu, kuru tie plāno lietot. Citiem uzturētājiem vajadzētu būt tiesībām to darīt brīvprātīgi. Šai datubāzes sadaļai vajadzētu būt bez maksas publiski piekļūstamai, informācijai vajadzētu būt viegli pārlūkojamai, saprotamai un mašīnlasāmai. ES datubāzei vajadzētu būt arī lietotājdraudzīgai, piemēram, nodrošinot meklēšanas funkcijas, tostarp atslēgvārdus, kas ļauj plašai sabiedrībai atrast attiecīgo informāciju, kas iesniedzama, reģistrējot augsta riska MI sistēmas, un par augsta riska MI sistēmu veidiem, kas izklāstītas šīs regulas pielikumā, kurai atbilst augsta riska MI sistēmas. ES datubāzē būtu jāreģistrē arī jebkādas augsta riska MI sistēmu būtiskas modifikācijas. Attiecībā uz augsta riska MI sistēmām tiesībaizsardzības, migrācijas, patvēruma un robežkontroles pārvaldības jomā reģistrācijas pienākumi būtu jāizpilda drošā nepubliskā ES datubāzes sadaļā. Piekļuve drošajai nepublikajai sadaļai būtu stingri jāierobežo, atļaujot to tikai Komisijai, kā arī tirgus uzraudzības iestādēm attiecībā uz minētās datubāzes valsts sadaļu. Augsta riska MI sistēmas kritiskās infrastruktūras jomā būtu jāreģistrē tikai valsts līmenī. Komisijai vajadzētu būt ES datubāzes pārzinim saskaņā ar Regulu (ES) 2018/1725. Lai nodrošinātu datubāzes pilnīgu funkcionalitāti pēc tās darbības sākšanas, ES datubāzes izveides procedūrā būtu jāietver Komisijas veikta funkcionālo specifikāciju izstrāde un neatkarīgs revīzijas ziņojums. Komisijai, veicot savus ES datubāzes datu pārziņa uzdevumus, būtu jāņem vērā kibernetikas drošības riski. Lai maksimāli palielinātu datubāzes pieejamību un izmantošanu sabiedrībai, ES datubāzei, tostarp ar tās starpniecību sniegtajai informācijai, jāatbilst Direktīvā (ES) 2019/882 noteiktajām prasībām.
- (132) Dažas MI sistēmas, kas paredzētas mijiedarbībai ar fiziskām personām vai satura ģenerēšanai, var radīt konkrētus uzdošanās par citu personu vai maldināšanas riskus neatkarīgi no tā, vai tās ir pieskaitāmas augsta riska sistēmām vai nav. Tāpēc dažos apstākļos šādu sistēmu lietošanai būtu jāpiemēro konkrēti pārredzamības pienākumi, neskarot augsta riska MI sistēmām noteiktās prasības un pienākumus un ievērojot mērķtiecīgus izņēmumus, kas paredzēti, lai ņemtu vērā tiesībaizsardzības jomas īpašās vajadzības. Jo īpaši fiziskas personas būtu jāinformē, ka tās mijiedarbojas ar MI sistēmu, ja vien tas nav pats par sevi saprotams no tādas fiziskas personas viedokļa, kura ir samērā labi informēta, uzmanīga un apdomīga, ņemot vērā apstākļus un izmantošanas kontekstu. Īstenojot minēto pienākumu, būtu jāņem vērā tām fiziskajām personām raksturīgās iezīmes, kuras vecuma vai invaliditātes dēļ pieder pie neaizsargātām grupām, ciktāl MI sistēma ir paredzēta mijiedarbībai arī ar minētajām grupām. Turklāt fiziskām personām būtu jāpaziņo, ja tās ir pakļautas tādu MI sistēmu darbībai, kuras, apstrādājot to biometriskos datus, var identificēt vai izsecināt minēto personu emocijas vai nodomus vai iedalīt tās konkrētās kategorijās. Šādas konkrētas kategorijas var būt saistītas ar tādiem aspektiem kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, personības iezīmes, etniskā izcelsme, personīgās vēlmes un intereses. Šāda informācija un paziņojumi būtu jāsniedz formātos, kuriem var piekļūt personas ar invaliditāti.

- (133) Dažādas MI sistēmas var ģenerēt lielu daudzumu sintētiska satura, kas cilvēkiem kļūst arvien grūtāk atšķirams no cilvēka radīta un autentiska satura. Šo sistēmu plašā pieejamība un pieaugošās spējas būtiski ietekmē informācijas ekosistēmas integritāti un uzticēšanos tai, radot jaunus plaša mēroga maldinošas informācijas un manipulācijas, krāpšanas, uzdošanās par citu personu un patērētāju maldināšanas riskus. Ņemot vērā minēto ietekmi, straujo tehnoloģiskās attīstības tempu un vajadzību pēc jaunām informācijas izcelsmes izsekošanas metodēm un paņēmieniem, ir lietderīgi noteikt prasību, ka minēto sistēmu nodrošinātāji paredz iegultus tehniskus risinājumus, kas ļauj iekļaut mašīnlasāma formāta marķējumu un atklāt, ka iznākumu ir ģenerējis vai manipulējis nevis cilvēks, bet gan MI sistēma. Šādiem paņēmieniem un metodēm vajadzētu būt pietiekami uzticamiem, sadarbspējīgiem, efektīviem un robustiem, ciktāl tas ir tehniski iespējams, ņemot vērā pieejamos paņēmienus vai šādu paņēmieni kombināciju, kas var būt piemēroti, piemēram, ūdenszīmes, metadatu identifikāciju, kriptogrāfiskās metodes satura izcelsmes un autentiskuma pierādīšanai, reģistrēšanas metodes, pirkstu nospiedumus vai citus paņēmienus. Īstenojot šo pienākumu, nodrošinātājiem būtu jāņem vērā arī dažādo satura veidu specifika un ierobežojumi un attiecīgā jomas tehnoloģiskā attīstība un tirgus norises, kā atspoguļots vispāratzītos jaunākos sasniegumos. Šādus paņēmienus un metodes var īstenot MI sistēmas līmenī vai MI modeļa līmenī, tostarp vispārīga lietojuma MI modeļos, kas ģenerē saturu, tādējādi atvieglojot šā pienākuma izpildi MI sistēmas lejasposma nodrošinātājam. Lai saglabātu samērīgumu, ir lietderīgi paredzēt, ka šim marķēšanas pienākumam nebūtu jāattiecas uz MI sistēmām, kas galvenokārt pilda palīgfunkciju standarta rediģēšanai, vai uz MI sistēmām, kas būtiski nemaina uzturētāja sniegtos ievades datus vai to semantiku.
- (134) Papildus tehniskajiem risinājumiem, ko pielieto MI sistēmas nodrošinātāji, uzturētājiem, kuri MI sistēmu lieto, lai ģenerētu vai manipulētu tādu attēlu, audio vai video saturu, kas ievērojami atgādina reālas personas, objektus, vietas, subjektus vai notikumus un kas personai maldinoši šķistu autentisks vai īstas (dziļviltrojumi), būtu arī skaidri un atšķiramā veidā jāizpauž, ka saturs ir mākslīgi radīts vai manipulēts, attiecīgi marķējot MI radīto iznākumu un izpaužot tā mākslīgo izcelsmi. Šā pārredzamības pienākuma ievērošanu nevajadzētu interpretēt kā norādi uz to, ka MI sistēmas vai tās iznākuma lietošana ierobežo tiesības uz vārda brīvību un tiesības uz mākslas un zinātnes brīvību, kas garantētas Pamattiesību hartā, jo īpaši tad, ja saturs ir daļa no acīmredzami radoša, satīriskā, mākslinieciskā, fikcionāla vai analoga darba vai programmas, ievērojot atbilstošus trešo personu tiesību un brīvību aizsardzības pasākumus. Minētajos gadījumos šajā regulā noteiktais pārredzamības pienākums attiecībā uz dziļviltrojumiem attiecas tikai uz šāda ģenerēta vai manipulēta satura esamības izpaušanu piemērotā veidā, kas netraucē izrādīt vai baudīt darbu, tostarp tā parastu izmantošanu un lietošanu, vienlaikus saglabājot darba lietderību un kvalitāti. Turklāt ir arī lietderīgi paredzēt līdzīgu izpaušanas pienākumu attiecībā uz MI ģenerētu vai manipulētu tekstu, ciktāl tas ir publicēts, lai sabiedrību informētu par sabiedrības interešu jautājumiem, izņemot gadījumus, kad MI ģenerēto saturu ir pārskatījis cilvēks vai tam ir veikta redakcionāla kontrole un ja fiziska vai juridiska persona ir redakcionāli atbildīga par satura publikāciju.
- (135) Neskarot pārredzamības pienākumu obligāto raksturu un pilnīgu piemērojamību, Komisija var arī rosināt un sekmēt prakses kodeksu izstrādi Savienības līmenī, lai atvieglotu ar mākslīgi ģenerēta vai manipulēta satura atklāšanu un marķēšanu saistītu pienākumu efektīvu īstenošanu, tostarp atbalstīt praktiskus pasākumus, lai attiecīgā gadījumā padarītu atklāšanas mehānismus pieejamus un atvieglotu sadarbību ar citiem vērtības ķēdes dalībniekiem, izplatītu saturu vai pārbaudītu tā autentiskumu un izcelsmi, dodot sabiedrībai iespēju efektīvi atšķirt MI ģenerēto saturu.
- (136) Pienākumi, kas šajā regulā noteikti dažu MI sistēmu nodrošinātājiem un uzturētājiem, lai varētu atklāt un izpaust, ka minēto sistēmu iznākumi ir mākslīgi ģenerēti vai manipulēti, ir īpaši būtiski nolūkā veicināt Regulas (ES) 2022/2065 efektīvu īstenošanu. Tas jo īpaši attiecas uz ļoti lielu tiešsaistes platformu vai ļoti lielu tiešsaistes meklētājprogrammu nodrošinātāju pienākumiem identificēt un mazināt sistēmiskos riskus, kas var rasties no mākslīgi ģenerēta vai manipulēta satura izplatīšanas, jo īpaši iespējamību, ka radīsies faktiskā vai paredzama negatīva ietekme uz demokrātiskajiem procesiem, pilsonisko diskursu un vēlēšanu procesiem, tostarp izplatot dezinformāciju. Šajā regulā noteiktā prasība marķēt MI sistēmu ģenerētu saturu neskar Regulas (ES) 2022/2065 16. panta 6. punktā noteikto pienākumu mitināšanas pakalpojumu sniedzējiem izskatīt paziņojumus par nelikumīgu saturu, kas saņemti saskaņā ar minētās regulas 16. panta 1. punktu, un tai nebūtu jāietekmē novērtējums un lēmums par konkrētā satura nelikumību. Minētais novērtējums būtu jāveic, tikai atsaucoties uz noteikumiem, kas reglamentē satura likumību.

- (137) Šajā regulā reglamentēto attiecībā uz MI sistēmām noteikto pārredzamības pienākumu izpildi nevajadzētu interpretēt kā norādi uz to, ka sistēmas vai tās iznākuma lietošana ir likumīga saskaņā ar šo regulu vai citiem Savienības un dalībvalstu tiesību aktiem, un tai nebūtu jāskar citi MI sistēmu uzturētāju pārredzamības pienākumi, kas noteikti Savienības vai valsts tiesību aktos.
- (138) MI ir strauji attīstošos tehnoloģiju kopums, kam nepieciešama regulatīvā uzraudzība un droša un kontrolēta vide eksperimentēšanai, vienlaikus nodrošinot atbildīgu inovāciju un atbilstošu aizsardzības un riska mazināšanas pasākumu integrēšanu. Lai nodrošinātu inovāciju sekmējošu, nākotnes prasībām atbilstošu un pret traucējumiem noturīgu tiesisko regulējumu, dalībvalstīm būtu jānodrošina, ka to valsts kompetentās iestādes valsts līmenī izveido vismaz vienu MI "regulatīvo smilškastī" nolūkā sekmēt inovatīvu MI sistēmu izstrādi un testēšanu stingrā regulatīvā uzraudzībā, pirms šīs sistēmas laiž tirgū vai citādi nodod ekspluatācijā. Dalībvalstis šo pienākumu varētu arī izpildīt, piedaloties jau esošajās "regulatīvajās smilškastēs" vai kopīgi ar vienu vai vairākām dalībvalstu kompetentajām iestādēm izveidojot smilškastī, ciktāl šāda piedalīšanās iesaistītajām dalībvalstīm nodrošina līdzvērtīgu valsts tvēruma līmeni. MI "regulatīvās smilškastēs" varētu izveidot fiziskā, digitālā vai hibrīdā formā, un tajās var ietvert gan fiziskus, gan digitālus produktus. Izveidotajām iestādēm būtu arī jānodrošina, ka MI "regulatīvajām smilškastēm" ir to darbībai pietiekami resursi, tostarp finanšu resursi un cilvēkresursi.
- (139) MI "regulatīvo smilškastu" mērķiem vajadzētu būt – veicināt MI inovāciju, radot kontrolētu eksperimentēšanas un testēšanas vidi izstrādes un pirmstirdzniecības posmā ar nolūku nodrošināt inovatīvu MI sistēmu atbilstību šīs regulas noteikumiem un citiem attiecīgiem Savienības un valsts tiesību aktiem. Turklāt MI regulatīvajām smilškastēm vajadzētu būt vērstām uz juridiskās noteiktības uzlabošanu novatoriem un kompetento iestāžu uzraudzību un izpratni par MI lietošanas radītajām iespējām, jauniem riskiem un ietekmi, iestādēm un uzņēmumiem atvieglot regulatīvu mācīšanos, tostarp nolūkā nākotnē pielāgot tiesisko regulējumu, atbalstīt sadarbību un paraugprakses apmaiņu ar MI "regulatīvajā smilškastē" iesaistītajām iestādēm un paātrināt piekļuvi tirgiem, tostarp novēršot šķēršļus MVU, tostarp jaunuzņēmumiem. MI "regulatīvajām smilškastēm" vajadzētu būt plaši pieejamām visā Savienībā, un īpaša uzmanība būtu jāpievērš tam, ka tām var piekļūt MVU, tostarp jaunuzņēmumi. Dalībai MI "regulatīvajā smilškastē" būtu jākoncentrējas uz jautājumiem, kas rada juridisko nenoteiktību nodrošinātājiem un potenciālajiem nodrošinātājiem, lai tie varētu ieviest inovācijas, eksperimentēt ar MI Savienībā un veicināt uz pierādījumiem balstītu regulatīvo mācīšanos. Tāpēc MI sistēmu uzraudzībai MI "regulatīvajā smilškastē" būtu jāaptver to izstrāde, apmācība, testēšana un validēšana pirms sistēmu laišanas tirgū vai nodošanas ekspluatācijā, kā arī tādu būtisku modifikāciju jēdziens un rašanās, kuru dēļ var būt nepieciešama jauna atbilstības novērtēšanas procedūra. Ja šādu MI sistēmu izstrādes un testēšanas laikā konstatēti kādi būtiski riski, būtu jāveic pienācīga risku mazināšana un, ja tas neizdodas, izstrādes un testēšanas procesu būtu jāaptur. Attiecīgā gadījumā valstu kompetentajām iestādēm, kas izveido MI "regulatīvās smilškastēs", būtu jāsadarbojas ar citām attiecīgajām iestādēm, tostarp tām, kas uzrauga pamattiesību aizsardzību, un tās varētu ļaut MI ekosistēmā iesaistīt citus dalībniekus, piemēram, valsts vai Eiropas standartizācijas organizācijas, pazīnotās struktūras, testēšanas un eksperimentēšanas struktūras, pētniecības un eksperimentēšanas laboratorijas, Eiropas digitālās inovācijas centrus un attiecīgās ieinteresēto personu un pilsoniskās sabiedrības organizācijas. Lai nodrošinātu vienotu īstenošanu visā Savienībā un apjomradītus ietaupījumus, ir lietderīgi noteikt kopīgus noteikumus MI "regulatīvo smilškastu" īstenošanai un sistēmu sadarbībai starp attiecīgajām iestādēm, kuras iesaistītas "smilškastu" uzraudzībā. MI "regulatīvajām smilškastēm", kas izveidotas saskaņā ar šo regulu, nevajadzētu skart citus tiesību aktus, kas ļauj izveidot citas smilškastes, kuru mērķis ir nodrošināt atbilstību tiesību aktiem, kas nav šī regula. Attiecīgā gadījumā attiecīgajām kompetentajām iestādēm, kas atbild par šīm citām "regulatīvajām smilškastēm", būtu jāapsver ieguvumi, ko sniedz minēto smilškastu izmantošana arī nolūkā nodrošināt MI sistēmu atbilstību šai regulai. Vienojoties valstu kompetentajām iestādēm un MI "regulatīvās smilškastēs" dalībniekiem, testēšanu reālos apstākļos var veikt un uzraudzīt arī MI "regulatīvās smilškastēs" ietvaros.
- (140) Šai regulai būtu jānodrošina juridiskais pamats, kas nodrošinātājiem un potenciālajiem nodrošinātājiem MI "regulatīvajā smilškastē" ļauj tikai gadījumos, kad tiek ievēroti konkrēti nosacījumi, personas datus, kas savākti citiem nolūkiem, MI "regulatīvās smilškastēs" ietvaros izmantot dažu MI sistēmu izstrādei sabiedrības interesēs saskaņā ar Regulas (ES) 2016/679 6. panta 4. punktu un 9. panta 2. punkta g) apakšpunktu un Regulas (ES) 2018/1725 5., 6. un 10. pantu un neskarot Direktīvas (ES) 2016/680 4. panta 2. punktu un 10. pantu. Visi pārējie datu pārziņu pienākumi un datu subjektu tiesības saskaņā ar regulām (ES) 2016/679 un (ES) 2018/1725 un Direktīvu (ES) 2016/680 joprojām tiek piemēroti. Jo īpaši šai regulai nebūtu jānodrošina juridiskais pamats Regulas (ES) 2016/679 22. panta 2. punkta b) apakšpunkta un Regulas (ES) 2018/1725 24. panta 2. punkta b) apakšpunkta nozīmē. Nodrošinātājiem un potenciālajiem nodrošinātājiem MI "regulatīvajā smilškastē" būtu jānodrošina atbilstoši

aizsardzības pasākumi un jāsadarbojas ar kompetentajām iestādēm, tostarp sekojot to norādēm un rīkojoties efektīvi un godprātīgi, lai pienācīgi mazinātu jebkādas konstatētos būtiskos riskus drošumam, veselībai un pamattiesībām, kas varētu rasties minētajā “smilškastē” veiktās izstrādes, testēšanas un eksperimentēšanas gaitā.

- (141) Lai paātrinātu šīs regulas pielikumā uzskaitīto augsta riska MI sistēmu izstrādes un laišanas tirgū procesu, ir svarīgi, lai šādu sistēmu nodrošinātāji vai potenciāli nodrošinātāji arī varētu gūt labumu no konkrēta režīma minēto sistēmu testēšanai reālos apstākļos, nepiedaloties MI “regulatīvajā smilškastē”. Tomēr šādos gadījumos, ņemot vērā šādas testēšanas iespējamo ietekmi uz privātpersonām, būtu jānodrošina, ka ar šo regulu tiek ieviestas atbilstošas un pietiekamas garantijas un nosacījumi nodrošinātājiem vai potenciālajiem nodrošinātājiem. Šādās garantijās cita starpā būtu jāietver fizisku personu informētas piekrišanas pieprasīšana dalībai testēšanā reālos apstākļos, izņemot tiesībaizsardzības jomu, kur informētas piekrišanas iegūšana liegtu veikt MI sistēmas testēšanu. Subjektu piekrišana piedalīties šādā testēšanā saskaņā ar šo regulu atšķiras no datu subjektu piekrišanas viņu personas datu apstrādei saskaņā ar attiecīgajiem datu aizsardzības tiesību aktiem un neskar to. Ir svarīgi arī līdz minimumam samazināt riskus un dot iespēju kompetentajām iestādēm veikt uzraudzību un tāpēc pieprasīt potenciālajiem nodrošinātājiem iesniegt kompetentajai tirgus uzraudzības iestādei testēšanas plānu reālos apstākļos, reģistrēt testēšanu īpašās ES datubāzes sadaļās, ievērojot dažus ierobežotus izņēmumus, noteikt ierobežojumus attiecībā uz laikposmu, kurā testēšanu var veikt, un pieprasīt neaizsargātu personu aizsardzības papildu pasākumus, tostarp attiecībā uz personām, kas pieder pie neaizsargātām grupām, kā arī rakstisku vienošanos, kurā noteiktas potenciālo nodrošinātāju un uzturētāju lomas un pienākumi un efektīva uzraudzība, ko veic kompetents personāls, kas iesaistīts testēšanā reālos apstākļos. Turklāt ir lietderīgi paredzēt papildu aizsardzības pasākumus, lai nodrošinātu, ka MI sistēmas prognozes, ieteikumus vai lēmumus var faktiski reversēt un ņemt vērā un ka personas dati tiek aizsargāti un dzēsti, kad subjekti ir atsaukušas savu piekrišanu piedalīties testēšanā, neskarot savas Savienības datu aizsardzības tiesību aktos paredzētās datu subjektu tiesības. Attiecībā uz datu nodošanu ir arī lietderīgi paredzēt, ka dati, kas savākti un apstrādāti testēšanai reālos apstākļos, trešām valstīm būtu jānodod tikai tad, ja ir īstenoti piemēroti un piemērojami Savienības tiesību aktos paredzēti aizsardzības pasākumi, jo īpaši saskaņā ar Savienības datu aizsardzības tiesību aktos paredzētajiem personas datu nodošanas pamatiem, savukārt attiecībā uz nepersondatiem ir ieviesti atbilstoši aizsardzības pasākumi saskaņā ar Savienības tiesību aktiem, piemēram, Eiropas Parlamenta un Padomes Regulām (ES) 2022/868 ⁽⁴²⁾ un (ES) 2023/2854 ⁽⁴³⁾.
- (142) Lai nodrošinātu, ka MI sniedz sabiedrībai un videi labvēlīgus rezultātus, dalībvalstis tiek mudinātas atbalstīt un veicināt MI risinājumu pētniecību un izstrādi, kas atbalsta sabiedrībai un videi labvēlīgus rezultātus, piemēram, uz MI balstītus risinājumus, kas vērsti uz to, lai palielinātu piekļūstamību personām ar invaliditāti, novērstu sociālekonomisko nevienlīdzību vai sasniegtu vides mērķrādītājus, piešķirot pietiekamus resursus, tostarp publisko un Savienības finansējumu, un attiecīgā gadījumā un ar noteikumu, ka ir izpildīti atbilstības un atlases kritēriji, jo īpaši apsverot projektus, kuriem ir šādi mērķi. Šādu projektu pamatā vajadzētu būt starpdisciplinārai sadarbībai starp MI izstrādātājiem un ekspertiem nevienlīdzības un nediskriminācijas, piekļūstamības, patērētāju, vides un digitālo tiesību jautājumos, kā arī akadēmiskajām aprindām.
- (143) Lai veicinātu un aizsargātu inovāciju, ir svarīgi īpaši ņemt vērā tādu MVU, tostarp jaunuzņēmumu intereses, kas ir MI sistēmu nodrošinātāji vai uzturētāji. Šajā nolūkā dalībvalstīm būtu jāizstrādā iniciatīvas, kas ir vērstas uz šiem operatoriem, arī saistībā ar izpratnes veicināšanu un informēšanu. Dalībvalstīm būtu jānodrošina MVU, tostarp jaunuzņēmumiem, kuriem ir juridiskā adrese vai filiāle Savienībā, prioritāru piekļuvi MI “regulatīvajām smilškastēm”, ar noteikumu, ka tie izpilda atbilstības nosacījumus un atlases kritērijus, neliedzot citiem nodrošinātājiem un potenciālajiem nodrošinātājiem piekļūt “smilškastēm”, ar noteikumu, ka ir izpildīti tie paši nosacījumi un kritēriji. Dalībvalstīm būtu jāizmanto esošie kanāli un attiecīgā gadījumā jāizveido jauni īpaši kanāli saziņai ar MVU, tostarp jaunuzņēmumiem, uzturētājiem, citiem novatoriem un vajadzības gadījumā vietējām publiskām iestādēm, lai visās izstrādes stadijās atbalstītu MVU, sniedzot norādījumus un atbildot uz jautājumiem par šīs regulas īstenošanu. Attiecīgā gadījumā šiem kanāliem būtu jāsadarbības, lai radītu sinerģijas un nodrošinātu, ka to norādījumi MVU, tostarp jaunuzņēmumiem, un uzturētājiem ir viendabīgi. Turklāt dalībvalstīm būtu jāsekmē MVU un citu attiecīgo ieinteresēto personu līdzdalība standartizācijas izstrādes procesos. Turklāt būtu jāņem vērā nodrošinātāju, kuri ir

⁽⁴²⁾ Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (OV L 152, 3.6.2022., 1. lpp.).

⁽⁴³⁾ Eiropas Parlamenta un Padomes Regula (ES) 2023/2854 (2023. gada 13. decembris) par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu un ar ko groza Regulu (ES) 2017/2394 un Direktīvu (ES) 2020/1828 (Datu akts) (OV L, 2023/2854, 22.12.2023., ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

MVU, tostarp jaunuzņēmumi, konkrētās intereses un vajadzības paziņotajām struktūrām, nosakot maksu par atbilstības novērtēšanu. Komisijai būtu regulāri jānovērtē MVU, tostarp jaunuzņēmumu, sertifikācijas un atbilstības nodrošināšanas izmaksas, izmantojot pārredzamas konsultācijas, un būtu jāstrādā kopīgi ar dalībvalstīm pie tā, lai samazinātu šādas izmaksas. Piemēram, ar obligāto dokumentāciju un saziņu ar iestādēm saistītie tulkošanas izdevumi var radīt ievērojamas izmaksas nodrošinātājiem un citiem operatoriem, jo īpaši mazākiem. Iespējams, ka dalībvalstīm vajadzētu nodrošināt, ka viena no valodām, ko tās nosaka un pieņem kā valodu attiecīgajai nodrošinātāju dokumentācijai un saziņai ar operatoriem, ir valoda, kuru plaši saprot pēc iespējas lielāks pārrobežu uzturētāju skaits. Lai ņemtu vērā MVU, tostarp jaunuzņēmumu, īpašās vajadzības, Komisijai pēc MI padomes pieprasījuma būtu jānodrošina standartizētas veidnes jomām, uz kurām attiecas šī regula. Turklāt Komisijai būtu jāpapildina dalībvalstu centieni, visiem nodrošinātājiem un uzturētājiem nodrošinot vienotu informācijas platformu ar viegli izmantojamu informāciju saistībā ar šo regulu, organizējot atbilstīgas komunikācijas kampaņas, lai palielinātu informētību par pienākumiem, kas izriet no šīs regulas, un izvērtējot un veicinot paraugprakses konvergenci publiskā iepirkuma procedūrās saistībā ar MI sistēmām. Vidējiem uzņēmumiem, kas līdz nesenam laikam tika kvalificēti kā mazie uzņēmumi Komisijas Ieteikuma 2003/361/EK⁽⁴⁴⁾ pielikuma nozīmē, vajadzētu būt piekļuvei minētajiem atbalsta pasākumiem, jo minētajiem jaunajiem vidējiem uzņēmumiem dažkārt var trūkt juridisko resursu un apmācības, kas vajadzīgi, lai nodrošinātu pienācīgu izpratni par šo regulu un atbilstību tai.

- (144) Lai veicinātu un aizsargātu inovāciju, platformai “MI pēc pieprasījuma”, visām attiecīgajām Savienības finansēšanas programmām un projektiem, piemēram, programmai “Digitālā Eiropa”, “Apvārsnis Eiropa”, ko Komisija un dalībvalstis attiecīgi īsteno Savienības vai valsts līmenī, būtu jāpalīdz sasniegt šīs regulas mērķus.
- (145) Lai minimizētu ar īstenošanu saistītos riskus, kas izriet no zināšanu un zinātības trūkuma tirgū, kā arī veicinātu nodrošinātāju, īpaši MVU, tostarp jaunuzņēmumu, un paziņoto 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 Savienības vai valsts līmenī, būtu jāpalīdz šīs regulas īstenošanā. Platforma “MI pēc pieprasījuma”, Eiropas digitālās inovācijas centri un testēšanas un eksperimentēšanas struktūras savu attiecīgo uzdevumu un kompetences ietvaros jo īpaši spēj sniegt tehnisku un zinātnisku atbalstu nodrošinātājiem un paziņotajām struktūrām.
- (146) Turklāt, ņemot vērā dažu operatoru ļoti mazo lielumu un lai nodrošinātu proporcionālītāti attiecībā uz inovācijas izmaksām, ir lietderīgi ļaut mikrouzņēmumiem vienkāršotā veidā pildīt vienu no visdārgākajiem pienākumiem, proti, izveidot kvalitātes pārvaldības sistēmu, kas samazinātu administratīvo slogu un izmaksas minētajiem uzņēmumiem, neietekmējot aizsardzības līmeni un nepieciešamību ievērot augsta riska MI sistēmu prasības. Komisijai būtu jāizstrādā pamatnostādnes ar mērķi precizēt kvalitātes vadības sistēmas elementus, kas šādā vienkāršotā veidā jāpilda mikrouzņēmumiem.
- (147) Ir lietderīgi, ka Komisija struktūrām, grupām vai laboratorijām, kuras izveidotas vai akreditētas, ievērojot attiecīgos Savienības saskaņošanas tiesību aktus, un izpilda uzdevumus to produktu vai ierīču, uz kuriem attiecas minētie Savienības saskaņošanas tiesību akti, atbilstības novērtēšanas kontekstā, cik vien iespējams atvieglot piekļuvi testēšanas un eksperimentēšanas struktūrām. Tas jo paši attiecas uz ekspertu grupām, ekspertu laboratorijām un references laboratorijām medicīnisko ierīču jomā saskaņā ar Regulu (ES) 2017/745 un Regulu (ES) 2017/746.
- (148) Šai regulai būtu jāizveido pārvaldības satvars, kas ļautu gan koordinēt, gan atbalstīt šīs regulas piemērošanu valsts līmenī, kā arī veidot spējas Savienības līmenī un integrēt ieinteresētās personas MI jomā. Lai efektīvi īstenotu un izpildītu šo regulu, ir vajadzīgs pārvaldības satvars, kas ļauj koordinēt un uzkrāt būtiskas speciālās zināšanas Savienības līmenī. MI birojs tika izveidots ar Komisijas lēmumu⁽⁴⁵⁾, un tā uzdevums ir attīstīt Savienības speciālās zināšanas un spējas MI jomā un veicināt Savienības tiesību aktu īstenošanu MI jomā. Dalībvalstīm būtu jāatvieglot MI biroja uzdevumu izpilde, lai atbalstītu Savienības speciālo zināšanu un spēju attīstību Savienības līmenī un stiprinātu digitālā vienotā tirgus darbību. Turklāt būtu jāizveido MI padome, kuras sastāvā būtu dalībvalstu pārstāvji, zinātniskā grupa zinātniskās kopienas integrēšanai un konsultatīvais forums, kura mērķis ir Savienības un valsts līmenī sniegt ieinteresēto personu ieguldījumu šīs regulas īstenošanā. Savienības speciālo zināšanu un spēju attīstībā būtu jāietver

⁽⁴⁴⁾ Komisijas 2003. gada 6. maija Ieteikums par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

⁽⁴⁵⁾ Komisijas Lēmums (2024. gada 24. janvāris), ar ko izveido Eiropas Mākslīgā intelekta biroju, C(2024) 390.

arī esošo resursu un speciālo zināšanu izmantošana, jo īpaši izmantojot sinerģijas ar struktūrām, kas izveidotas saistībā ar citu tiesību aktu izpildi Savienības līmenī, un sinerģijas ar saistītām iniciatīvām Savienības līmenī, piemēram, kopuzņēmumu *EuroHPC* un MI testēšanas un eksperimentēšanas struktūrām programmas “Digitālā Eiropa” ietvaros.

- (149) Lai sekmētu netraucētu, efektīvu un saskaņotu šīs regulas īstenošanu, būtu jāizveido MI padome. MI padomei būtu jāatspoguļo dažādās MI ekosistēmas intereses, un tās sastāvā vajadzētu būt dalībvalstu pārstāvjiem. MI padomei būtu jāatbild par vairākiem konsultatīviem uzdevumiem, tostarp atzinumu, ieteikumu, konsultāciju sniegšanu vai norādījumu līdzveidošanu jautājumos, kas saistīti ar šīs regulas īstenošanu, tostarp par izpildes panākšanu, tehniskajām specifikācijām vai pašreizējiem standartiem attiecībā uz šajā regulā noteiktajām prasībām, kā arī par Komisijas un dalībvalstu un to kompetento iestāžu konsultēšanu konkrētos jautājumos saistībā ar MI. Lai dalībvalstīm dotu zināmu elastību savu pārstāvju izraudzīšanā MI padomē, šādi pārstāvji var būt jebkura persona, kura pieder pie publiskām struktūrām un kurai vajadzētu būt attiecīgajām kompetencēm un pilnvarām sekmēt koordināciju valsts līmenī un veicināt MI padomes uzdevumu izpildi. MI padomei būtu jāizveido divas pastāvīgas apakšgrupas, lai nodrošinātu platformu sadarbībai un apmaiņai starp tirgus uzraudzības iestādēm un paziņojošajām iestādēm jautājumos, kas attiecīgi saistīti ar tirgus uzraudzību un paziņotajām struktūrām. Tirgus uzraudzības pastāvīgajai apakšgrupai būtu jādarbojas kā šīs regulas administratīvās sadarbības grupai (ADCO) Regulas (ES) 2019/1020 30. panta nozīmē. Saskaņā ar minētās regulas 33. pantu Komisijai būtu jāatbalsta tirgus uzraudzības pastāvīgās apakšgrupas darbības, veicot tirgus izvērtējumus vai pētījumus, jo īpaši nolūkā apzināt šīs regulas aspektus, kam nepieciešama konkrēta un steidzama koordinācija starp tirgus uzraudzības iestādēm. MI padome vajadzības gadījumā var izveidot citas pastāvīgas vai pagaidu apakšgrupas konkrētu jautājumu izskatīšanai. MI padomei attiecīgā gadījumā būtu arī jāsadarbjas ar attiecīgajām ES struktūrām, ekspertu grupām un tīkliem, kas darbojas attiecīgo ES tiesību aktu kontekstā, tostarp jo īpaši ar tiem, kas darbojas saskaņā ar attiecīgiem ES tiesību aktiem datu, digitālo produktu un pakalpojumu jomā.
- (150) Lai nodrošinātu ieinteresēto personu iesaistīšanos šīs regulas īstenošanā un piemērošanā, būtu jāizveido konsultatīvais forums ar mērķi sniegt konsultācijas un tehniskas speciālās zināšanas MI padomei un Komisijai. Lai nodrošinātu dažādu un līdzsvarotu ieinteresēto personu pārstāvību starp komerciālām un nekomerciālām interesēm un komerciālo interešu kategorijā attiecībā uz MVU un citiem uzņēmumiem, konsultatīvajā forumā cita starpā būtu jāiekļauj rūpniecība, jaunuzņēmumi, MVU, akadēmiskās aprindas, pilsoniskā sabiedrība, tostarp sociālie partneri, kā arī Pamattiesību aģentūra, ENISA, Eiropas Standartizācijas komiteja (CEN), Eiropas Elektrotehniskās standartizācijas komiteja (CENELEC) un Eiropas telesakaru standartu institūts (ETSI).
- (151) Lai atbalstītu šīs regulas īstenošanu un izpildi, jo īpaši MI biroja uzraudzības darbības attiecībā uz vispārējas nozīmes MI modeļiem, būtu jāizveido neatkarīgu ekspertu zinātniskā grupa. Neatkarīgie eksperti, kas veido zinātnisko grupu, būtu jāizraugās, pamatojoties uz jaunākajām zinātniskajām vai tehniskajām speciālajām zināšanām MI jomā, un tiem savi uzdevumi būtu jāveic neatkarīgi un objektīvi un jānodrošina uzdevumu un darbību izpildes gaitā iegūtās informācijas un datu konfidencialitāte. Lai varētu stiprināt valstu spējas, kas vajadzīgas šīs regulas efektīvai izpildei, dalībvalstīm to izpildes darbībām vajadzētu būt iespējai lūgt atbalstu no ekspertu rezerves, kas veido zinātnisko grupu.
- (152) Lai atbalstītu MI sistēmu pienācīgu izpildi un stiprinātu dalībvalstu spējas, būtu jāizveido Savienības MI testēšanas atbalsta struktūras, kas būtu jā dara pieejamas dalībvalstīm.
- (153) Dalībvalstīm ir būtiska loma šīs regulas piemērošanā un izpildē. Šajā sakarā katrai dalībvalstij šīs regulas piemērošanas un īstenošanas uzraudzībai būtu jāizraugās vismaz viena paziņojošā iestāde un vismaz viena tirgus uzraudzības iestāde kā valsts kompetentās iestādes. Dalībvalstis var nolemt iecelt jebkāda veida publisku struktūru valsts kompetento iestāžu uzdevumu veikšanai šīs regulas nozīmē saskaņā ar to konkrētajām valsts organizatoriskajām iezīmēm un vajadzībām. Lai vairotu dalībvalstu organizatorisku efektivitāti un izveidotu vienotu kontaktpunktu saziņai ar sabiedrību un citiem partneriem dalībvalstu un Savienības līmenī, katrai dalībvalstij būtu jāizraugās tirgus uzraudzības iestāde, kas darbojas kā vienotais kontaktpunkts.

- (154) Valsts kompetentām iestādēm savas pilnvaras būtu jāīsteno neatkarīgi, objektīvi un bez aizspriedumiem, lai aizsargātu savu darbību un uzdevumu objektivitātes principus un nodrošinātu šīs regulas piemērošanu un īstenošanu. Šo iestāžu locekļiem būtu jāatturas no jebkādas rīcības, kas nav saderīga ar viņu pienākumiem, un uz viņiem būtu jāattiecināta šajā regulā paredzētie konfidencialitātes noteikumi.
- (155) Lai nodrošinātu, ka augsta riska MI sistēmu nodrošinātāji pieredzi augsta riska MI sistēmu lietošanā var ņemt vērā, uzlabojot savas sistēmas un projektēšanas un izstrādes procesu, vai savlaicīgi veikt jebkādu iespējamu korektīvu darbību, visiem nodrošinātājiem būtu jāizveido pēctirgus pārraudzības sistēma. Attiecīgā gadījumā pēctirgus pārraudzībai būtu jāietver analīze par mijiedarbību ar citām MI sistēmām, tostarp citām ierīcēm un programmatūru. Pēctirgus pārraudzībai nevajadzētu attiekties uz uzturētāju, kas ir tiesībsargāšanas iestādes, sensitīviem operatīvajiem datiem. Minētā sistēma ir svarīga arī, lai varētu efektīvi un savlaicīgi novērst iespējamus riskus, kas rodas, MI sistēmām turpinot "mācīties" pēc to laišanas tirgū vai nodošanas ekspluatācijā. Šajā kontekstā būtu arī jānosaka, ka nodrošinātājiem ir jāievieš sistēma ar mērķi ziņot attiecīgajām iestādēm par to MI sistēmu lietošanas izraisītiem nopietniem incidentiem, proti, incidentu vai darbības traucējumu, kas izraisa nāvi vai nopietnu kaitējumu veselībai, nopietniem un neatgriezeniskiem kritiskās infrastruktūras pārvaldības un darbības traucējumiem, Savienības tiesību aktos pamattiesību aizsardzībai paredzēto pienākumu pārkāpumiem vai nopietnu kaitējumu īpašumam vai videi.
- (156) 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 pilnībā. Tirgus uzraudzības iestādēm, kas izraudzītas, ievērojot šo regulu, vajadzētu būt visām izpildes pilnvarām, kas paredzētas šajā regulā un Regulā (ES) 2019/1020, un tām būtu jāīsteno savas pilnvaras un jāveic savi pienākumi neatkarīgi, objektīvi un bez aizspriedumiem. Lai gan uz lielāko daļu MI sistēmu neattiecas konkrētas prasības un pienākumi, kas paredzēti šajā regulā, tirgus uzraudzības iestādes var veikt pasākumus attiecībā uz visām MI sistēmām, ja tās saskaņā ar šo regulu rada risku. Ņemot vērā šīs regulas piemērošanas jomā ietilpstošo Savienības iestāžu, aģentūru un struktūru konkrēto raksturu, ir lietderīgi izraudzīties Eiropas Datu aizsardzības uzraudzītāju par to kompetento tirgus uzraudzības iestādi. Tam nebūtu jāskar valsts kompetento iestāžu izraudzīšanās, ko veic dalībvalstis. Tirgus uzraudzības darbībām nevajadzētu ietekmēt uzraudzīto vienību spēju neatkarīgi veikt savus uzdevumus, ja šāda neatkarība ir prasīta Savienības tiesību aktos.
- (157) Šī regula neskar to attiecīgo valsts publisku iestāžu vai struktūru kompetenci, uzdevumus, pilnvaras un neatkarību, kuras uzrauga Savienības tiesību aktu, kas aizsargā pamattiesības, piemērošanu, tostarp līdztiesības struktūru un datu aizsardzības iestāžu kompetenci, uzdevumus, pilnvaras un neatkarību. Kad tas nepieciešams to pilnvaru īstenošanai, minētajām valsts publiskām iestādēm vai struktūrām vajadzētu būt arī piekļuvei jebkādai dokumentācijai, kas sagatavota saskaņā ar šo regulu. Būtu jānosaka konkrēta drošības procedūra, lai nodrošinātu pienācīgu un savlaicīgu izpildi attiecībā uz MI sistēmām, kas rada risku veselībai, drošībai un pamattiesībām. Procedūra attiecībā uz šādām MI sistēmām, kas rada risku, būtu jāpiemēro augsta riska MI sistēmām, kas rada risku, aizliegtām sistēmām, kas laistas tirgū, nodotas ekspluatācijā vai izmantotas, pārkāpjot šajā regulā noteikto aizliegto praksi, un MI sistēmām, kas darītas pieejamas, pārkāpjot šajā regulā noteiktās pārredzamības prasības, un rada risku.
- (158) Savienības tiesību akti finanšu pakalpojumu jomā ietver iekšējās pārvaldes un riska pārvaldības noteikumus un prasības, kas attiecas uz regulētām finanšu iestādēm minēto pakalpojumu sniegšanas gaitā, arī tad, kad tās lieto MI sistēmas. Lai nodrošinātu šajā regulā noteikto pienākumu un Savienības finanšu pakalpojumu tiesību aktu attiecīgo noteikumu un prasību saskaņotu piemērošanu un izpildi, par minēto tiesību aktu uzraudzību un izpildi kompetentās iestādes, jo īpaši tās kompetentās iestādes, kas definētas Eiropas Parlamenta un Padomes Regulā (ES) Nr. 575/2013⁽⁴⁶⁾ un Eiropas Parlamenta un Padomes Direktīvās 2008/48/EK⁽⁴⁷⁾, 2009/138/EK⁽⁴⁸⁾,

⁽⁴⁶⁾ Eiropas Parlamenta un Padomes Regula (ES) Nr. 575/2013 (2013. gada 26. jūnijs) par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 176, 27.6.2013., 1. lpp.).

⁽⁴⁷⁾ Eiropas Parlamenta un Padomes Direktīva 2008/48/EK (2008. gada 23. aprīlis) par patēriņa kredītīgumiem un ar ko atceļ Direktīvu 87/102/EEK (OV L 133, 22.5.2008., 66. lpp.).

⁽⁴⁸⁾ Eiropas Parlamenta un Padomes Direktīva 2009/138/EK (2009. gada 25. novembris) par uzņēmējdarbības uzsākšanu un veikšanu apdrošināšanas un pārapdrošināšanas jomā (Maksāspēja II) (OV L 335, 17.12.2009., 1. lpp.).

2013/36/ES⁽⁴⁹⁾, 2014/17/ES⁽⁵⁰⁾ un (ES) 2016/97⁽⁵¹⁾, savas attiecīgās kompetences ietvaros būtu jāizraugās par kompetentajām iestādēm šīs regulas īstenošanas uzraudzībai, tostarp tirgus uzraudzības darbībām, attiecībā uz MI sistēmām, kuras nodrošina vai izmanto regulētas un uzraudzītas finanšu iestādes, ja vien dalībvalstis nenolemj izraudzīties citu iestādi šo tirgus uzraudzības uzdevumu izpildei. Minētajām kompetentajām iestādēm vajadzētu būt visām pilnvarām, kas paredzētas šajā regulā un Regulā (ES) 2019/1020, lai izpildītu šajā regulā noteiktās prasības un pienākumus, tostarp pilnvarām veikt ex post tirgus uzraudzības darbības, kuras attiecīgā gadījumā var integrēt to esošajos uzraudzības mehānismos un procedūrās, kā paredzēts attiecīgajos Savienības tiesību aktos finanšu pakalpojumu jomā. Ir lietderīgi paredzēt, ka, pildot tirgus uzraudzības iestādes pienākumus, kā tas paredzēts šajā regulā, valstu iestādēm, kas atbild par to kredītiestāžu uzraudzību, kuras tiek regulētas ar Direktīvu 2013/36/ES un kuras piedalās vienotajā uzraudzības mehānismā, kas izveidots ar Padomes Regulu (ES) Nr. 1024/2013⁽⁵²⁾, būtu nekavējoties jāziņo Eiropas Centrālajai bankai visa tirgus uzraudzības darbību gaitā identificētā informācija, kas varētu būt noderīga Eiropas Centrālās bankas prudenciālās uzraudzības uzdevumu veikšanai, kā noteikts minētajā regulā. Lai vēl vairāk uzlabotu saskaņotību starp šo regulu un noteikumiem, kuri attiecas uz kredītiestādēm, ko regulē Direktīva 2013/36/ES, ir arī lietderīgi dažus nodrošinātāju procesuālos pienākumus saistībā ar riska pārvaldību, pēctirgus pārraudzību un dokumentāciju integrēt pašreizējos pienākumos un procedūrās, kas noteiktas Direktīvā 2013/36/ES. Lai novērstu pārklāšanos, būtu jāparedz arī ierobežotas atkāpes attiecībā uz nodrošinātāju kvalitātes vadības sistēmu un pārraudzības pienākumu, kas noteikts augsta riska MI sistēmu uzturētajiem, ciktāl tie attiecas uz kredītiestādēm, ko regulē Direktīva 2013/36/ES. Tas pats režīms būtu jāpiemēro apdrošināšanas un pārapdrošināšanas sabiedrībām un apdrošināšanas pārvaldītājsabiedrībām saskaņā ar Direktīvu 2009/138/EK un apdrošināšanas starpniekiem saskaņā ar Direktīvu (ES) 2016/97, kā arī cita veida finanšu iestādēm, uz kurām attiecas prasības par iekšējo pārvaldi, mehānismiem vai procesiem, kas noteiktas, ievērojot attiecīgos Savienības tiesību aktus finanšu pakalpojumu jomā, lai nodrošinātu konsekvenču un vienlīdzīgu attieksmi finanšu nozarē.

- (159) Katrai šīs regulas pielikumā uzskaitītajai augsta riska MI sistēmu tirgus uzraudzības iestādei biometrijas jomā, ciktāl minētās sistēmas tiek izmantotas tiesībaizsardzības, migrācijas, patvēruma un robežkontroles pārvaldības vai tiesvedības un demokrātisko procesu nolūkos, vajadzētu būt efektīvām izmeklēšanas un korektīvām pilnvarām, tostarp vismaz pilnvarām iegūt piekļuvi visiem apstrādātajiem personas datiem un visai informācijai, kas vajadzīga tās uzdevumu izpildei. Tirgus uzraudzības iestādēm vajadzētu būt iespējai īstenot savas pilnvaras, rīkojoties pilnīgi neatkarīgi. Jebkuram ierobežojumam, kas attiecas uz to piekļuvi sensitīviem operatīvajiem datiem saskaņā ar šo regulu, nevajadzētu skart pilnvaras, kas tām piešķirtas ar Direktīvu (ES) 2016/680. Nevienam izņēmumam, kas attiecas uz datu izpaušanu valsts datu aizsardzības iestādēm saskaņā ar šo regulu, nevajadzētu ietekmēt minēto iestāžu pašreizējās vai turpmākās pilnvaras ārpus šīs regulas piemērošanas jomu.
- (160) Tirgus uzraudzības iestādēm un Komisijai vajadzētu būt iespējai ierosināt kopīgas darbības, tostarp kopīgas izmeklēšanas, kas jāveic tirgus uzraudzības iestādēm vai tirgus uzraudzības iestādēm kopā ar Komisiju, nolūkā veicināt atbilstību, konstatēt neatbilstību, uzlabot informētību un sniegt norādījumus saistībā ar šo regulu attiecībā uz konkrētām augsta riska MI sistēmu kategorijām, par kurām konstatēts, ka tās rada nopietnu risku divās vai vairāk dalībvalstīs. Kopīgas darbības nolūkā veicināt atbilstību būtu jāveic saskaņā ar Regulas (ES) 2019/1020 9. pantu. MI birojam būtu jānodrošina kopīgas izmeklēšanas centrāla koordinācija.
- (161) Savienības un valstu līmenī ir jāprecizē pienākumi un kompetences attiecībā uz MI sistēmām, kas balstās uz vispārīga lietojuma MI modeļiem. Lai izvairītos no kompetenču pārklāšanās gadījumos, kad MI sistēma balstās uz vispārīga lietojuma MI modeli un šā modeļa un sistēmas nodrošināšanu veic viens un tas pats nodrošinātājs, uzraudzībai būtu

⁽⁴⁹⁾ 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.).

⁽⁵⁰⁾ Eiropas Parlamenta un Padomes Direktīva 2014/17/ES (2014. gada 4. februāris) par patērētāju kredītlīgumiem saistībā ar mājokļa nekustamo īpašumu un ar ko groza Direktīvas 2008/48/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 (OV L 60, 28.2.2014., 34. lpp.).

⁽⁵¹⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/97 (2016. gada 20. janvāris) par apdrošināšanas izplatīšanu (OV L 26, 2.2.2016., 19. lpp.).

⁽⁵²⁾ Padomes Regula (ES) Nr. 1024/2013 (2013. gada 15. oktobris), ar ko Eiropas Centrālajai bankai uztic īpašus uzdevumus saistībā ar politikas nostādņām, kas attiecas uz kredītiestāžu prudenciālo uzraudzību (OV L 287, 29.10.2013., 63. lpp.).

jānotiek Savienības līmenī ar MI biroja starpniecību, kuram šajā nolūkā vajadzētu būt tirgus uzraudzības iestādes pilnvarām Regulas (ES) 2019/1020 nozīmē. Visos pārējos gadījumos valstu tirgus uzraudzības iestādes saglabā atbildību par MI sistēmu uzraudzību. Tomēr attiecībā uz vispārīga lietojuma MI sistēmām, kuras uzturētāji var tieši izmantot vismaz vienam nolūkam, kas ir klasificēts kā augsta riska nolūks, tirgus uzraudzības iestādēm būtu jāsadarbojas ar MI biroju, lai veiktu atbilstības izvērtēšanu un attiecīgi informētu padomi un citas tirgus uzraudzības iestādes. Turklāt tirgus uzraudzības iestādēm vajadzētu būt iespējai pieprasīt palīdzību no MI biroja, ja tirgus uzraudzības iestāde nespēj pabeigt izmeklēšanu attiecībā uz augsta riska MI sistēmu, jo tā nevar piekļūt noteiktai informācijai, kas ir saistīta ar vispārīga lietojuma MI modeli, uz kuru balstās augsta riska MI sistēma. Tādos gadījumos *mutatis mutandis* būtu jāpiemēro Regulas (ES) 2019/1020 VI nodaļas procedūra attiecībā uz savstarpējo palīdzību pārrobežu lietās.

- (162) Lai pēc iespējas labāk izmantotu Savienības centralizētās speciālās zināšanas un sinerģijas Savienības līmenī, Komisijas kompetencē vajadzētu būt vispārīga lietojuma MI modeļu nodrošinātāju uzraudzībai un izpildes pilnvarām. MI birojam vajadzētu būt iespējai veikt visas nepieciešamās darbības, lai pārraudzītu šīs regulas efektīvu īstenošanu attiecībā uz vispārīga lietojuma MI modeļiem. Tai vajadzētu būt iespējai izmeklēt iespējamus vispārīga lietojuma MI modeļu nodrošinātāju noteikumu pārkāpumus gan pēc savas iniciatīvas, ņemot vērā pārraudzības darbību rezultātus, gan pēc tirgus uzraudzības iestāžu pieprasījuma saskaņā ar šajā regulā izklāstītajiem nosacījumiem. Lai atbalstītu MI biroja efektīvu pārraudzību, tai vajadzētu paredzēt iespēju lejasposma nodrošinātājiem iesniegt sūdzības par iespējamām to noteikumu pārkāpumiem, kas attiecas uz vispārīga lietojuma MI modeļu un sistēmu nodrošinātājiem.
- (163) Lai papildinātu vispārīga lietojuma MI modeļu pārvaldības sistēmas, zinātniskajai grupai būtu jāatbalsta MI biroja pārraudzības darbības un atsevišķos gadījumos tā var MI birojam sniegt kvalificētus brīdinājumus, kuri izraisa turpmākus pasākumus, piemēram, izmeklēšanu. Tam būtu jāattiecas uz gadījumiem, kad zinātniskajai grupai ir pamats aizdomām, ka vispārīga lietojuma MI modelis rada konkrētu un identificējamu risku Savienības līmenī. Turklāt tam būtu jāattiecas uz gadījumiem, kad zinātniskajai grupai ir pamats aizdomām, ka vispārīga lietojuma MI modelis atbilst kritērijiem, kuru dēļ tas tiktu klasificēts kā vispārīga lietojuma MI modelis ar sistēmisku risku. Lai zinātniskajai grupai sniegtu informāciju, kas vajadzīga minēto uzdevumu izpildei, būtu jāparedz mehānisms, saskaņā ar kuru zinātniskā grupa var pieprasīt Komisijai, lai tā pieprasa dokumentāciju vai informāciju no nodrošinātāja.
- (164) MI birojam vajadzētu būt iespējai veikt nepieciešamās darbības, lai pārraudzītu šajā regulā noteikto vispārīga lietojuma MI modeļu nodrošinātāju pienākumu efektīvu īstenošanu un izpildi. MI birojam vajadzētu būt iespējai izmeklēt iespējamus pārkāpumus saskaņā ar šajā regulā paredzētajām pilnvarām, tostarp, pieprasot dokumentāciju un informāciju, veicot izvērtēšanu, kā arī pieprasot vispārīga lietojuma MI modeļu nodrošinātājiem veikt pasākumus. Veicot izvērtēšanu, nolūkā izmantot neatkarīgas speciālās zināšanas, MI birojam vajadzētu būt iespējai piesaistīt neatkarīgus ekspertus, lai tie veiktu izvērtēšanu tā vārdā. Atbilstība pienākumiem būtu jāpanāk, cita starpā pieprasot veikt pienācīgus pasākumus, tostarp riska mazināšanas pasākumus identificēto sistēmisko risku gadījumā, kā arī ierobežojot modeļa pieejamību tirgū, to izņemot vai atsaucot no tirgus. Drošības nolūkā, vajadzības gadījumā pārsniedzot šajā regulā paredzētās procesuālās tiesības, vispārīga lietojuma MI modeļu nodrošinātājiem vajadzētu būt Regulas (ES) 2019/1020 18. pantā paredzētajām procesuālajām tiesībām, kas *mutatis mutandis* būtu jāpiemēro, neskarot konkrētākas šajā regulā paredzētās procesuālās tiesības.
- (165) Tādu MI sistēmu, kas nav augsta riska MI sistēmas, izstrāde saskaņā ar šīs regulas prasībām varētu izraisīt ētiska un uzticama mākslīgā intelekta plašāku ieviešanu Savienībā. Tādu MI sistēmu, kas nav augsta riska MI sistēmas, nodrošinātāji būtu jāmudina izstrādāt rīcības kodeksus, tostarp saistītus pārvaldības mehānismus, kuru mērķis būtu veicināt dažu vai visu augsta riska MI sistēmām piemērojamo obligāto prasību brīvprātīgu piemērošanu, kuras pielāgotas, ņemot vērā sistēmu paredzēto nolūku un saistīto zemāko risku, kā arī ņemot vērā pieejamos tehniskos risinājumus un nozares paraugpraksi, piemēram, modeļus un datu kartes. Tāpat visus MI sistēmu – neatkarīgi no tā, vai tās ir vai nav augsta riska sistēmas, – un MI modeļu uzturētājus un attiecīgā gadījumā ieviesējus būtu jāmudina brīvprātīgi piemērot papildu prasības, kas ir saistītas, piemēram, ar elementiem Savienības ētikas vadlīnijās

uzticamam MI, ar vides ilgtspēju, MI pratības pasākumiem, iekļaujošu un daudzveidīgu MI sistēmu projektēšanu un izstrādi, tostarp pievēršot uzmanību neaizsargātām personām un pieejamībai personām ar invaliditāti, ar ieinteresēto personu līdzdalību, attiecīgā gadījumā MI sistēmu projektēšanā un izstrādē iesaistot attiecīgās ieinteresētās personas, piemēram, uzņēmēju un pilsoniskās sabiedrības organizācijas, akadēmiskās aprindas, pētniecības organizācijas, arodbiedrības un patērētāju aizsardzības organizāciju, un ar daudzveidību, tostarp dzimumu līdzsvaru izstrādes komandās. Lai nodrošinātu brīvprātīgo rīcības kodeksu efektivitāti, to pamatā vajadzētu būt skaidriem mērķiem un galvenajiem snieguma rādītājiem, lai izmērītu minēto mērķu sasniegšanu. Attiecīgā gadījumā tie būtu jāizstrādā arī iekļaujošā veidā, iesaistot attiecīgās ieinteresētās personas, piemēram, uzņēmēju un pilsoniskās sabiedrības organizācijas, akadēmiskās aprindas, pētniecības organizācijas, arodbiedrības un patērētāju aizsardzības organizāciju. Komisija var izstrādāt iniciatīvas, tostarp nozaru iniciatīvas, ar mērķi veicināt tādu tehnisko šķēršļu mazināšanu, kuri kavē pārrobežu datu apmaiņu MI izstrādei, tostarp par datu piekļuves infrastruktūru un dažādu veidu datu semantisko un tehnisko savietojamību.

- (166) Ir svarīgi, lai ar produktiem saistītas MI sistēmas, kuras saskaņā ar šo regulu nav augsta riska sistēmas un kurām līdz ar to nav jāatbilst prasībām, kas šajā regulā noteiktas augsta riska MI sistēmām, tomēr būtu drošas, kad tās tiek laistas tirgū vai nodotas ekspluatācijā. Minētā mērķa sekmēšanas nolūkā Eiropas Parlamenta un Padomes Regula (ES) 2023/988⁽⁵³⁾ tiktu piemērota kā drošības tīkls.
- (167) 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 saskaņā ar Savienības vai valsts tiesību aktiem. Tām savi uzdevumi un darbības būtu jāveic tā, lai jo īpaši aizsargātu intelektuālā īpašuma tiesības, konfidencialu uzņēmējdarbības informāciju un komercnoslēpumus, šīs regulas efektīvu īstenošanu, sabiedrības un valsts drošības intereses, kriminālprocesu un administratīvo procesu neaizskaramību un klasificētas informācijas integritāti.
- (168) Atbilstība šai regulai būtu jāpanāk, piemērojot sodus un citus izpildes panākšanas pasākumus. Dalībvalstīm būtu jāveic visi šīs regulas noteikumu īstenošanas nodrošināšanai nepieciešamie pasākumi, tostarp, nosakot iedarbīgus, samērīgus un atturošus sodus par noteikumu pārkāpumiem, un ievērojot *ne bis in idem* principu. Lai stiprinātu un saskaņotu administratīvos sodus par šīs regulas pārkāpumiem, būtu jāparedz maksimālais administratīvais naudas sods par konkrētiem specifiskiem pārkāpumiem. Novērtējot naudas sodu apmēru, dalībvalstīm katrā atsevišķā gadījumā būtu jāņem vērā visi attiecīgie konkrētās situācijas apstākļi, jo īpaši pienācīgi ņemot vērā pārkāpuma un tā seku raksturu, smagumu un ilgumu, kā arī nodrošinātāja lielumu, jo īpaši gadījumā, ja nodrošinātājs ir MVU, tostarp jaunuzņēmums. Eiropas Datu aizsardzības uzraudzītājam vajadzētu būt pilnvarotam uzlikt naudas sodus Savienības iestādēm, aģentūrām un struktūrām, kuras ietilpst šīs regulas piemērošanas jomā.
- (169) Atbilstība šajā regulā noteiktajiem vispārīga lietojuma MI modeļu nodrošinātāju pienākumiem būtu jāpanāk, cita starpā piemērojot naudas sodus. Šajā nolūkā būtu arī jānosaka atbilstošs naudas sodu apmērs par minēto pienākumu pārkāpumiem, tostarp par to pasākumu neievērošanu, kurus Komisija pieprasījusi saskaņā ar šo regulu, ievērojot atbilstīgus noilguma termiņus saskaņā ar proporcionālītātes principu. Visus lēmumus, ko saskaņā ar šo regulu pieņēmusi Komisija, var pārskatīt Eiropas Savienības Tiesa saskaņā ar LESD, tostarp Tiesas neierobežotajai jurisdikcijai attiecībā uz sankcijām, ievērojot LESD 261. pantu.
- (170) Savienības un valstu tiesību aktos jau ir paredzēti efektīvi tiesiskās aizsardzības līdzekļi fiziskām un juridiskām personām, kuru tiesības un brīvības nelabvēlīgi ietekmē MI sistēmu lietošana. Neskarot minētos tiesiskos aizsardzības līdzekļus, jebkurai fiziskai vai juridiskai personai, kurai ir pamats uzskatīt, ka ir pārkāpta šī regula, vajadzētu būt tiesīgai iesniegt sūdzību attiecīgajai tirgus uzraudzības iestādei.
- (171) Skartajām personām vajadzētu būt tiesībām saņemt paskaidrojumu, ja uzturētāja lēmums galvenokārt pamatojas uz iznākumu, kas iegūts no konkrētām augsta riska MI sistēmām, kuras ietilpst šīs regulas piemērošanas jomā, un ja minētais lēmums rada juridiskas sekas vai līdzīgā veidā būtiski ietekmē minētās personas tādā veidā, ka tās uzskata,

⁽⁵³⁾ Eiropas Parlamenta un Padomes Regula (ES) 2023/988 (2023. gada 10. maijs) par ražojumu vispārēju drošumu, ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1025/2012 un Eiropas Parlamenta un Padomes Direktīvu (ES) 2020/1828 un atceļ Eiropas Parlamenta un Padomes Direktīvu 2001/95/EK un Padomes Direktīvu 87/357/EEK (OV L 135, 23.5.2023., 1. lpp.).

ka tas nelabvēlīgi ietekmē to veselību, drošību vai pamattiesības. Minētajam skaidrojumam vajadzētu būt skaidram un jēgpilnam, un tam būtu jānodrošina pamats, saskaņā ar kuru skartās personas var īstenot savas tiesības. Tiesības saņemt paskaidrojumu nebūtu jāpiemēro tādu MI sistēmu lietošanai, attiecībā uz kurām izņēmumi vai ierobežojumi izriet no Savienības vai valsts tiesību aktiem, un tās būtu jāpiemēro tikai tiktāl, ciktāl šīs tiesības jau nav paredzētas Savienības tiesību aktos.

- (172) Personas, kas attiecībā uz šīs regulas pārkāpumiem rīkojas kā trauksmes cēļi, būtu jāaizsargā saskaņā ar Savienības tiesību aktiem. Tādēļ ziņošanai par šīs regulas pārkāpumiem un to personu aizsardzībai, kas ziņo par šādiem pārkāpumiem, būtu jāpiemēro Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1937 ⁽⁵⁴⁾.
- (173) Lai nodrošinātu, ka tiesisko regulējumu vajadzības gadījumā ir iespējams pielāgot, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu ar mērķi grozīt nosacījumus, saskaņā ar kuriem MI sistēma nav uzskatāma par augsta riska sistēmu, MI sistēmu sarakstu, noteikumus par tehnisko dokumentāciju, ES atbilstības deklarācijas saturu, noteikumus par atbilstības novērtēšanas procedūram, noteikumus, ar ko nosaka augsta riska MI sistēmas, kurām būtu jāpiemēro atbilstības novērtēšanas procedūra, kas balstīta uz kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtēšanu, maksimālo vērtību, kritērijus un rādītājus, tostarp, papildinot minētos kritērijus un rādītājus, noteikumus par vispārīga lietojuma MI modeļu ar sistēmisku risku klasificēšanu, vispārīga lietojuma MI modeļu ar sistēmisku risku izraudzīšanās kritērijus, tehnisko dokumentāciju vispārīga lietojuma MI modeļu nodrošinātājiem un informāciju par pārredzamību vispārīga lietojuma MI modeļu nodrošinātājiem. 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 procesu ⁽⁵⁵⁾. Jo īpaši, 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.
- (174) Ņemot vērā tehnoloģiju straujo attīstību un šīs regulas efektīvai piemērošanai nepieciešamās tehniskās zināšanas, Komisijai būtu jāizvērtē un jāpārskata šī regula līdz 2029. gada 2. augustam un pēc tam reizi četros gados un jāiesniedz ziņojums Eiropas Parlamentam un Padomei. Turklāt, ņemot vērā ietekmi uz šīs regulas piemērošanas jomu, Komisijai reizi gadā būtu jāveic novērtējums par nepieciešamību grozīt augsta riska MI sistēmu sarakstu un aizliegtās prakses sarakstu. Turklāt līdz 2028. gada 2. augustam un pēc tam reizi četros gados Komisijai būtu jāizvērtē un jāsniedz ziņojums Eiropas Parlamentam un Padomei par nepieciešamību grozīt augsta riska jomu sarakstu šīs regulas pielikumā, par MI sistēmām, kurām piemēro pārredzamības pienākumus, par uzraudzības un pārvaldības sistēmas efektivitāti un par vispārīga lietojuma MI modeļu energoefektīvas izstrādes standartizācijas nodevumu izstrādē gūto progresu, tostarp vajadzību pēc turpmākiem pasākumiem vai darbībām. Visbeidzot, līdz 2028. gada 2. augustam un pēc tam reizi trīs gados Komisijai būtu jāizvērtē brīvprātīgo rīcības kodeksu ietekme un efektivitāte, lai veicinātu prasību piemērošanu attiecībā uz MI sistēmām, kas nav augsta riska MI sistēmas, un, iespējams, citu papildu prasību piemērošanu attiecībā uz tādām MI sistēmām.
- (175) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ⁽⁵⁶⁾.
- (176) Ņemot vērā to, ka šīs regulas mērķi, proti, uzlabot iekšējā tirgus darbību un veicināt uz cilvēku orientēta un uzticama MI ieviešanu, vienlaikus nodrošinot augstu veselības, drošuma, Hartā nostiprināto pamattiesību, tostarp demokrātijas, tiesiskuma un vides aizsardzības, līmeni pret MI sistēmu radītām kaitīgām sekām Savienībā, un

⁽⁵⁴⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1937 (2019. gada 23. oktobris) par to personu aizsardzību, kuras ziņo par Savienības tiesību aktu pārkāpumiem (OV L 305, 26.11.2019., 17. lpp.).

⁽⁵⁵⁾ OV L 123, 12.5.2016., 1. lpp.

⁽⁵⁶⁾ 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.).

atbalstīt inovāciju, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet tās mēroga vai iedarbības dēļ to 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 minētā mērķa sasniegšanai.

- (177) Lai nodrošinātu juridisko noteiktību, nodrošinātu pienācīgu pielāgošanās laikposmu operatoriem un izvairītos no tirgus traucējumiem, tostarp nodrošinot MI sistēmu lietošanas nepārtrauktību, ir lietderīgi, ka šo regulu augsta riska MI sistēmām, kas laistas tirgū vai nodotas ekspluatācijā pirms tās vispārējās piemērošanas sākuma dienas, piemēro tikai tad, ja no minētā datuma šajās sistēmās notikušas būtiskas izmaiņas to uzbūvē vai to paredzētajā nolūkā. Ir lietderīgi precizēt, ka šajā sakarā jēdziens "būtiskas izmaiņas" būtu jāsaprot kā pēc būtības līdzvērtīgs jēdzienam "būtiska modifikācija", ko izmanto tikai attiecībā uz augsta riska MI sistēmām, ievērojot šo regulu. Izņēmuma kārtā un ņemot vērā publisko pārskatatbildību, to MI sistēmu operatoriem, kas ir tādu lielapjoma IT sistēmu sastāvdaļas, kas izveidotas ar šīs regulas pielikumā uzskaitītajiem tiesību aktiem, un to augsta riska MI sistēmu operatoriem, ko paredzēts izmantot publiskajās iestādēs, būtu jāveic nepieciešamie pasākumi, lai izpildītu šīs regulas prasības līdz 2030. gada beigām un līdz 2030. gada 2. augustam.
- (178) Augsta riska MI sistēmu nodrošinātāji tiek mudināti jau pārejas periodā brīvprātīgi sākt pildīt attiecīgos šajā regulā noteiktos pienākumus.
- (179) Šī regula būtu jāpiemēro no 2026. gada 2. augusta. Tomēr, ņemot vērā nepieņemamo risku, kas zināmā mērā ir saistīts ar MI lietošanu, aizliegumi, kā arī šīs regulas vispārīgie noteikumi būtu jāpiemēro jau no 2025. gada 2. februāra. Lai gan minēto aizliegumu pilnīga ietekme izriet no šīs regulas pārvaldības un izpildes panākšanas, ir svarīgi paredzēt aizliegumu piemērošanu, lai ņemtu vērā nepieņemamus riskus un ietekmētu citas procedūras, piemēram, civiltiesību jomā. Turklāt ar pārvaldi un atbilstības novērtēšanu saistītajai infrastruktūrai būtu jāsāk darboties pirms 2026. gada 2. augusta, tāpēc noteikumi par paziņotajām struktūrām un pārvaldes struktūru būtu jāpiemēro no 2025. gada 2. augusta. ņemot vērā straujo tempu, kādā attīstās tehnoloģijas un tiek pieņemti vispārīga lietojuma MI modeļi, pienākumi vispārīga lietojuma MI modeļu nodrošinātājiem būtu jāpiemēro no 2025. gada 2. augusta. Prakses kodeksiem vajadzētu būt gataviem līdz 2025. gada 2. maijam, lai nodrošinātāji varētu savlaicīgi apliecināt atbilstību. MI birojam būtu jānodrošina, ka klasificēšanas noteikumi un procedūras tiek atjauninātas, ņemot vērā tehnoloģiju attīstību. Turklāt dalībvalstīm būtu jānosaka noteikumi par sodiem, tostarp administratīviem naudas sodiem, un tie jāpaziņo Komisijai, un jānodrošina to pienācīga un efektīva īstenošana līdz šīs regulas piemērošanas sākuma dienai. Tāpēc noteikumi par sodiem būtu jāpiemēro no 2025. gada 2. augusta.
- (180) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. un 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju un Eiropas Datu aizsardzības kolēģiju, kas 2021. gada 18. jūnijā sniedza kopīgu atzinumu,

IR PIENĒMUŠI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

1. Šīs regulas mērķis ir uzlabot iekšējā tirgus darbību un veicināt uz cilvēku orientēta un uzticama mākslīgā intelekta (MI) izmantošanu, vienlaikus nodrošinot augstu veselības, drošuma, Hartā nostiprināto pamattiesību, tostarp demokrātijas un tiesiskuma, un vides aizsardzības līmeni pret MI sistēmu radītām kaitīgām sekām Savienībā, un atbalstot inovāciju.

2. Šī regula nosaka:

a) saskaņotus noteikumus par MI sistēmu laišanu tirgū, nodošanu ekspluatācijā un izmantošanu Savienībā;

- b) dažas MI prakses aizliegumus;
- c) konkrētas prasības augsta riska MI sistēmām un pienākumus šādu sistēmu operatoriem;
- d) saskaņotus pārredzamības noteikumus dažām MI sistēmām;
- e) saskaņotus noteikumus par vispārīga lietojuma MI modeļu laišanu tirgū;
- f) tirgus pārraudzības, tirgus uzraudzības pārvaldības un izpildes panākšanas noteikumus;
- g) pasākumus inovācijas atbalstam, īpašu uzmanību pievēršot MVU, tostarp jaunuzņēmumiem.

2. pants

Darbības joma

1. Šo regulu piemēro:

- a) nodrošinātājiem, kas Savienībā laiž tirgū vai nodod ekspluatācijā MI sistēmas vai laiž tirgū vispārīga lietojuma MI modeļus, neatkarīgi no tā, vai minētie nodrošinātāji ir iedibināti vai atrodas Savienībā jeb vai trešā valstī;
- b) MI sistēmu uzturētājiem, kuru iedibinājuma vieta ir Savienībā vai kuri atrodas Savienībā;
- c) tādu MI sistēmu nodrošinātājiem un uzturētājiem, kuru iedibinājuma vieta ir vai kuri atrodas trešā valstī, ja MI sistēmas radīto iznākumu izmanto Savienībā;
- d) MI sistēmu importētājiem un izplatītājiem;
- e) produktu ražotājiem, kas laiž tirgū vai nodod ekspluatācijā MI sistēmu kopā ar savu produktu un ar savu nosaukumu vai preču zīmi;
- f) nodrošinātāju pilnvarotiem pārstāvjiem, kuri nav iedibināti Savienībā;
- g) skartajām personām, kas atrodas Savienībā.

2. MI sistēmām, kas klasificētas kā augsta riska MI sistēmas saskaņā ar 6. panta 1. punktu saistībā ar produktiem, uz kuriem attiecas I pielikuma B iedaļā minētie Savienības saskaņošanas tiesību akti, piemēro tikai 6. panta 1. punktu, 102. līdz 109. pantu un 112. pantu. Regulas 57. pantu piemēro tikai tiktāl, ciktāl šajā regulā paredzētās prasības augsta riska MI sistēmām ir integrētas minētajos Savienības saskaņošanas tiesību aktos.

3. Šī regula neattiecas uz jomām, kas ir ārpus Savienības tiesību tvēruma, un tā jebkurā gadījumā neietekmē dalībvalstu kompetences attiecībā uz valsts drošību neatkarīgi no tā, kāda veida vienībai dalībvalstis ir uzticējušas veikt uzdevumus saistībā ar minētajām kompetencēm.

Šī regula neattiecas uz MI sistēmām, ja un ciktāl tās tiek laistas tirgū, nodotas ekspluatācijā vai izmantotas ar modifikāciju vai bez tās vienīgi militāros, aizsardzības vai valsts drošības nolūkos, neatkarīgi no tā, kāda veida vienība veic minētās darbības.

Šī regula neattiecas uz MI sistēmām, kuras netiek laistas tirgū vai nodotas ekspluatācijā Savienībā, ja iznākumu Savienībā izmanto vienīgi militāros, aizsardzības vai valsts drošības nolūkos, neatkarīgi no tā, kāda veida vienība veic minētās darbības.

4. Šī regula neattiecas ne uz publiskām iestādēm trešā valstī, ne starptautiskām organizācijām, kas ir šīs regulas piemērošanas jomā, ievērojot 1. punktu, ja minētās iestādes vai organizācijas izmanto MI sistēmas starptautiskās sadarbības vai nolīgumu ietvaros par tiesībaizsardzības un tiesu iestāžu sadarbību ar Savienību vai ar vienu vai vairākām dalībvalstīm, ar noteikumu, ka šāda trešā valsts vai starptautiskā organizācija sniedz pietiekamas garantijas attiecībā uz individuālo pamattiesību un pamatbrīvību aizsardzību.

5. Šī regula neietekmē to noteikumu piemērošanu, kuri attiecas uz starpnieku pakalpojumu sniedzēju atbildību, kā paredzēts Regulas (ES) 2022/2065 II nodaļā.

6. Šī regula neattiecas uz MI sistēmām vai MI modeļiem, tostarp to radīto iznākumu, kas konkrēti izstrādāti un nodoti ekspluatācijā vienīgi zinātniskās pētniecības un izstrādes nolūkā.
7. Personas datiem, ko apstrādā saistībā ar šajā regulā noteiktajām tiesībām un pienākumiem, piemēro Savienības tiesību aktus personas datu aizsardzības, privātuma un sakaru konfidencialitātes jomā. Šī regula neietekmē Regulu (ES) 2016/679 vai (ES) 2018/1725, vai Direktīvu 2002/58/EK vai (ES) 2016/680, neskarot šīs regulas 10. panta 5. punktu un 59. pantu.
8. Šī regula neattiecas uz pētniecības, testēšanas vai izstrādes darbībām, kas saistītas ar MI sistēmām vai MI modeļiem pirms to laišanas tirgū vai nodošanas ekspluatācijā. Šādas darbības veic saskaņā ar piemērojamiem Savienības tiesību aktiem. Minētā izslēgšana neattiecas uz testēšanu reālos apstākļos.
9. Šī regula neskar noteikumus, kas paredzēti citos Savienības tiesību aktos, kuri saistīti ar patērētāju aizsardzību un produktu drošumu.
10. Šī regula neattiecas uz tādu uzturētāju pienākumiem, kuri ir fiziskas personas, kas MI sistēmas izmanto tikai personiskas neprofesionālas darbības veikšanai.
11. Šī regula neliedz Savienībai vai dalībvalstīm saglabāt vai ieviest tiesību aktus, noteikumus vai administratīvas normas, kas ir labvēlīgākas pret darba ņēmējiem viņu tiesību aizsardzības ziņā attiecībā uz situācijām, kad darba devējs izmanto MI sistēmas, vai veicināt vai atļaut darba ņēmējiem izdevīgāku koplīgumu piemērošanu.
12. Šī regula neattiecas uz MI sistēmām, kas laistas apgrozībā ar bezmaksas un atklātā pirmkoda licencēm, ja vien tās netiek laistas tirgū vai nodotas ekspluatācijā kā augsta riska MI sistēmas vai kā MI sistēma, uz kuru attiecas 5. vai 50. pants.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

- 1) “MI sistēma” ir mašinizēta sistēma, kura projektēta darboties ar dažādiem autonomijas līmeņiem, kura var pēc ieviešanas būt adaptīva, un kura ekspluatācijā ir implīcītiem mērķiem secina no informācijas, ko tā saņem, kā ģenerēt iznākumus, piemēram, prognozes, saturu, ieteikumus vai lēmumus, kas var ietekmēt fizisko vai virtuālo vidi;
- 2) “risks” ir kaitējuma rašanās varbūtības un minētā kaitējuma smaguma kombinācija;
- 3) “nodrošinātājs” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura par samaksu vai par brīvu izstrādā MI sistēmu vai vispārīga lietojuma MI modeli vai kura liek izstrādāt MI sistēmu vai vispārīga lietojuma MI modeli un laiž to tirgū vai nodod MI sistēmu ekspluatācijā ar savu nosaukumu/vārdu vai preču zīmi;
- 4) “uzturētājs” ir fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura lieto MI sistēmu, kas ir tās pārziņā, izņemot gadījumus, kad MI sistēmu lieto personiskas neprofesionālas darbības veikšanai;
- 5) “pilnvarotais pārstāvis” ir jebkura fiziska vai juridiska persona, kas atrodas vai ir iedibināta Savienībā un ir saņēmusi un akceptējusi rakstisku pilnvarojumu no MI sistēmas vai vispārīga lietojuma MI modeļa nodrošinātāja, lai tā vārdā attiecīgi veiktu un pildītu šajā regulā noteiktos pienākumus un procedūras;
- 6) “importētājs” ir jebkura fiziska vai juridiska persona, kas atrodas vai ir iedibināta Savienībā un laiž tirgū MI sistēmu ar trešā valstī iedibinātas fiziskas vai juridiskas personas nosaukumu/vārdu vai preču zīmi;
- 7) “izplatītājs” ir jebkura fiziska vai juridiska persona piegādes ķēdē, kas nav nodrošinātājs vai importētājs un kas MI sistēmu dara pieejamu Savienības tirgū;
- 8) “operators” ir nodrošinātājs, produkta ražotājs, uzturētājs, pilnvarotais pārstāvis, importētājs vai izplatītājs;

- 9) "laist tirgū" nozīmē pirmo reizi MI sistēmu vai vispārīga lietojuma MI modeli darīt pieejamu Savienības tirgū;
- 10) "darīt pieejamu tirgū" nozīmē, veicot komercdarbību, par samaksu vai par brīvu piegādāt MI sistēmu vai vispārīga lietojuma MI modeli izplatīšanai vai lietošanai Savienības tirgū;
- 11) "nodot ekspluatācijā" nozīmē MI sistēmas piegādi pirmajai lietošanai tieši uzturētājam vai pašu lietošanai Savienībā tai paredzētajā nolūkā;
- 12) "paredzētais nolūks" ir lietojums, kuram nodrošinātājs ir paredzējis MI sistēmu, arī konkrētais konteksts un lietošanas nosacījumi, kas norādīti nodrošinātāja sniegtajā informācijā, kura iekļauta lietošanas instrukcijā, reklāmas vai pārdošanas materiālos un paziņojumos, kā arī tehniskajā dokumentācijā;
- 13) "saprātīgi paredzama nepareiza lietošana" ir MI sistēmas lietošana tādā veidā, kas neatbilst tai paredzētajam nolūkam, bet var rasties no saprātīgi paredzamas cilvēka rīcības vai mijiedarbības ar citām sistēmām, tai skaitā citām MI sistēmām;
- 14) "drošības sastāvdaļa" ir produkta vai MI sistēmas sastāvdaļa, kura pilda šā produkta vai MI sistēmas drošības funkciju vai kuras atteice vai darbības traucējumi apdraud personu veselību un drošību vai īpašuma drošību;
- 15) "lietošanas instrukcija" ir informācija, ko sniedz nodrošinātājs, lai uzturētāju informētu jo īpaši par MI sistēmas paredzēto nolūku un pareizu lietošanu;
- 16) "MI sistēmas atsaukšana" ir jebkurš pasākums, kura mērķis ir panākt MI sistēmas, kas ir darīta uzturētājiem pieejama, atpakaļnododšanu nodrošinātājam vai izņemšanu no ekspluatācijas, vai lietošanas atspējošanu;
- 17) "MI sistēmas izņemšana" ir katrs pasākums, kura mērķis ir novērst to, ka piegādes ķēdē esoša MI sistēma tiek darīta pieejama tirgū;
- 18) "MI sistēmas veikspēja" ir MI sistēmas spēja sasniegt tai paredzēto nolūku;
- 19) "paziņojošā iestāde" ir valsts iestāde, kas atbild par vajadzīgo procedūru izveidi un izpildi atbilstības novērtēšanas struktūru novērtēšanai, izraudzīšanai un paziņošanai, kā arī to pārraudzībai;
- 20) "atbilstības novērtēšana" ir process, kurā apliecina, vai ir izpildītas šīs regulas III nodaļas 2. iedaļā noteiktās prasības, kas attiecas uz augsta riska MI sistēmu;
- 21) "atbilstības novērtēšanas struktūra" ir struktūra, kas kā trešā persona veic atbilstības novērtēšanas darbības, ieskaitot testēšanu, sertifikāciju un pārbaudi;
- 22) "paziņotā struktūra" ir atbilstības novērtēšanas struktūra, kas paziņota saskaņā ar šo regulu un citiem attiecīgajiem Savienības saskaņošanas tiesību aktiem;
- 23) "būtiska modifikācija" ir tādas MI sistēmas izmaiņas pēc tās laišanas tirgū vai nodošanas ekspluatācijā, kuras nav paredzētas vai plānotas sākotnējā riska novērtējumā, ko veic nodrošinātājs, un kuru dēļ ir ietekmēta MI sistēmas atbilstība II nodaļas 2. iedaļā noteiktajām prasībām vai kuru dēļ tiek mainīts paredzētais nolūks, attiecībā uz kuru MI sistēma ir novērtēta;
- 24) "CE zīme" ir marķējums, ar kuru nodrošinātājs norāda, ka MI sistēma atbilst prasībām, kas paredzētas III nodaļas 2. iedaļā un citos piemērojamos Savienības saskaņošanas tiesību aktos, un kas paredz tās uzlikšanu;
- 25) "pēcirtgus pārraudzības sistēma" ir visas darbības, ko MI sistēmu nodrošinātāji veic, lai apkopotu un pārskatītu pieredzi, kura gūta, lietojot MI sistēmas, ko tie laiž tirgū vai nodod ekspluatācijā, ar mērķi identificēt vajadzību nekavējoties piemērot nepieciešamās korektīvās vai preventīvās darbības;
- 26) "tirgus uzraudzības iestāde" ir valsts iestāde, kas veic darbības un pasākumus, ievērojot Regulu (ES) 2019/1020;

- 27) "saskaņots standarts" ir saskaņots standarts, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta c) apakšpunktā;
- 28) "kopīgā specifikācija" ir tehnisko specifikāciju kopums, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 4. punktā, kas nodrošina līdzekļus dažu šajā regulā noteiktu prasību izpildei;
- 29) "apmācības dati" ir dati, ko izmanto MI sistēmas apmācībai, pielāgojot tās apgūstamos parametrus;
- 30) "validēšanas dati" ir dati, ko izmanto apmācītās MI sistēmas izvērtēšanai un tās neapgūstamo parametru un mācību procesa pielāgošanai, lai cita starpā novērstu nepietiekamu vai pārmērīgu pielāgošanu;
- 31) "validēšanas datu kopa" ir atsevišķa datu kopa vai apmācības datu kopas daļa, kā vai nu fiksēts, vai mainīgs tās sadalījums;
- 32) "testēšanas dati" ir dati, ko izmanto, lai nodrošinātu MI sistēmas neatkarīgu izvērtēšanu nolūkā apstiprināt šīs sistēmas sagaidāmo veiktspēju pirms tās laišanas tirgū vai nodošanas ekspluatācijā;
- 33) "ievaddati" ir MI sistēmā ievadītie vai tās tieši iegūtie dati, pamatojoties uz kuriem, šī sistēma rada iznākumu;
- 34) "biometriskie dati" ir personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, piemēram, sejas attēli vai daktiloskopiskie dati;
- 35) "biometriskā identifikācija" ir cilvēka fizisko, fizioloģisko, uzvedības vai psiholoģisko īpašību automatizēta atpazīšana nolūkā noskaidrot fiziskas personas identitāti, salīdzinot minētā indivīda biometriskos datus ar datubāzē glabātiem indivīdu biometriskajiem datiem;
- 36) "biometriskā verifikācija" ir automatizēta fizisku personu identitātes verifikācija "viens pret vienu", tostarp autentifikācija, kas notiek, fiziskas personas biometriskos datus salīdzinot ar iepriekš sniegtiem biometriskajiem datiem;
- 37) "īpašu kategoriju personas dati" ir personas datu kategorijas, kas minētas Regulas (ES) 2016/679 9. panta 1. punktā, Direktīvas (ES) 2016/680 10. pantā un Regulas (ES) 2018/1725 10. panta 1. punktā;
- 38) "sensitīvi operatīvie dati" ir ar noziedzīgu nodarījumu novēršanas, atklāšanas, izmeklēšanas vai kriminālvajāšanas darbībām saistīti operatīvie dati, kuru izpaušana varētu apdraudēt kriminālprocesa integritāti;
- 39) "emociju atpazīšanas sistēma" ir MI sistēma, kuras mērķis ir identificēt vai izsecināt fizisku personu emocijas vai nodomus, pamatojoties uz viņu biometriskajiem datiem;
- 40) "biometriskās kategorizācijas sistēma" ir MI sistēma, kuras mērķis ir noteikt fizisku personu piederību konkrētām kategorijām, pamatojoties uz viņu biometriskajiem datiem, ja vien tas nepapildina citus komercpakalpojumus un nav absolūti nepieciešams objektīvu tehnisku iemeslu dēļ;
- 41) "biometriskās tālidentifikācijas sistēma" ir MI sistēma, kuras nolūks ir identificēt fiziskas personas bez to aktīvas iesaistīšanas, parasti no attāluma salīdzinot personas biometriskos datus ar atsauces datubāzē esošajiem biometriskajiem datiem;
- 42) "reāllaika biometriskās tālidentifikācijas sistēma" ir biometriskās tālidentifikācijas sistēma, kurā biometrisko datu uztveršana, salīdzināšana un identificēšana notiek bez būtiskas aiztures, ietverot ne tikai tūlītēju identifikāciju, bet arī ierobežotu īslaicīgu aizturi, lai novērstu apiešanu;
- 43) "vēlāklaika biometriskās tālidentifikācijas sistēma" ir biometriskās tālidentifikācijas sistēma, kas nav reāllaika biometriskās tālidentifikācijas sistēma;
- 44) "publiski pieklūstama vieta" ir jebkura publiskā vai privātā īpašumā esoša fiziska vieta, kas ir pieklūstama nenoteiktam skaitam fizisku personu, neatkarīgi no tā, vai var būt piemērojami daži konkrēti piekļuves nosacījumi, un neatkarīgi no iespējamās kapacitātes ierobežojumiem;

- 45) "tiesībaizsardzības iestāde" ir:
- a) publiska iestāde, kuras kompetencē ir novērst, izmeklēt, atklāt noziedzīgus nodarījumus vai saukt pie atbildības par tiem, vai izpildīt kriminālsodus, tostarp pasargāt no draudiem sabiedriskajai drošībai un tos novērst; vai
 - b) cita struktūra vai vienība, kurai dalībvalsts tiesībās uzticēts īstenot publisku varu un publiskas pilnvaras ar mērķi novērst, izmeklēt atklāt noziedzīgus nodarījumus vai saukt pie atbildības par tiem, vai izpildīt kriminālsodus, tostarp pasargāt no draudiem sabiedriskajai drošībai un tos novērst;
- 46) "tiesībaizsardzība" ir darbības, ko veic tiesībaizsardzības iestādes vai to vārdā, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu;
- 47) "MI birojs" ir Komisijas funkcija, ar kuru sniedz ieguldījumu MI sistēmu un vispārīga lietojuma MI modeļu pārvaldības īstenošanā, pārraudzībā un uzraudzībā, ko paredz Komisijas 2024. gada 24. janvāra lēmumu; atsaucies uz MI biroju šajā regulā saprot kā atsaucies uz Komisiju;
- 48) "valsts kompetentā iestāde" ir paziņojošā iestāde vai tirgus uzraudzības iestāde; attiecībā uz MI sistēmām, ko nodod ekspluatācijā vai izmanto Savienības iestādes, aģentūras, biroji un struktūras, atsaucies uz valstu kompetentajām iestādēm vai tirgus uzraudzības iestādēm šajā regulā ir atsaucies uz Eiropas Datu aizsardzības uzraudzītāju;
- 49) "nopietns incidents" ir jebkurš incidents vai MI sistēmas darbības traucējums, kas tieši vai netieši izraisa kādas no šīm sekām:
- a) personas nāve vai nopietns kaitējums personas veselībai;
 - b) nopietni un neatgriezeniski kritiskās infrastruktūras pārvaldības vai darbības traucējumi;
 - c) Savienības tiesību aktos pamattiesību aizsardzībai paredzēto pienākumu pārkāpums;
 - d) nopietns kaitējums īpašumam vai videi;
- 50) "personas dati" ir personas dati, kā definēts Regulas (ES) 2016/679 4. panta 1. punktā;
- 51) "nepersondati" ir dati, kas nav Regulas (ES) 2016/679 4. panta 1. punktā definētie personas dati;
- 52) "profilēšana" ir profilēšana, kā definēts Regulas (ES) 2016/679 4. panta 4. punktā;
- 53) "testēšanas reālos apstākļos plāns" ir dokuments, kurā aprakstīti testēšanas mērķi, metodika, ģeogrāfiskais, iedzīvotāju skaita un laika tvērums, pārraudzība, organizācija un veikšana reālos apstākļos;
- 54) "smilškastēs" plāns" ir dokuments, par kuru vienojušies iesaistītais nodrošinātājs un kompetentā iestāde un kurā aprakstīti smilškastēs satvarā veicamo pasākumu mērķi, nosacījumi, laika grafiks, metodika un prasības;
- 55) "MI "regulatīvā smilškastē"" ir kontrolēts satvars, ko izveido valsts kompetentā iestāde un kas piedāvā MI sistēmu nodrošinātājiem vai potenciālajiem nodrošinātājiem iespēju izstrādāt, apmācīt, validēt un attiecīgā gadījumā reālos apstākļos testēt inovatīvu MI sistēmu, ievērojot smilškastēs plānu uz ierobežotu laiku regulatīvās uzraudzības ietvaros;
- 56) "MI pratība" ir prasmes, zināšanas un izpratne, kas nodrošinātājiem, uzturētājiem un skartajām personām dod iespēju, ņemot vērā to tiesības un pienākumus šīs regulas kontekstā, veikt MI sistēmu informētu uzturēšanu, kā arī gūt izpratni par MI iespējām un riskiem un par potenciālo kaitējumu, ko tas var radīt;

- 57) "testēšana reālos apstākļos" ir MI sistēmas pagaidu testēšana tai paredzētajam nolūkam reālos apstākļos ārpus laboratorijas vai citādi simulētas vides, lai vāktu uzticamus un robustus datus un novērtētu un verificētu MI sistēmas atbilstību šīs regulas prasībām, un to neuzskata par MI sistēmas laišanu tirgū vai nodošanu ekspluatācijā šīs regulas nozīmē, ar noteikumu, ka ir izpildīti visi 57. vai 60. panta nosacījumi;
- 58) "subjekts" saistībā ar testēšanu reālos apstākļos ir fiziska persona, kas piedalās testēšanā reālos apstākļos;
- 59) "informēta piekrišana" ir subjekta labprātīgi, konkrēti, nepārprotami un brīvprātīgi pausta gatavība piedalīties konkrētā testēšanā reālos apstākļos pēc tam, kad tas ir saņēmis informāciju par visiem testēšanas aspektiem, kuri ir būtiski subjekta lēmumam tajā piedalīties;
- 60) "dziļviltojums" ir MI ģenerēts vai manipulēts attēls, audio vai video saturs, kurš atgādina reālas personas, priekšmetus, vietas, vienības vai notikumus un maldinātu personu, ka attiecīgais saturs ir autentisks vai patiess;
- 61) "plašas ietekmes pārkāpums" ir jebkura darbība vai bezdarbība, kas ir pretrunā Savienības tiesību aktiem, kuri aizsargā indivīdu intereses, un kas:
- a) ir kaitējusi vai varētu kaitēt tādu indivīdu kolektīvajām interesēm, kuri dzīvo vismaz divās dalībvalstīs, no kurām neviena nav tā pati dalībvalsts, kurā:
 - i) sākusies vai notikusi attiecīgā darbība vai bezdarbība,
 - ii) atrodas vai ir iedibināts attiecīgais nodrošinātājs vai, attiecīgā gadījumā, tā pilnvarotais pārstāvis; vai
 - iii) ir iedibināts uzturētājs, ja pārkāpumu ir izdarījis uzturētājs;
 - b) ir radījusi, rada vai, iespējams, radīs kaitējumu indivīdu kolektīvajām interesēm, un kam ir kopīgas iezīmes, tostarp tā ir viena un tā pati nelikumīgā prakse vai tiek pārkāptas vienas un tās pašas intereses, un ko viens un tas pats operators vienlaikus izdara vismaz trīs dalībvalstīs;
- 62) "kritiskā infrastruktūra" ir kritiskā infrastruktūra, kā definēts Direktīvas (ES) 2022/2557 2. panta 4. punktā;
- 63) "vispārīga lietojuma MI modelis" ir MI modelis – tostarp, ja šāds MI modelis ir apmācīts ar lielu datu apjomu, izmantojot pašuzraudzību plašā mērogā –, kuram piemīt ievērojams vispārīgums un kurš spēj kompetenti veikt plašu atšķirīgu uzdevumu klāstu neatkarīgi no tā, kādā veidā modelis ir laists tirgū, un kuru var integrēt dažādās lejasposma sistēmās vai lietotnēs, izņemot MI modeļus, ko pirms to laišanas tirgū izmanto pētniecības, izstrādes vai prototipu izstrādes darbībām;
- 64) "augstas ietekmes spējas" ir spējas, kas atbilst vai pārsniedz spējas, kuras ir iekļautas modernākajos vispārīga lietojuma MI modeļos;
- 65) "sistēmisks risks" ir risks, kas konkrēti piemīt vispārīga lietojuma MI modeļu augstas ietekmes spējām, kam ir būtiska ietekme uz Savienības tirgu to tvēruma dēļ vai faktisku vai saprātīgi paredzamu negatīvu seku dēļ uz sabiedrības veselību, drošumu, sabiedrisko drošību, pamattiesībām vai uz sabiedrību kopumā, un kas var plaši izplatīties visā vērtības ķēdē;
- 66) "vispārīga lietojuma MI sistēma" ir MI sistēma, kura ir balstīta uz vispārīga lietojuma MI modeli, un kam ir spējas kalpot dažādiem mērķiem gan saistībā ar tiešo lietojumu, gan integrēšanu citās MI sistēmās;
- 67) "peldošā komata operācija" ir jebkura matemātiska darbība vai vērtības piešķiršana, kurā izmanto skaitļus ar peldošo komatu, kas ir reālo skaitļu apakškopa un kurus datoros parasti attēlo kā noteiktas precizitātes veselu skaitli, reizinātu ar veselu skaitli, kurš kāpināts noteiktā veselā pakāpē;
- 68) "lejasposma nodrošinātājs" ir MI sistēmas, tostarp vispārīga lietojuma MI sistēmas, kas integrē MI modeli, nodrošinātājs neatkarīgi no tā, vai MI modeli nodrošina pats un to vertikāli integrē, vai to nodrošina cita vienība, pamatojoties uz līgumattiecībām.

4. pants

MI pratība

MI sistēmu nodrošinātāji un uzturētāji veic pasākumus, ar ko cik iespējams labi nodrošina pietiekamu MI pratības līmeni savam personālam un citām personām, kuras to vārdā iesaistītas MI sistēmu darbībā un izmantošanā, ņemot vērā viņu tehniskās zināšanas, pieredzi, izglītību un apmācību un MI sistēmu izmantošanai paredzēto kontekstu, kā arī ņemot vērā personas vai personu grupas, attiecībā uz ko MI sistēmas paredzēts lietot.

II NODAĻA

AIZLIEGTA MI PRAKSE

5. pants

Aizliegta MI prakse

1. Ir aizliegta šāda MI prakse:

- a) tādas MI sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kas izmanto cilvēka neapzinātus subliminālus paņēmienus vai tīši manipulatīvus vai maldinošus paņēmienus, kuru mērķis ir būtiski iespaidot personas vai personu grupas uzvedību vai kuriem ir tādas sekas, kas ievērojami pasliktina viņu spēju pieņemt informētu lēmumu, tādējādi liekot tām pieņemt lēmumu, ko tās citādi nebūtu pieņēmušas, tādā veidā, kas šai personai, citai personai vai personu grupai rada vai pamatoti ticami radīs būtisku kaitējumu;
- b) tādas MI sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana, kura izmanto kādu no kādas fiziskas personas vai konkrētas personu grupas neaizsargātības iezīmēm viņu vecuma, invaliditātes vai konkrētas sociālās vai ekonomiskās situācijas dēļ un kuras mērķis vai sekas ir minētās personas vai minētajai grupai piederīgas personas uzvedības būtiska iespaidošana tādā veidā, kas attiecīgajai personai vai citai personai rada vai ir saprātīgi iespējams, ka radīs būtisku kaitējumu;
- c) MI sistēmu laišana tirgū, nodošana ekspluatācijā vai lietošana nolūkā izvērtēt vai klasificēt fiziskas personas vai personu grupas noteiktā laikposmā, pamatojoties uz viņu sociālo uzvedību vai zināmām, izsecinātām vai prognozētām personas vai personības īpašībām, ja sociālais novērtējums ved pie viena vai abiem šādiem iznākumiem:
 - i) kaitējoša vai nelabvēlīga attieksme pret dažām fiziskām personām vai personu grupām sociālos kontekstos, kas nav saistīti ar kontekstiem, kuros dati tika sākotnēji ģenerēti vai savākti;
 - ii) kaitējoša vai nelabvēlīga attieksme pret dažām fiziskām personām vai personu grupām, kas nav pamatota vai nav samērīga ar viņu sociālo uzvedību vai tās smagumu;
- d) MI sistēmas laišana tirgū, nodošana ekspluatācijā šim konkrētajam mērķim vai lietošana fizisku personu radītā riska novērtējuma veikšanai, lai novērtētu vai prognozētu risku, ka fiziska persona varētu izdarīt noziedzīgu nodarījumu, kura balstās vienīgi uz fiziskas personas profilēšanu vai uz tās personisko īpašību un rakstura iezīmju novērtēšanu; šo aizliegumu nepiemēro MI sistēmām, kuras izmanto, lai atbalstītu cilvēka veiktu novērtējumu par personas iesaistīšanos noziedzīgā darbībā, kurš jau ir balstīts uz objektīviem un pārbaudāmiem faktiem, kas ir tieši saistīti ar noziedzīgu darbību;
- e) tādu MI sistēmu laišana tirgū, nodošana ekspluatācijā šim konkrētajam mērķim vai lietošana, kuras izveido vai paplašina sejas atpazīšanas datubāzes, nemērķorientēti rasmējot sejas attēlus no interneta vai videonovērošanas sistēmu video;
- f) MI sistēmu laišana tirgū, nodošana ekspluatācijā šim konkrētajam mērķim vai lietošana fiziskas personas emociju izsecināšanai darbavietā vai izglītības iestādēs, izņemot tad, ja MI sistēmas izmantošanu paredzēts ieviest vai laist tirgū medicīnisku vai drošības iemeslu dēļ;

- g) tādu biometriskās kategorizācijas sistēmu laišana tirgū vai nodošana ekspluatācijā, vai lietošana, kuras individuāli kategorizē fiziskas personas, pamatojoties uz viņu biometriskajiem datiem, lai atvedinātu vai izsecinātu viņu rasi, politiskos uzskatus, dalību arodbiedrībās, reliģiskos vai filozofiskos uzskatus, dzimumdzīvi vai seksuālo orientāciju; šis aizliegums neattiecas uz likumīgi iegūtu biometrisko datu kopu, piemēram, attēlu, marķēšanu vai filtrēšanu, pamatojoties uz biometriskajiem datiem, vai biometrisko datu kategorizēšanu tiesībsardzības jomā;
- h) reāllaika biometriskās tālidentifikācijas sistēmu izmantošana publiski pieklūstamās vietās tiesībsardzības nolūkos, izņemot tad, ja – un tiklīdz, cik – tāda izmantošana ir absolūti nepieciešama kādam no šiem mērķiem:
- i) konkrētu nolaupīšanas, cilvēku tirdzniecības vai cilvēku seksuālas izmantošanas upuru mērķtiecīga meklēšana, kā arī bezvēsts pazudušu personu meklēšana;
 - ii) konkrēta, būtiska un nenovēršama apdraudējuma fizisku personu dzīvībai vai fiziskai drošībai vai reālu un pašreizēju vai reālu un paredzamu teroristu uzbrukuma draudu novēršana;
 - iii) par noziedzīga nodarījuma izdarīšanu aizdomās turētas personas atrašanās vietas noteikšana vai personas identificēšana nolūkā veikt kriminālizmeklēšanu vai kriminālvajāšanu vai kriminālsoda izpildi par II pielikumā minētajiem nodarījumiem, par kuriem attiecīgajā dalībvalstī var piemērot brīvības atņemšanas sodu vai ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz četri gadi.

Pirmās daļas h) punkts neskar Regulas (ES) 2016/679 9. pantu attiecībā uz biometrisko datu apstrādi nolūkos, kas nav tiesībsardzība.

2. Reāllaika biometriskās tālidentifikācijas sistēmu lietošanu publiski pieklūstamās vietās tiesībsardzības nolūkos ar kādu no 1. punkta pirmās daļas h) apakšpunktā minētajiem mērķiem ievieš minētajā punktā noteiktajos nolūkos, lai apstiprinātu konkrētas personas identitāti, un tajā ņem vērā šādus elementus:

- a) tās situācijas raksturs, kuras dēļ var notikt tāda lietošana, jo īpaši tā kaitējuma smagums, iespējamība un apmērs, kas tiktu radīts, ja sistēma netiktu lietota;
- b) sistēmas lietošanas sekas attiecībā uz visu attiecīgo personu tiesībām un brīvībām, jo īpaši minēto seku smagums, iespējamība un apmērs.

Turklāt reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski pieklūstamās vietās tiesībsardzības nolūkos šā panta 1. punkta pirmās daļas h) apakšpunktā minētajiem mērķiem atbilst nepieciešamiem un samērīgiem aizsardzības pasākumiem un nosacījumiem attiecībā uz lietošanu saskaņā ar valsts tiesību aktiem, kuri atļauj to lietošanu, jo īpaši laika, ģeogrāfisku un personisku ierobežojumu ziņā. Reāllaika biometriskās tālidentifikācijas sistēmu lietošanu publiski pieklūstamās vietās atļauj vienīgi tad, ja tiesībsardzības iestāde ir pabeigusi 27. pantā paredzēto novērtējumu par ietekmi uz pamattiesībām un ir reģistrējusi sistēmu ES datubāzē saskaņā ar 49. pantu. Tomēr pienācīgi pamatotos steidzamos gadījumos šādu sistēmu lietošanu var sākt bez reģistrācijas ES datubāzē ar noteikumu, ka šāda reģistrācija tiek pabeigta bez liekas kavēšanās.

3. Šā panta 1. punkta pirmās daļas h) apakšpunkta un 2. punkta nolūkos katrai reāllaika biometriskās tālidentifikācijas sistēmas lietošanai tiesībsardzības nolūkos publiski pieklūstamās vietās ir nepieciešama iepriekšēja atļauja, ko izsniegusi tiesu iestāde vai neatkarīga administratīvā iestāde, kuras lēmums ir saistošs, tajā dalībvalstī, kurā šo sistēmu paredzēts lietot, un kas izsniegta pēc pamatota pieprasījuma un saskaņā ar šķīti izstrādātiem valsts tiesību aktu noteikumiem, kas minēti 5. punktā. Tomēr pienācīgi pamatotā steidzamā gadījumā šādas sistēmas lietošanu var sākt bez atļaujas ar noteikumu, ka šādu atļauju pieprasa bez liekas kavēšanās ne vēlāk kā 24 stundu laikā. Ja šāda atļauja netiek piešķirta, lietošanu nekavējoties pārtrauc un visus datus, kā arī tādas lietošanas rezultātus un iznākumus nekavējoties atmet un dzēš.

Kompetentā tiesu iestāde vai neatkarīga administratīvā iestāde, kuras lēmums ir saistošs, piešķir atļauju tikai tad, ja, pamatojoties uz tai iesniegtiem objektīviem pierādījumiem vai skaidrām norādēm, tā atzīst, ka attiecīgās reāllaika biometriskās tālidentifikācijas sistēmas lietošana ir nepieciešama un samērīga, lai sasniegtu vienu no 1. punkta pirmās daļas h) apakšpunktā noteiktajiem mērķiem, kas norādīts pieprasījumā, un jo īpaši tā notiek tikai tiklīdz, cik tas absolūti

nepieciešams laikposma, kā arī ģeogrāfiskā un personiskā tvēruma ziņā. Lemjot par pieprasījumu, minētā iestāde ņem vērā 2. punktā minētos elementus. Nevienu lēmumu, kas personai rada nelabvēlīgas tiesiskas sekas, nevar pieņemt, balstoties vienīgi uz reāllaika biometriskās tālidentifikācijas sistēmu sniegto iznākumu.

4. Neskarot 3. punktu, par katru reāllaika biometriskās tālidentifikācijas sistēmas lietošanu publiski pieklūstamās vietās tiesībaizsardzības nolūkos paziņo attiecīgajai tirgus uzraudzības iestādei un valsts datu aizsardzības iestādei saskaņā ar 5. punktā minētajiem tiesību aktu noteikumiem. Paziņojumā iekļauj vismaz 6. punktā norādīto informāciju, un tajā neiekļauj sensitīvus operatīvos datus.

5. Dalībvalsts var nolemt paredzēt iespēju pilnīgi vai daļēji atļaut reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu publiski pieklūstamās vietās tiesībaizsardzības nolūkos, ievērojot ierobežojumus un nosacījumus, kas uzskaitīti 1. punkta pirmās daļas h) apakšpunktā un 2. un 3. punktā. Attiecīgās dalībvalstis savos tiesību aktos nosaka vajadzīgos sīki izstrādātos noteikumus par 3. punktā minēto atļauju pieprasīšanu, izsniegšanu un izmantošanu, kā arī ar tām saistīto attiecīgo uzraudzību un ziņošanu. Minētajos noteikumos arī norāda, attiecībā uz kuriem no 1. punkta pirmās daļas h) apakšpunktā uzskaitītajiem mērķiem – tostarp kuru minētā punkta h) apakšpunkta iii) punktā norādīto noziedzīgo nodarījumu gadījumā – kompetentajām iestādēm var atļaut minētās sistēmas lietot tiesībaizsardzības nolūkos. Dalībvalstis minētos noteikumus paziņo Komisijai ne vēlāk kā 30 dienas pēc to pieņemšanas. Dalībvalstis saskaņā ar Savienības tiesību aktiem var ieviest ierobežojošākus tiesību aktus par biometriskās tālidentifikācijas sistēmu lietošanu.

6. Dalībvalstu valsts tirgus uzraudzības iestādes un valsts datu aizsardzības iestādes, kurām ir paziņots par reāllaika biometriskās tālidentifikācijas sistēmas lietošanu publiski pieklūstamās vietās tiesībaizsardzības nolūkos, ievērojot 4. punktu, iesniedz Komisijai gada ziņojumus par šādu lietošanu. Minētajā nolūkā Komisija nodrošina dalībvalstīm un valsts tirgus uzraudzības un datu aizsardzības iestādēm veidni, kurā ietver informāciju par to lēmumu skaitu, kurus attiecībā uz atļaujas pieprasījumiem saskaņā ar 3. punktu pieņēmušas kompetentās tiesu iestādes vai neatkarīga administratīvā iestāde, kuras lēmumi ir saistoši, un par to rezultātiem.

7. Komisija publicē gada ziņojumus par reāllaika biometriskās tālidentifikācijas sistēmas lietošanu publiski pieklūstamās vietās tiesībaizsardzības nolūkos, pamatojoties uz dalībvalstīs agregētiem datiem, kas balstīti uz 6. punktā minētajiem gada ziņojumiem. Minētie gada ziņojumi neietver sensitīvus operatīvos datus par saistītajām tiesībaizsardzības darbībām.

8. Šis pants neietekmē aizliegumus, ko piemēro, ja MI prakse pārkāpj citus Savienības tiesību aktus.

III NODAĻA

AUGSTA RISKĀ MI SISTĒMAS

1. IEDAĻA

MI sistēmu klasificēšana par augsta riska MI sistēmām

6. pants

Noteikumi klasificēšanai par augsta riska MI sistēmām

1. Neatkarīgi no tā, vai MI sistēmu laiž tirgū vai nodod ekspluatācijā neatkarīgi no a) un b) apakšpunktā minētajiem produktiem, minēto MI sistēmu uzskata par augsta riska sistēmu, ja ir izpildīti abi šie nosacījumi:

- a) MI sistēmu paredzēts izmantot kā produkta drošības sastāvdaļu, vai MI sistēma pati par sevi ir produkts, uz kuru attiecas Savienības saskaņošanas tiesību akti, kas uzskaitīti I pielikumā;
- b) produktam, kura drošības sastāvdaļa, ievērojot a) apakšpunktu, ir MI sistēma, vai pašai MI sistēmai kā produktam ir vajadzīgs trešās personas veikts atbilstības novērtējums, lai to varētu laist tirgū vai nodot ekspluatācijā saskaņā ar Savienības saskaņošanas tiesību aktiem, kas uzskaitīti I pielikumā.

2. Papildus 1. punktā minētajām augsta riska MI sistēmām par augsta riska sistēmām uzskata III pielikumā minētās MI sistēmas.

3. Atkāpjoties no 2. punkta, III pielikumā minēto MI sistēmu neuzskata par augsta riska sistēmu, ja tā nerada būtisku kaitējuma risku fizisku personu veselībai, drošībai vai pamattiesībām, tostarp būtiski neietekmē lēmumu pieņemšanas iznākumu.

Pirmo daļu piemēro, ja ir izpildīts jebkurš no šādiem nosacījumiem:

- a) MI sistēma ir paredzēta šaura procedūras uzdevuma veikšanai;
- b) MI sistēma ir paredzēta iepriekš pabeigtas cilvēka darbības rezultāta uzlabošanai;
- c) MI sistēma ir paredzēta lēmumu pieņemšanas modeļu vai noviržu no iepriekšējiem lēmumu pieņemšanas modeļiem atklāšanai, un tā nav paredzēta, lai aizstātu vai ietekmētu iepriekš pabeigtu cilvēka veiktu novērtējumu, bez pienācīgas cilvēka veikta pārskatīšanas; vai
- d) MI sistēma ir paredzēta sagatavošanās uzdevuma veikšanai saistībā ar novērtējumu, kas ir būtisks III pielikumā uzskaitīto lietošanas gadījumu nolūkos.

Neatkarīgi no pirmās daļas III pielikumā minētu MI sistēmu vienmēr uzskata par augsta riska MI sistēmu, ja MI sistēma veic fizisku personu profilēšanu.

4. Nodrošinātājs, kas uzskata, ka III pielikumā minēta MI sistēma nav augsta riska sistēma, dokumentē tās novērtējumu pirms minētā sistēma tiek laista tirgū vai nodota ekspluatācijā. Uz šādu nodrošinātāju attiecas 49. panta 2. punktā paredzētais reģistrācijas pienākums. Pēc valsts kompetento iestāžu pieprasījuma nodrošinātājs uzrāda novērtējuma dokumentāciju.

5. Komisija pēc apspriešanās ar Eiropas Mākslīgā intelekta padomi (MI padomi) un ne vēlāk kā 2026. gada 2. februārī sniedz pamatnostādnes, kurās precizē šā panta praktisko īstenošanu saskaņā ar 96. pantu, kopā ar izsmelšu sarakstu ar praktiskiem piemēriem par MI sistēmu, kuras ir augsta riska MI sistēmas, un to, kuras nav augsta riska MI sistēmas, lietošanas gadījumiem.

6. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu šā panta 3. punkta otro daļu, lai pievienotu jaunus nosacījumus tajā noteiktajiem nosacījumiem, vai grozītu tos, ja ir konkrēti un ticami pierādījumi, ka ir MI sistēmas, kas ietilpst III pielikuma tvērumā, bet nerada būtisku kaitējuma risku fizisku personu veselībai, drošībai vai pamattiesībām.

7. Komisija pieņem deleģētos aktus saskaņā ar 97. pantu, lai grozītu 3. punkta otro daļu, lai svītrotu jebkuru no tajā noteiktajiem nosacījumiem, ja ir konkrēti un ticami pierādījumi, ka tas ir vajadzīgs, lai uzturētu veselības, drošības un pamattiesību aizsardzības līmeni, ko paredz šī regula.

8. Nevienš 3. punkta otrajā daļā paredzētais nosacījumu grozījums, kas pieņemts saskaņā ar šā panta 6. un 7. punktu, nemazina veselības, drošības un pamattiesību aizsardzības vispārējo līmeni, ko paredz šī regula un tas nodrošina saskanību ar deleģētajiem aktiem, kas pieņemti, ievērojot 7. panta 1. punktu, un ņem vērā tirgus norises un tehnoloģiju attīstību.

7. pants

Grozījumi III pielikumā

1. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu III pielikumu, pievienojot vai mainot augsta riska MI sistēmu lietošanas gadījumus, ja ir izpildīti abi šie nosacījumi:

- a) MI sistēmas ir paredzētas lietošanai jebkurā no III pielikumā uzskaitītajām jomām;
- b) MI sistēmas rada kaitējuma risku veselībai un drošībai vai nelabvēlīgu ietekmi uz pamattiesībām, un minētais risks ir līdzvērtīgs ar vai lielāks par kaitējuma vai nelabvēlīgas ietekmes risku, ko rada augsta riska MI sistēmas, kuras jau minētas III pielikumā.

2. Novērtējot 1. punkta b) apakšpunktā paredzēto nosacījumu, Komisija ņem vērā šādus kritērijus:
- a) MI sistēmas paredzētais nolūks;
 - b) kādā mērā MI sistēma ir lietota vai ir domājams, ka tiks lietota;
 - c) MI sistēmas apstrādāto un izmantoto datu raksturs un apjoms, jo īpaši tas, vai tiek apstrādāti īpašu kategoriju personas dati;
 - d) kādā mērā MI sistēma darbojas autonomi, un kāda ir iespēja cilvēkam neņemt vērā lēmumu vai ieteikumus, kuri var radīt potenciālu kaitējumu;
 - e) kādā mērā MI sistēmas lietošana jau ir nodarījusi kaitējumu veselībai un drošībai, tai ir bijusi nelabvēlīga ietekme uz pamattiesībām, vai tā ir raisījusi nopietnas bažas par šāda kaitējuma vai nelabvēlīgas ietekmes iespējamību, kā liecina, piemēram, ziņojumi vai dokumentēti apgalvojumi, kas iesniegti valsts kompetentajām iestādēm, vai, attiecīgā gadījumā, citi ziņojumi;
 - f) šāda kaitējuma vai šādas nelabvēlīgas ietekmes iespējamais apmērs, jo īpaši attiecībā uz to intensitāti un spēju skart daudzus cilvēkus vai nesamērīgi ietekmēt kādu konkrētu personu grupu;
 - g) kādā mērā personas, kam potenciāli ir nodarīts kaitējums vai kuras cieš no nelabvēlīgas ietekmes, ir atkarīgas no MI sistēmas radītā iznākuma, jo īpaši tāpēc, ka praktisku vai juridisku iemeslu dēļ nav saprātīgi iespējams atteikties no tāda iznākuma;
 - h) kādā mērā spēku samērs nav līdzvērtīgs vai personas, kam potenciāli ir nodarīts kaitējums vai kuras cieš no nelabvēlīgas ietekmes, ir neaizsargātā stāvoklī attiecībā pret MI sistēmas uzturētāju, jo īpaši statusa, pilnvaru, zināšanu, ekonomisko vai sociālo apstākļu vai vecuma dēļ;
 - i) kādā mērā iznākums, kas radīts, iesaistot MI sistēmu, ir viegli izlabojams vai reversējams, ņemot vērā tehniskos risinājumus, kas pieejami labošanai vai reversēšanai; iznākumus, kam ir nelabvēlīga ietekme uz veselību, drošību vai pamattiesībām, neuzskata par viegli izlabojamiem vai reversējamiem;
 - j) vai un kādā mērā MI sistēmas ieviešana dotu ieguvumu indivīdiem, grupām vai sabiedrībai kopumā, ieskaitot iespējamus produktu drošības uzlabojumus;
 - k) kādā mērā spēkā esošie Savienības tiesību akti nosaka:
 - i) efektīvus tiesību aizsardzības pasākumus saistībā ar MI sistēmas radītajiem riskiem, izņemot prasības par kaitējuma atlīdzināšanu;
 - ii) efektīvus pasākumus minēto risku novēršanai vai būtiskai samazināšanai.
3. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu III pielikumā ietverto sarakstu, svītrojot augsta riska MI sistēmas, ja ir izpildīti abi šie nosacījumi:
- a) attiecīgā augsta riska MI sistēma vairs nerada būtiskus riskus pamattiesībām, veselībai vai drošībai, ņemot vērā 2. punktā uzskaitītos kritērijus;
 - b) svītrosana nesamazina vispārējo veselības, drošības un pamattiesību aizsardzības līmeni, kas paredzēts Savienības tiesību aktos.

2. IEDAĻA

Prasības augsta riska MI sistēmām

8. pants

Atbilstība prasībām

1. Augsta riska MI sistēmas atbilst šajā iedaļā noteiktajām prasībām, ņemot vērā tām paredzētos nolūkus, kā arī vispāratzītos jaunākos sasniegumus MI un ar MI saistīto tehnoloģiju jomā. Nodrošinot atbilstību minētajām prasībām, ņem vērā 9. pantā minēto riska pārvaldības sistēmu.

2. Ja produkts satur MI sistēmu, kurai piemēro šīs regulas prasības, kā arī I pielikuma A iedaļā uzskaitīto Savienības saskaņošanas tiesību aktu prasības, nodrošinātāji ir atbildīgi par to, lai tiktu nodrošināts, ka to produkts pilnībā atbilst visām piemērojamajām prasībām saskaņā ar piemērojamajiem Savienības saskaņošanas tiesību aktiem. Nodrošinot 1. punktā minēto augsta riska MI sistēmu atbilstību šajā iedaļā noteiktajām prasībām un lai nodrošinātu konsekvenci, nepieļautu dublēšanos un samazinātu papildu slogu, nodrošinātājiem ir izvēles iespēja attiecīgā gadījumā integrēt nepieciešamos testēšanas un ziņošanas procesus, informāciju un dokumentāciju, ko tie sniedz attiecībā uz savu produktu, dokumentācijā un procedūrās, kas jau pastāv un ir prasītas I pielikuma A iedaļā uzskaitītajos Savienības saskaņošanas tiesību aktos.

9. pants

Riska pārvaldības sistēma

1. Saistībā ar augsta riska MI sistēmām izveido, ievieš, dokumentē un uztur riska pārvaldības sistēmu.
2. Riska pārvaldības sistēmu saprot kā nepārtrauktu iteratīvu procesu, ko plāno un kas norit visā augsta riska MI sistēmas darbībā, un tam nepieciešama regulāra sistemātiska pārskatīšana un atjaunināšana. Tajā ietilpst šādi posmi:
 - a) to zināmo un saprātīgi paredzamo risku apzināšana un analīze, ko augsta riska MI sistēma var radīt veselībai, drošībai vai pamattiesībām, ja augsta riska MI sistēmu lieto saskaņā ar tai paredzēto nolūku;
 - b) to risku aplēšana un izvērtēšana, kas var rasties, ja augsta riska MI sistēmu lieto atbilstoši paredzētajam nolūkam, un saprātīgi paredzamas nepareizas lietošanas apstākļos;
 - c) citu iespējamo risku izvērtēšana, pamatojoties uz to datu analīzi, kas savākti no 72. pantā minētās pēctirgus pārraudzības sistēmas;
 - d) saskaņā ar šā punkta a) apakšpunktu apzinātu risku novēršanai paredzētu piemērotu un mērķorientētu riska pārvaldības pasākumu pieņemšana.
3. Šajā pantā minētie riski attiecas tikai uz tiem riskiem, kurus var saprātīgi mazināt vai novērst, izstrādājot vai projektējot augsta riska MI sistēmu vai sniedzot atbilstīgu tehnisko informāciju.
4. Riska pārvaldības pasākumos, kas minēti 2. punkta d) apakšpunktā, pienācīgi ņem vērā sekas un iespējamo mijiedarbību, ko rada šajā iedaļā noteikto prasību kombinēta piemērošana, lai efektīvāk samazinātu riskus, vienlaikus panākot pienācīgu līdzsvaru minēto prasību izpildei paredzēto pasākumu īstenošanā.
5. Riska pārvaldības pasākumi, kas minēti 2. punkta d) apakšpunktā, ir tādi, ka attiecīgie ar katru apdraudējumu saistītie atlikušie riski, kā arī augsta riska MI sistēmu kopējais atlikušais risks tiek uzskatīti par pieņemamiem.

Nosakot vispiemērotākos riska pārvaldības pasākumus, nodrošina:

- a) apzināto un izvērtēto risku likvidēšanu vai samazināšanu, ievērojot 2. punktu, ciktāl tas tehniski iespējams, ar augsta riska MI sistēmas atbilstīgu projektēšanu un izstrādi;
- b) attiecīgā gadījumā atbilstīgu riska mazināšanas un kontroles pasākumu īstenošanu, ar ko pievēršas riskiem, kurus nevar likvidēt;
- c) informācijas sniegšanu, kas prasīta, ievērojot 13. pantu, un attiecīgā gadījumā uzturētāju apmācību.

Lai likvidētu vai samazinātu riskus, kas saistīti ar augsta riska MI sistēmas lietošanu, pienācīgi ņem vērā tehniskās zināšanas, pieredzi, izglītību, apmācību, kas tiek gaidīta attiecībā uz uzturētāju, un paredzamo kontekstu, kurā sistēmu paredzēts izmantot.

6. Augsta riska MI sistēmas testē, lai noteiktu vispiemērotākos un mērķtiecīgākos riska pārvaldības pasākumus. Testēšana nodrošina, ka augsta riska MI sistēmas darbojas konsekventi paredzētajam nolūkam un ka tās atbilst šajā iedaļā noteiktajām prasībām.
7. Testēšanas procedūras var ietvert testēšanu reālos apstākļos saskaņā ar 60. pantu.
8. Augsta riska MI 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 MI sistēmai paredzētajam nolūkam.
9. Īstenojot 1.–7. punktā paredzēto riska pārvaldības sistēmu, nodrošinātāji apsver, vai, ņemot vērā tai paredzēto nolūku, pastāv iespēja, ka augsta riska MI sistēmai būs negatīva ietekme uz personām, kas jaunākas par 18 gadiem, un attiecīgā gadījumā citām neaizsargātām grupām.
10. Attiecībā uz augsta riska MI sistēmu nodrošinātājiem, uz kuriem saskaņā ar citiem attiecīgiem Savienības tiesību aktu noteikumiem attiecas prasības par iekšējiem riska pārvaldības procesiem, 1.–9. punktā paredzētie aspekti var būt daļa no vai apvienoti ar riska pārvaldības procedūrām, kas izveidotas, ievērojot minētos tiesību aktus.

10. pants

Dati un datu pārvaldība

1. Augsta riska MI sistēmas, kurās izmanto metodes, kas saistītas ar MI modeļu apmācību ar datiem, izstrādā, pamatojoties uz apmācības, validēšanas un testēšanas datu kopām, kas atbilst 2.–5. punktā minētajiem kvalitātes kritērijiem, ikreiz, kad tiek izmantotas šādas datu kopas.
2. Apmācības, validēšanas un testēšanas datu kopām piemēro datu pārvaldību un pārvaldības praksi, kas ir piemērota augsta riska MI sistēmai paredzētajam nolūkam. Minētā prakse attiecas jo īpaši uz:
 - a) attiecīgām izstrādes izvēlēm;
 - b) datu vākšanas procesiem un datu izcelsmi, un personas datu gadījumā – uz datu vākšanas sākotnējo nolūku;
 - c) attiecīgām datu sagatavošanas apstrādes darbībām, piemēram, anotēšanu, marķēšanu, tīrīšanu, atjaunināšanu, bagātināšanu un agregēšanu;
 - d) pieņēmumu formulēšanu, jo īpaši attiecībā uz informāciju, kuru šiem datiem vajadzētu izmērīt un attēlot;
 - e) nepieciešamo datu kopu pieejamības, daudzuma un piemērotības novērtējumu;
 - f) tādas iespējamās neobjektivitātes pārbaudi, kas varētu ietekmēt cilvēku veselību un drošību, nelabvēlīgi ietekmēt pamattiesības vai izraisīt diskrimināciju, kura aizliegta ar Savienības tiesību aktiem, jo īpaši, ja izvaddati ietekmē ievaddatus turpmākām darbībām;
 - g) pienācīgus pasākumus, lai atklātu, novērstu, mazinātu iespējamu neobjektivitāti, kas identificēta saskaņā ar f) apakšpunktu;
 - h) tādu attiecīgu datu trūkumu vai nepilnību identificēšanu, kas liedz ievērot šo regulu, un to, kā šos trūkumus un nepilnības var novērst.
3. Apmācības, validēšanas un testēšanas datu kopas ir atbilstošas, pietiekami reprezentatīvas un, cik vien iespējams, bez kļūdām un pilnīgas, ņemot vērā paredzēto nolūku. Tām ir atbilstoši statistiskie raksturlielumi, tostarp vajadzības gadījumā attiecībā uz personām vai personu grupām, attiecībā uz kurām paredzēts izmantot konkrēto augsta riska MI sistēmu. Minētos datu kopu raksturlielumus var izpildīt atsevišķu datu kopu vai to kombinācijas līmenī.
4. Datu kopās, ciktāl to nosaka paredzētais nolūks, ņem vērā raksturlielumus vai elementus, kas raksturīgi konkrētajai ģeogrāfiskajai, kontekstuālajai, uzvedības vai funkcionālajai videi, kurā paredzēts lietot augsta riska MI sistēmu.

5. Ciktāl tas ir absolūti nepieciešams, lai nodrošinātu neobjektivitātes atklāšanu un labošanu saistībā ar augsta riska MI sistēmām saskaņā ar šā panta 2. punkta f) un g) apakšpunktu, šādu sistēmu nodrošinātāji var izņēmuma kārtā apstrādāt īpašu kategoriju personas datus, ievērojot atbilstošus fizisku personu pamattiesību un pamatbrīvību aizsardzības pasākumus. Lai notiktu šāda apstrāde, papildus noteikumiem, kas paredzēti Regulās (ES) 2016/679 un (ES) 2018/1725 un Direktīvā (ES) 2016/680, jāievēro visi turpmāk minētie nosacījumi:

- a) neobjektivitātes atklāšanu un labošanu nevar rezultatīvi panākt, apstrādājot citus datus, tostarp sintētiskus vai anonimizētus datus;
- b) uz īpašajām personas datu kategorijām attiecas tehniski ierobežojumi saistībā ar personas datu atkalizmantošanu un jaunākie drošības un privātuma saglabāšanas pasākumi, tostarp pseidonimizācija;
- c) uz īpašajām personas datu kategorijām attiecas pasākumi nolūkā nodrošināt, ka apstrādātie personas dati ir droši, aizsargāti, uz tiem attiecas piemēroti aizsardzības pasākumi, tostarp stingra piekļuves kontrole un dokumentācija, lai novērstu ļaunprātīgu izmantošanu, un nodrošinātu, ka piekļuve minētajiem personas datiem ir tikai pilnvarotām personām un ar atbilstīgiem konfidencialitātes pienākumiem;
- d) īpašajās kategorijās ietilpstošos personas datus nepārsūta, nenodod vai citādi nedara piekļūstamus citām pusēm;
- e) īpašajās kategorijās ietilpstošos personas datus dzēš, tiklīdz neobjektivitāte ir izlabota vai ir pienākušas to glabāšanas perioda beigas – atkarībā no tā, kas notiek vispirms;
- f) ieraksti par apstrādes darbībām, ievērojot Regulām (ES) 2016/679 un (ES) 2018/1725 un Direktīvu (ES) 2016/680, ietver pamatojumu, kāpēc īpašo kategoriju personas datu apstrāde bija absolūti nepieciešama, lai atklātu un izlabotu neobjektivitāti, un kāpēc šo mērķi nevarēja sasniegt, apstrādājot citus datus.

6. Attiecībā uz tādu augsta riska MI sistēmu izstrādi, kurās netiek izmantotas metodes, kas paredz MI modeļu apmācību, 2.–5. punktu piemēro tikai testēšanas datu kopām.

11. pants

Tehniskā dokumentācija

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

Tehnisko dokumentāciju sagatavo tā, lai apliecinātu, ka attiecīgā augsta riska MI sistēma atbilst šajā iedaļā noteiktajām prasībām, un valstu kompetentajām iestādēm un paziņotajām struktūrām skaidrā un visaptverošā veidā sniedz nepieciešamo informāciju, lai novērtētu MI sistēmas atbilstību minētajām prasībām. Tajā ir vismaz IV pielikumā izklāstītie elementi. MVU, tostarp jaunuzņēmumi, IV pielikumā norādītos tehniskās dokumentācijas elementus var iesniegt vienkāršotā veidā. Minētajā nolūkā Komisija izveido vienkāršotu tehniskās dokumentācijas veidlapu, ņemot vērā mazo uzņēmumu un mikrouzņēmumu vajadzības. Ja MVU, tostarp jaunuzņēmums, izvēlas IV pielikumā prasīto informāciju sniegt vienkāršotā veidā, tas izmanto šajā punktā minēto veidlapu. Paziņotās struktūras pieņem veidlapu atbilstības novērtēšanas nolūkos.

2. Ja tiek laista tirgū vai nodota ekspluatācijā augsta riska MI sistēma, kas saistīta ar produktu, uz kuru attiecas I pielikuma A iedaļā uzskaitītie Savienības saskaņošanas tiesību akti, sagatavo vienotu tehniskās dokumentācijas kopumu, kurā ir visa informācija, kas noteikta 1. punktā, kā arī informācija, kas prasīta minētajos tiesību aktos.

3. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. 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 iedaļā noteiktajām prasībām.

12. pants

Uzskaitē

1. Augsta riska MI sistēmas tehniski ļauj automātiski reģistrēt notikumus (žurnāldatnes) visā sistēmas darbības laikā.
2. Lai nodrošinātu tādu augsta riska MI sistēmas darbības izsekojamības līmeni, kas atbilst sistēmai paredzētajam nolūkam, reģistrēšanas spējas dod iespēju reģistrēt notikumus, kas attiecas uz:
 - a) tādu situāciju identificēšanu, kurās augsta riska MI sistēma var radīt risku 79. panta 1. punkta nozīmē vai kurās var notikt būtiska modifikācija;
 - b) 72. pantā minētās pēctirgus pārraudzības atvieglošanu; un
 - c) augsta riska MI sistēmu darbības pārraudzību, kas minēta 26. panta 5. punktā.
3. Augsta riska MI sistēmām, kas minētas III pielikuma 1. punkta a) apakšpunktā, reģistrēšanas spējas nodrošina vismaz:
 - a) katras sistēmas lietošanas perioda (katras lietošanas sākuma datums un laiks un beigu datums un laiks) reģistrāciju;
 - b) informāciju par atsaucē 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 uzturētājiem

1. Augsta riska MI sistēmas projektē un izstrādā tā, lai nodrošinātu, ka to darbība ir pietiekami pārredzama, lai uzturētāji varētu interpretēt sistēmas iznākumus un tos pienācīgi izmantot. Nodrošina atbilstošu pārredzamības veidu un pakāpi, lai panāktu atbilstību attiecīgajiem nodrošinātāja un uzturētāja pienākumiem, kas noteikti 3. iedaļā.
2. Augsta riska MI sistēmām pievieno lietošanas instrukciju piemērotā digitālā formātā vai citādi, un tajā ietver kodolīgu, pilnīgu, pareizu un skaidru informāciju, kas ir būtiska, pieejama un saprotama uzturētājiem.
3. Lietošanas instrukcijā iekļauj vismaz šādu informāciju:
 - a) nodrošinātāja un attiecīgā gadījumā tā pilnvarotā pārstāvja identitāte un kontaktinformācija;
 - b) augsta riska MI sistēmas raksturlielumi, spējas un tās veikspējas ierobežojumi, tostarp:
 - i) tai paredzētais nolūks;
 - ii) 15. pantā minētais precizitātes, ietverot tās rādītājus, robustuma un kiberdrošības līmenis, par kuru ir testēta un validēta attiecīgā augsta riska MI sistēma un kuru var gaidīt, un visi zināmie un paredzamie apstākļi, kas var ietekmēt sagaidāmo precizitātes, robustuma un kiberdrošības līmeni;
 - iii) zināmie vai paredzamie apstākļi, kas saistīti ar augsta riska MI sistēmas lietošanu atbilstoši tai paredzētajam nolūkam vai saprātīgi paredzamas nepareizas lietošanas apstākļos un kas var radīt riskus veselībai un drošībai vai pamattiesībām, kuri minēti 9. panta 2. punktā;
 - iv) attiecīgā gadījumā – augsta riska MI sistēmas tehniskās spējas un raksturlielumi, lai sniegtu informāciju, kas ir būtiska, lai izskaidrotu tās iznākumu;

- v) attiecīgā gadījumā – tās veikspēja saistībā ar konkrētām personām vai personu grupām, attiecībā uz kurām sistēmu paredzēts izmantot;
 - vi) attiecīgā gadījumā – ievaddatu specifikācijas vai cita būtiska informācija attiecībā uz izmantotajām apmācības, validēšanas un testēšanas datu kopām, ņemot vērā augsta riska MI sistēmai paredzēto nolūku;
 - vii) attiecīgā gadījumā – informācija, kas ļauj uzturētājiem interpretēt augsta riska MI sistēmas iznākumus un tos pienācīgi izmantot;
- c) izmaiņas augsta riska MI sistēmā un tās veikspējā, kuras sākotnējās atbilstības novērtēšanas brīdī ir noteicis nodrošinātājs, ja tādas ir;
- d) cilvēka virsvadības pasākumi, kas minēti 14. pantā, tostarp tehniskie pasākumi, kuri ieviesti, lai palīdzētu uzturētājiem interpretēt augsta riska MI sistēmu iznākumus;
- e) nepieciešamie skaitļošanas un aparatūras resursi, paredzamais augsta riska MI sistēmas darbmūžs un visi uzturēšanas un apkopes pasākumi, tostarp to biežums, kas nepieciešami, lai nodrošinātu šīs MI sistēmas pareizu darbību, arī saistībā ar programmatūras atjauninājumiem;
- f) ja tas ir attiecīgi – augsta riska MI sistēmā iekļauto mehānismu apraksts, kas uzturētājiem dod iespēju pienācīgi vākt, glabāt un interpretēt žurnāldatnes saskaņā ar 12. pantu.

14. pants

Cilvēka virsvadība

1. Augsta riska MI sistēmas projektē un izstrādā, izmantojot arī atbilstošus cilvēka – mašīnas saskarnes rīkus, tā, lai fiziskas personas tās varētu efektīvi virsvadīt laikā, kad tās tiek lietotas.
2. Cilvēka virsvadības mērķis ir novērst vai mazināt riskus attiecībā uz veselību, drošību vai pamattiesībām, kuri var rasties, ja augsta riska MI sistēmu lieto atbilstoši paredzētajam nolūkam vai saprātīgi paredzamas nepareizas lietošanas apstākļos, jo īpaši, ja šādi riski arvien pastāv, neraugoties uz citu šajā iedaļā noteikto prasību piemērošanu.
3. Virsvadības pasākumi ir samērīgi augsta riska MI sistēmas riskiem, autonomijas līmenim un lietošanas kontekstam, un tos nodrošina, izmantojot vienu vai abus šos pasākumu veidus:
 - a) pasākumi, kurus nodrošinātājs identificē un integrē augsta riska MI sistēmā, ja tas ir tehniski iespējams, pirms tās laišanas tirgū vai nodošanas ekspluatācijā;
 - b) pasākumi, kurus nodrošinātājs identificē pirms augsta riska MI sistēmas laišanas tirgū vai nodošanas ekspluatācijā un kuri ir atbilstīgi, lai uzturētājs tos īstenotu.
4. Šā panta 1., 2. un 3. punkta īstenošanas nolūkā augsta riska MI sistēmu uzturētājam nodrošina tā, lai fiziskās personas, kurām ir uzticēta cilvēka virsvadība, atbilstoši un samērīgi varētu:
 - a) pareizi izprast augsta riska MI sistēmas attiecīgās spējas un ierobežojumus un spēt pienācīgi uzraudzīt tās darbību, tostarp, lai atklātu un novērstu anomālijas, disfunkcijas un neparedzētu veikspēju;
 - b) apzināties iespējamo tendenci automātiski uzticēties vai pārāk uzticēties augsta riska MI sistēmas radītajiem iznākumiem (automatizācijas izraisīta nosliece), jo īpaši attiecībā uz augsta riska MI sistēmām, kuras lieto, lai sniegtu informāciju vai ieteikumus lēmumiem, kas jāpieņem fiziskām personām;
 - c) pareizi interpretēt augsta riska MI sistēmas radīto iznākumu, ņemot vērā, piemēram, pieejamos interpretācijas rīkus un metodes;

- d) katrā atsevišķā situācijā izlemt nelietot augsta riska MI sistēmu vai citādi neņemt vērā, aizstāt ar citu vai reversēt augsta riska MI sistēmas darbības iznākumu;
- e) iejaukties augsta riska MI sistēmas darbībā vai pārtraukt sistēmu, izmantojot pogu “stop” vai līdzīgu procedūru, kas ļauj sistēmai apstāties drošā stāvoklī.

5. Attiecībā uz augsta riska MI sistēmām, kas minētas III pielikuma 1. punkta a) apakšpunktā, šā panta 3. punktā minētie pasākumi ir tādi, kas nodrošina, ka uzturētājs papildus neveic nekādas darbības vai nepieņem nekādu lēmumu, pamatojoties uz identifikāciju, kas izriet no attiecīgās sistēmas, ja tādu identifikāciju nav atsevišķi verificējušas un apstiprinājušas vismaz divas fiziskas personas, kurām ir vajadzīgā kompetence, apmācība un pilnvaras.

Prasību par vismaz divu fizisku personu veiktu atsevišķu verifikāciju nepiemēro augsta riska MI sistēmām, ko izmanto tiesībsardzības, migrācijas, robežkontroles vai patvēruma nolūkos, ja Savienības vai valsts tiesību aktos šīs prasības piemērošana tiek uzskatīta par nesamērīgu.

15. pants

Precizitāte, robustums un kiberdrošība

1. Augsta riska MI sistēmas projektē un izstrādā tā, lai tās sasniegtu pienācīgu precizitātes, robustuma un kiberdrošības līmeni un lai tās minētajos aspektos konsekventi darbotos visu darbību laikā.
2. Lai pievērstos tehniskajiem aspektiem saistībā ar to, kā izmērīt 1. punktā noteiktos attiecīgos precizitātes un robustuma līmeņus un jebkādos citus attiecīgus veiktspējas rādītājus, Komisija sadarbībā ar attiecīgajām ieinteresētajām personām un organizācijām, piemēram, metroloģijas un salīdzinošās novērtēšanas iestādēm, attiecīgā gadījumā veicina etalonrādītāju un mērījumu metodiku izstrādi.
3. Augsta riska MI sistēmu precizitātes līmeni un attiecīgos precizitātes rādītājus norāda tām pievienotajā lietošanas instrukcijā.
4. Augsta riska MI sistēmas ir cik iespējams noturīgas pret kļūdām, defektiem vai neatbilstībām, kas var rasties pašā sistēmā vai vidē, kurā attiecīgā sistēma darbojas, jo īpaši sistēmas mijiedarbības ar fiziskām personām vai citām sistēmām dēļ. Šajā sakarā veic tehniskus un organizatoriskus pasākumus.

Augsta riska MI sistēmu robustumu var panākt ar tehniskiem redundances risinājumiem, kuru vidū var būt rezerves vai drošatteices plāni.

Augsta riska MI sistēmas, kas turpina mācīties pēc to laišanas tirgū vai nodošanas ekspluatācijā, izstrādā tā, lai, cik vien iespējams, likvidētu vai samazinātu iespējamu neobjektīvu iznākumu risku, kas ietekmē ievaddatus nākamās operācijās (atgriezeniskās saites cilpas), un lai nodrošinātu, ka visām šādām atgriezeniskās saites cilpām pienācīgi pievēršas ar atbilstošiem mazināšanas pasākumiem.

5. Augsta riska MI sistēmas ir noturīgas pret nepilnvarotu trešo personu mēģinājumiem mainīt to lietojumu, iznākumus vai veiktspēju, izmantojot sistēmas ietekmējamību.

Tehniskie risinājumi, kuru mērķis ir nodrošināt augsta riska MI sistēmu kiberdrošību, atbilst attiecīgajiem apstākļiem un riskiem.

Tehniskie risinājumi, kas paredzēti, lai novērstu MI konkrēto ietekmējamību, attiecīgā gadījumā ietver pasākumus, kuru mērķis ir novērst, atklāt, reaģēt uz, atrisināt un kontrolēt uzbrukumus, kuros tiek mēģināts manipulēt ar apmācības datu kopu (datu saindēšana) vai apmācībā izmantotām iepriekš apmācītām sastāvdaļām (modeļa saindēšana), ievaddatiem, kas paredzēti modeļa kļūdas izraisīšanai (pretiniecišķi piemēri vai modeļa maldināšana), uzbrukumiem konfidencialitātei vai modeļa nepilnībām.

3. IEDAĻA

Augsta riska MI sistēmu nodrošinātāju un uzturētāju un citu pušu pienākumi

16. pants

Augsta riska MI sistēmu nodrošinātāju pienākumi

Augsta riska MI sistēmu nodrošinātāji:

- a) nodrošina, ka to augsta riska MI sistēmas atbilst 2. iedaļā noteiktajām prasībām;
- b) uz augsta riska MI sistēmas vai, ja tas nav iespējams, attiecīgi uz tās iepakojuma vai tai pievienotajā dokumentācijā norāda savu nosaukumu/vārdu, reģistrēto tirdzniecības nosaukumu vai reģistrēto preču zīmi un adresi, kādā ar tiem var sazināties;
- c) ievieš kvalitātes vadības sistēmu, kas atbilst 17. pantam;
- d) glabā 18. pantā minēto dokumentāciju;
- e) glabā 19. pantā minētās žurnāldatnes, kuras automātiski ģenerējušas to augsta riska MI sistēmas, ja žurnāldatnes ir viņu pārziņā;
- f) nodrošina, ka attiecībā uz augsta riska MI sistēmu pirms tās laišanas tirgū vai nodošanas ekspluatācijā tiek veikta attiecīgā atbilstības novērtēšanas procedūra, kā minēts 43. pantā;
- g) sagatavo ES atbilstības deklarāciju saskaņā ar 47. pantu;
- h) saskaņā ar 48. pantu uzliek CE zīmi augsta riska MI sistēmai vai, ja tas nav iespējams, tās iepakojumam vai tai pievienotajai dokumentācijai, lai norādītu atbilstību šai regulai;
- i) pilda 49. panta 1. punktā minētos reģistrēšanas pienākumus;
- j) veic vajadzīgās korektīvās darbības un sniedz informāciju, kā prasīts 20. pantā;
- k) pēc valsts kompetentās iestādes pamatota pieprasījuma apliecina augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām;
- l) nodrošina, ka augsta riska MI sistēma atbilst piekļūstamības prasībām saskaņā ar Direktīvām (ES) 2016/2102 un (ES) 2019/882.

17. pants

Kvalitātes vadības sistēma

1. Augsta riska MI sistēmu nodrošinātāji 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 MI sistēmas modifikāciju pārvaldības procedūru ievērošana;
- b) metodes, procedūras un sistemātiskas darbības, kas jāizmanto augsta riska MI sistēmas projektēšanai, projekta kontrolei un projekta verificēšanai;
- c) metodes, procedūras un sistemātiskas darbības, kas jāizmanto augsta riska MI sistēmas izstrādei, kvalitātes kontrolei un kvalitātes nodrošināšanai;
- d) pārbaudes, testēšanas un validēšanas procedūras, kas jāveic pirms augsta riska MI 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 vai neaptver visas attiecīgās 2. iedaļā paredzētās prasības, līdzekļi, kas jāizmanto, lai nodrošinātu, ka augsta riska MI sistēma atbilst minētajām prasībām;
- f) datu pārvaldības sistēmas un procedūras, ietverot datu iegūšanu, datu vākšanu, datu analīzi, datu marķēšanu, datu glabāšanu, datu filtrēšanu, datizraci, datu agregēšanu, datu saglabāšanu un jebkuru citu darbību ar datiem, kas tiek veikta pirms augsta riska MI sistēmu laišanas tirgū vai nodošanas ekspluatācijā un to nolūkā;
- g) riska pārvaldības sistēma, kas minēta 9. pantā;
- h) pēctirgus pārraudzības sistēmas izveidošana, ieviešana un uzturēšana saskaņā ar 72. pantu;
- i) procedūras, kas saistītas ar ziņošanu par nopietnu incidentu saskaņā ar 73. pantu;
- j) komunikācijas organizēšana ar valstu kompetentajām iestādēm, citām attiecīgām iestādēm, ieskaitot tās, kas dod vai atbalsta piekļuvi datiem, paziņotajām 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 nodrošinātāja organizācijas lielumam. Nodrošinātāji jebkurā gadījumā ievēro tādu stingrības pakāpi un aizsardzības līmeni, kāds ir vajadzīgs, lai nodrošinātu augsta riska MI sistēmu atbilstību šai regulai.

3. Augsta riska MI sistēmu nodrošinātāji, uz kuriem attiecīgajos Savienības nozaru tiesību aktos attiecas pienākumi, kas saistīti ar kvalitātes vadības sistēmām vai līdzvērtīgu funkciju, var ietvert 1. punktā uzskaitītos aspektus kā daļu no kvalitātes vadības sistēmām, ievērojot minētos tiesību aktus.

4. Attiecībā uz nodrošinātājiem, kas ir finanšu iestādes, uz kurām attiecas prasības par to iekšējo pārvaldību, kārtību vai procesiem saskaņā ar Savienības tiesību aktiem finanšu pakalpojumu jomā, tiek uzskatīts, ka pienākums ieviest kvalitātes vadības sistēmu, izņemot šā panta 1. punkta g), h) un i) apakšpunktu, ir izpildīts, ja ir izpildīti noteikumi par iekšējās pārvaldes kārtību vai procesiem, ievērojot attiecīgos Savienības tiesību aktus finanšu pakalpojumu jomā. Minētajā nolūkā ņem vērā jebkurus 40. pantā minētos saskaņotos standartus.

18. pants

Dokumentācijas glabāšana

1. Nodrošinātājs uz laikposmu, kas beidzas 10 gadus pēc augsta riska MI 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 paziņotās struktūras;
- d) attiecīgā gadījumā – paziņoto struktūru izdotos lēmumus un citus dokumentus;
- e) ES atbilstības deklarāciju, kas minēta 47. pantā.

2. Katra dalībvalsts paredz nosacījumus, saskaņā ar kuriem 1. punktā minētā dokumentācija paliek pieejama valsts kompetentajām iestādēm uz minētajā punktā norādīto laikposmu tajos gadījumos, kad nodrošinātājs vai tā pilnvarotais pārstāvis, kas iedibināts tās teritorijā, bankrotē vai pārtrauc savu darbību pirms minētā laikposma beigām.
3. Nodrošinātāji, kas ir finanšu iestādes, uz kurām attiecas prasības par to iekšējo pārvaldību, kārtību vai procesiem saskaņā ar Savienības tiesību aktiem finanšu pakalpojumu jomā, tehnisko dokumentāciju uztur kā daļu no dokumentācijas, kuru glabā saskaņā ar attiecīgajiem Savienības tiesību aktiem finanšu pakalpojumu jomā.

19. pants

Automātiski ģenerētas žurnāldatnes

1. Augsta riska MI sistēmu nodrošinātāji glabā 12. panta 1. punktā minētās žurnāldatnes, ko automātiski ģenerē viņu augsta riska MI sistēmas, ciktāl žurnāldatnes ir viņu pārziņā. Neskarot piemērojamās Savienības vai valsts tiesību aktus, žurnāldatnes glabā laikposmu, kas atbilst augsta riska MI sistēmas paredzētajam nolūkam, vai vismaz sešus mēnešus, ja vien piemērojamajos Savienības vai valsts tiesību aktos, jo īpaši Savienības tiesību aktos par personas datu aizsardzību, nav noteikts citādi.
2. Nodrošinātāji, kas ir finanšu iestādes, uz kurām attiecas prasības par to iekšējo pārvaldību, kārtību vai procesiem saskaņā ar Savienības tiesību aktiem finanšu pakalpojumu jomā, žurnāldatnes, ko automātiski ģenerē to augsta riska MI sistēmas, uztur kā daļu no dokumentācijas, kuru glabā saskaņā ar attiecīgajiem tiesību aktiem finanšu pakalpojumu jomā.

20. pants

Korektīvās darbības un informēšanas pienākums

1. Augsta riska MI sistēmu nodrošinātāji, kas uzskata vai kam ir iemesls uzskatīt, ka augsta riska MI sistēma, kuru tie ir laiduši tirgū vai nodevuši ekspluatācijā, neatbilst šai regulai, nekavējoties veic nepieciešamās korektīvās darbības, kas vajadzīgas, lai panāktu sistēmas atbilstību vai, attiecīgi, to izņemtu, atspējotu vai atsauktu. Par to viņi informē attiecīgās augsta riska MI sistēmas izplatītājus un, attiecīgā gadījumā, uzturētājus, pilnvaroto pārstāvi un importētājus.
2. Ja augsta riska MI sistēma rada risku 79. panta 1. punkta nozīmē un minētais risks kļūst zināms nodrošinātājam, tas nekavējoties izmeklē cēloņus, attiecīgā gadījumā sadarbojoties ar ziņojošo uzturētāju, un informē par attiecīgo augsta riska MI sistēmu kompetentās tirgus uzraudzības iestādes, un, ja vajadzīgs, paziņoto struktūru, kas saskaņā ar 44. pantu izdevusi sertifikātu minētajai augsta riska MI sistēmai, jo īpaši par neatbilstības raksturu un visām attiecīgajām korektīvajām darbībām, kas veiktas.

21. pants

Sadarbība ar kompetentajām iestādēm

1. Augsta riska MI sistēmu nodrošinātāji pēc kompetentas iestādes pamatota pieprasījuma sniedz minētajai iestādei visu informāciju un dokumentāciju, kas vajadzīga, lai apliecinātu augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām, noformējot to iestādei viegli saprotami kādā no Savienības iestāžu oficiālajām valodām, kā norāda attiecīgā dalībvalsts.
2. Pēc kompetentās iestādes pamatota pieprasījuma nodrošinātāji kompetentajai iestādei, kas iesniedz pieprasījumu, attiecīgā gadījumā arī nodrošina piekļuvi 12. panta 1. punktā minētajām žurnāldatnēm, kuras automātiski ģenerē augsta riska MI sistēma, ciktāl šādas žurnāldatnes ir viņu pārziņā.
3. Ar visa informāciju, ko, ievērojot šo pantu, iegūst kompetentā iestāde, rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.

22. pants

Augsta riska MI sistēmu nodrošinātāju pilnvarotie pārstāvji

1. Nodrošinātāji, kas iedibināti trešās valstīs, pirms augsta riska sistēmu dara pieejamu Savienības tirgū, ar rakstisku pilnvaru iecel pilnvaroto pārstāvi, kurš iedibināts Savienībā.
2. Nodrošinātājs ļauj savam pilnvarotajam pārstāvim pildīt uzdevumus, kas norādīti no nodrošinātāja saņemtajā pilnvarojumā.
3. Pilnvarotais pārstāvis veic uzdevumus, kas norādīti no nodrošinātāja saņemtajā pilnvarojumā. Tas pēc pieprasījuma iesniedz tirgus uzraudzības iestādēm pilnvarojuma kopiju kādā no Savienības iestāžu oficiālajām valodām, kā norāda kompetentā iestāde. Šīs regulas nolūkos pilnvarojums pilnvarotajam pārstāvim dod tiesības veikt šādus uzdevumus:
 - a) pārliecināties, ka nodrošinātājs ir sagatavojis 47. pantā minēto ES atbilstības deklarāciju un 11. pantā minēto tehnisko dokumentāciju un ir veicis pienācīgu atbilstības novērtēšanas procedūru;
 - b) 10 gadus pēc augsta riska MI sistēmas laišanas tirgū vai nodošanas ekspluatācijā, glabāt kompetentajām iestādēm un 74. panta 10. punktā minētajām valsts iestādēm vai struktūrām pieejamu tā nodrošinātāja kontaktinformāciju, kurš ir iecēlis pilnvaroto pārstāvi, 47. pantā minētās ES atbilstības deklarācijas kopiju, tehnisko dokumentāciju un, attiecīgā gadījumā, paziņotās struktūras izdoto sertifikātu;
 - c) pēc pamatota pieprasījuma sniegt kompetentajai iestādei visu informāciju un dokumentāciju, tostarp to, kas minēta šīs daļas b) apakšpunktā, kas vajadzīga, lai apliecinātu augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām, tostarp piekļuvi augsta riska MI sistēmas automātiski ģenerētajām žurnāldatnēm, kā minēts 12. panta 1. punktā, ciktāl šādas žurnāldatnes ir nodrošinātāja pārziņā;
 - d) pēc pamatota pieprasījuma sadarboties ar kompetentajām iestādēm visās darbībās, ko tās veic saistībā ar augsta riska MI sistēmu, jo īpaši, lai ierobežotu un mazinātu riskus, kurus rada augsta riska MI sistēma;
 - e) attiecīgā gadījumā izpildīt 49. panta 1. punktā minētos reģistrācijas pienākumus vai, ja reģistrāciju veic pats nodrošinātājs, nodrošināt, ka VIII pielikuma A iedaļas 3. punktā minētā informācija ir pareiza.

Pilnvarojums ļauj kompetentajām iestādēm visos jautājumos, kas saistīti ar atbilstības nodrošināšanu šai regulai, vērsties pie pilnvarotā pārstāvja, nevis pie nodrošinātāja, vai papildus nodrošinātājam.

4. Pilnvarotais pārstāvis izbeidz pilnvarojumu, ja tas uzskata vai tam ir pamats uzskatīt, ka nodrošinātājs rīkojas pretēji saviem pienākumiem, kas noteikti šajā regulā. Šādā gadījumā par pilnvarojuma izbeigšanu un tās iemesliem tas nekavējoties informē attiecīgo tirgus uzraudzības iestādi, kā arī, vajadzības gadījumā, attiecīgo paziņoto struktūru.

23. pants

Importētāju pienākumi

1. Pirms augsta riska MI sistēmas laišanas tirgū šādas sistēmas importētāji nodrošina, ka sistēma atbilst šai regulai, pārliecinoties, ka:
 - a) augsta riska MI sistēmas nodrošinātājs ir veicis attiecīgo atbilstības novērtēšanas procedūru, kas minēta 43. pantā;
 - b) nodrošinātājs ir sagatavojis tehnisko dokumentāciju saskaņā ar 11. pantu un IV pielikumu;
 - c) sistēmai ir paredzētā CE zīme, un tai ir pievienota 47. pantā minētā ES atbilstības deklarācija un lietošanas instrukcija;
 - d) nodrošinātājs ir iecēlis pilnvaroto pārstāvi saskaņā ar 22. panta 1. punktu.

2. Ja importētājam ir pietiekams pamats uzskatīt, ka augsta riska MI sistēma neatbilst šai regulai vai ir falsificēta, vai tai pievienotā dokumentācija ir falsificēta, tas sistēmu nelaiž tirgū, kamēr nav panākts, ka tā ir atbilstoša. Ja augsta riska MI sistēma rada risku 79. panta 1. punkta nozīmē, importētājs par to informē sistēmas nodrošinātāju, pilnvarotos pārstāvjus un tirgus uzraudzības iestādes.
3. Uz augsta riska MI sistēmas un attiecīgā gadījumā uz tās iepakojuma vai tai pievienotajā dokumentācijā importētāji norāda savu nosaukumu/vārdu, reģistrēto tirdzniecības nosaukumu vai reģistrēto preču zīmi un adresi, kādā ar tiem var sazināties par augsta riska MI sistēmu.
4. Importētāji nodrošina, ka laikā, kamēr tie atbild par augsta riska MI sistēmu, tās glabāšanas vai pārvadāšanas apstākļi attiecīgā gadījumā neapdraud tās atbilstību šīs sadaļas 2. nodaļā noteiktajām prasībām.
5. Importētāji 10 gadus pēc augsta riska MI sistēmas laišanas tirgū vai nodošanas ekspluatācijā glabā paziņotās struktūras izdotā sertifikāta kopiju un, attiecīgā gadījumā, lietošanas instrukcijas un 47. pantā minētās ES atbilstības deklarācijas kopiju.
6. Importētāji pēc pamatota pieprasījuma sniedz attiecīgajām kompetentajām iestādēm visu informāciju un dokumentāciju – tostarp to, kas minēta 5. punktā –, kas vajadzīga, lai apliecinātu augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām; to sniedz valodā, kas tām ir viegli saprotama. Šajā nolūkā tie arī nodrošina, ka minētajām iestādēm var darīt pieejamu tehnisko dokumentāciju.
7. Importētāji sadarbojas ar attiecīgajām kompetentajām iestādēm visās darbībās, ko minētās iestādes veic attiecībā uz augsta riska MI sistēmu, kuru importētāji laidoši tirgū, jo īpaši, lai ierobežotu un mazinātu risku, ko tā rada.

24. pants

Izplatītāju pienākumi

1. Pirms augsta riska MI sistēmu dara pieejamu tirgū, izplatītāji pārliecinās, ka augsta riska MI sistēmai ir paredzētā CE zīme vai tai ir pievienota 47. pantā minētās ES atbilstības deklarācijas kopija un lietošanas instrukcija un ka, attiecīgi, minētās sistēmas nodrošinātājs un importētājs ir izpildījuši savus attiecīgos pienākumus, kas noteikti 16. panta b) un c) punktā un 23. panta 3. punktā.
2. Ja uz tā rīcībā esošas informācijas pamata izplatītājs uzskata vai tam ir pamats uzskatīt, ka augsta riska MI sistēma neatbilst 2. iedaļā norādītajām prasībām, tas augsta riska MI sistēmu nedara pieejamu tirgū, kamēr nav panākta sistēmas atbilstība minētajām prasībām. Turklāt, ja augsta riska sistēma rada risku 79. panta 1. punkta nozīmē, izplatītājs par to attiecīgi informē sistēmas nodrošinātāju vai importētāju.
3. Izplatītāji nodrošina, ka laikā, kad tie atbild par augsta riska MI sistēmu, tās glabāšanas vai pārvadāšanas apstākļi attiecīgā gadījumā neapdraud tās atbilstību 2. iedaļā noteiktajām prasībām.
4. Izplatītājs, kas, ņemot vērā tā rīcībā esošo informāciju, uzskata vai kam ir pamats uzskatīt, ka augsta riska MI sistēma, kuru tas darījis pieejamu tirgū, neatbilst 2. iedaļā noteiktajām prasībām, veic korektīvas darbības, kas vajadzīgas, lai panāktu šīs sistēmas atbilstību šīm prasībām, izņem vai atsauc to no tirgus vai nodrošina, ka minētās korektīvās darbības veic nodrošinātājs, importētājs vai attiecīgā gadījumā jebkurš attiecīgs operators. Ja augsta riska MI sistēma rada risku 79. panta 1. punkta nozīmē, izplatītājs nekavējoties par to informē sistēmas nodrošinātāju vai importētāju un par attiecīgo augsta riska MI sistēmu kompetentās iestādes, norādot sīku informāciju, jo īpaši par neatbilstību un veiktajām korektīvajām darbībām.
5. Pēc pamatota attiecīgās kompetentās iestādes pieprasījuma augsta riska MI sistēmas izplatītāji šai iestādei sniedz visu uz 1.–4. punktā paredzētajām to darbībām attiecīgu informāciju un dokumentāciju, kas vajadzīga, lai apliecinātu augsta riska sistēmas atbilstību šīs 2. iedaļā noteiktajām prasībām.
6. Izplatītāji sadarbojas ar attiecīgajām kompetentajām iestādēm visās darbībās, ko minētās iestādes veic attiecībā uz augsta riska MI sistēmu, kuru izplatītāji darījuši pieejamu tirgū, jo īpaši, lai ierobežotu vai mazinātu risku, ko tā rada.

25. pants

Pienākumi MI vērtības ķēdē

1. Katru izplatītāju, importētāju, uzturētāju vai citu trešo personu šajā regulā uzskata par augsta riska MI sistēmas nodrošinātāju, un uz to attiecas 16. pantā paredzētie nodrošinātāja pienākumi jebkuros no šiem apstākļiem:

- a) tie uzliek savu nosaukumu/vārdu vai preču zīmi augsta riska MI sistēmai, kura jau laista tirgū vai nodota ekspluatācijā, neskarot līgumiskas vienošanās, kas paredz, ka pienākumi tiek sadalīti citādi;
- b) tie veic būtisku modifikāciju augsta riska MI sistēmā, kura jau ir laista tirgū vai jau ir nodota ekspluatācijā, tādā veidā, ka tā joprojām paliek augsta riska MI sistēma, ievērojot 6. pantu;
- c) tie veic modifikāciju MI sistēmai paredzētajā nolūkā, tostarp vispārīga lietojuma MI sistēmai, kas nav klasificēta kā augsta riska sistēma un kas jau ir laista tirgū vai nodota ekspluatācijā, tādā veidā, ka attiecīgā MI sistēma kļūst par augsta riska MI sistēmu saskaņā ar 6. pantu.

2. Ja ir 1. punktā minētie apstākļi, nodrošinātājs, kas MI sistēmu sākotnēji laidis tirgū vai nodevis ekspluatācijā, vairs netiek uzskatīts par minētās konkrētās MI sistēmas nodrošinātāju šīs regulas nolūkos. Minētais sākotnējais nodrošinātājs cieši sadarbojas ar jauniem nodrošinātājiem un dara pieejamu nepieciešamo informāciju un nodrošina saprātīgi sagaidāmu tehnisko piekļuvi un citu palīdzību, kas vajadzīga, lai pildītu šajā regulā paredzētās prasības, jo īpaši attiecībā uz atbilstību augsta riska MI sistēmu atbilstības novērtējumam. Šo punktu nepiemēro gadījumos, kad sākotnējais nodrošinātājs ir skaidri norādījis, ka tā MI sistēma nav maināma uz augsta riska MI sistēmu un tādējādi uz to neattiecas pienākums nodot dokumentāciju.

3. Gadījumos, kad augsta riska MI sistēmas ir tādu produktu drošības sastāvdaļas, uz kuriem attiecas I pielikuma A iedaļā uzskaitītie Savienības saskaņošanas tiesību akti, produkta ražotāju uzskata par augsta riska MI sistēmas nodrošinātāju un uz to attiecas 16. pantā noteiktie pienākumi kādos no šādiem apstākļiem:

- a) augsta riska MI sistēma tiek laista tirgū kopā ar produktu ar produkta ražotāja nosaukumu/vārdu vai preču zīmi;
- b) augsta riska MI sistēma tiek nodota ekspluatācijā ar produkta ražotāja nosaukumu/vārdu vai preču zīmi pēc produkta laišanas tirgū.

4. Augsta riska MI sistēmas nodrošinātājs un trešā persona, kas piegādā MI sistēmu, rīkus, pakalpojumus, sastāvdaļas vai procesus, kuri tiek izmantoti vai integrēti augsta riska MI sistēmā, ar rakstisku vienošanos precizē, pamatojoties uz vispāratzītiem jaunākajiem sasniegumiem, nepieciešamo informāciju, spējas, tehnisko piekļuvi un citu palīdzību, lai augsta riska MI sistēmas nodrošinātājs varētu pilnībā izpildīt šajā regulā noteiktos pienākumus. Šo punktu nepiemēro trešām personām, kas dara pieejamus publiskus rīkus, pakalpojumus, procesus vai sastāvdaļas, kas nav vispārīga lietojuma MI modeļi ar bezmaksas un atvērtas piekļuves licenci.

MI birojs var izstrādāt un ieteikt brīvprātīgus paraugnoteikumus līgumiem starp augsta riska MI sistēmu nodrošinātājiem un trešām personām, kuras piegādā rīkus, pakalpojumus, sastāvdaļas vai procesus, ko izmanto vai integrē augsta riska MI sistēmās. Izstrādājot minētos brīvprātīgos līguma paraugnoteikumus, MI birojs ņem vērā iespējamās līgumiskās prasības, kas piemērojamas konkrētās nozarēs vai uzņēmējdarbības gadījumos. Brīvprātīgos paraugnoteikumus publicē, un tie ir bez maksas pieejami viegli lietojamā elektroniskā formātā.

5. Šā panta 2. un 3. punkts neskar nepieciešamību ievērot un aizsargāt intelektuālā īpašuma tiesības, konfidencialu uzņēmējdarbības informāciju un komercnoslēpumus saskaņā ar Savienības un valsts tiesību aktiem.

26. pants

Augsta riska MI sistēmu uzturētāju pienākumi

1. Augsta riska MI sistēmu uzturētāji veic pienācīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu, ka viņi šādas sistēmas lieto saskaņā ar sistēmām pievienoto lietošanas instrukciju, ievērojot 3. un 6. punktu.

2. Uzturētāji uztic cilvēka virsvadību fiziskām personām, kurām ir vajadzīgā kompetence, apmācība un pilnvaras, kā arī nepieciešamais atbalsts.

3. Šā panta 1. un 2. punktā noteiktie pienākumi neskar citus uzturētāju pienākumus, kas noteikti Savienības vai valsts tiesību aktos, un uzturētāja brīvību organizēt savus resursus un darbības, lai īstenotu nodrošinātāja norādītos cilvēka virsvadības pasākumus.

4. Neskarot 1. un 2. punktu, ciktāl uzturētājs īsteno kontroli pār ievaddatiem, minētais uzturētājs nodrošina, ka ievaddati ir attiecīgi un pietiekami reprezentatīvi, ņemot vērā augsta riska MI sistēmai paredzēto nolūku.

5. Uzturētāji pārbauga augsta riska MI sistēmas darbību, pamatojoties uz lietošanas instrukciju, un attiecīgā gadījumā informē nodrošinātājus saskaņā ar 72. pantu. Ja uzturētājiem ir pamats uzskatīt, ka augsta riska MI sistēmas lietošana saskaņā ar instrukciju var radīt risku 79. panta 1. punkta nozīmē, viņi bez liekas kavēšanās informē nodrošinātāju vai izplatītāju un attiecīgo tirgus uzraudzības iestādi un aptur minētās sistēmas lietošanu. Ja uzturētāji ir identificējuši nopietnu incidentu, viņi par minēto incidentu arī nekavējoties informē vispirms nodrošinātāju un pēc tam importētāju vai izplatītāju un attiecīgās tirgus uzraudzības iestādes. Ja uzturētājs nevar sazināties ar nodrošinātāju, *mutatis mutandis* piemēro 73. pantu. Šis pienākums neattiecas uz MI sistēmu uzturētāju, kas ir tiesībaizsardzības iestādes, sensitīviem operatīvajiem datiem.

Attiecībā uz uzturētājiem, kas ir finanšu iestādes, uz kurām attiecas Savienības finanšu pakalpojumu jomas tiesību aktos paredzētās prasības par to iekšējo pārvaldību, kārtību vai procesiem, pirmajā daļā noteikto pārraudzības pienākumu uzskata par izpildītu, ja ir izpildīti noteikumi par iekšējās pārvaldības kārtību, procesiem un mehānismiem, ievērojot attiecīgos tiesību aktus finanšu pakalpojumu jomā.

6. Augsta riska MI sistēmu uzturētāji glabā minētās augsta riska MI sistēmas ģenerētās žurnāldatnes, ciktāl šādas žurnāldatnes ir viņu pārziņā, tādu laikposmu, kas atbilst augsta riska MI sistēmai paredzētajam nolūkam – vismaz sešus mēnešus, ja vien piemērojamajos Savienības vai valsts tiesību aktos, jo īpaši Savienības tiesību aktos par personas datu aizsardzību, nav noteikts citādi.

Uzturētāji, kas ir finanšu iestādes, uz kurām attiecas Savienības finanšu pakalpojumu jomas tiesību aktos paredzētās prasības par to iekšējo pārvaldību, kārtību vai procesiem, žurnāldatnes uztur kā daļu no dokumentācijas, kuru glabā, ievērojot attiecīgos Savienības tiesību aktus finanšu pakalpojumu jomā.

7. Pirms augsta riska MI sistēmas nodošanas ekspluatācijā vai lietošanas darbavietā uzturētāji, kas ir darba devēji, informē darba ņēmēju pārstāvjus un skartos darba ņēmējus par to, ka uz viņiem attieksies augsta riska MI sistēmas lietošana. Šo informāciju attiecīgā gadījumā sniedz saskaņā ar noteikumiem un procedūrām, kas paredzētas Savienības un valsts tiesību aktos un praksē attiecībā uz darba ņēmēju un viņu pārstāvju informēšanu.

8. Augsta riska MI sistēmu uzturētāji, kas ir publiskas iestādes, vai Savienības iestādes, struktūras, biroji vai aģentūras pilda 49. pantā minētos reģistrācijas pienākumus. Ja šādi uzturētāji konstatē, ka augsta riska MI sistēma, kuru viņi plāno lietot, nav reģistrēta 71. pantā minētajā ES datubāzē, viņi minēto sistēmu nelieto un informē nodrošinātāju vai izplatītāju.

9. Attiecīgā gadījumā augsta riska MI sistēmu uzturētāji izmanto saskaņā ar šīs regulas 13. pantu sniegto informāciju, lai izpildītu pienākumu veikt novērtējumu par ietekmi uz datu aizsardzību, kā paredzēts Regulas (ES) 2016/679 35. pantā vai Direktīvas (ES) 2016/680 27. pantā.

10. Neskarot Direktīvu (ES) 2016/680, lai izmeklēšanas ietvaros veiktu personas, kas tiek turēta aizdomās vai ir notiesāta par noziedzīga nodarījuma izdarīšanu, mērķtiecīgu meklēšanu, vēlāklaika biometriskās identifikācijai paredzētas augsta riska MI sistēmas uzturētājs *ex-ante* vai bez liekas kavēšanās un ne vēlāk kā 48 stundu laikā lūdz tiesu iestādei vai administratīvai iestādei, kuras lēmums ir saistošs un uz ko attiecas tiesas pārbaude, atļauju lietot minēto sistēmu, izņemot gadījumus, kad tā tiek lietota potenciāla aizdomās turamā sākotnējai identifikācijai, pamatojoties uz objektīviem un pārbaudāmiem faktiem, kas ir tieši saistīti ar nodarījumu. Katra lietošana ir ierobežota un attiecas tikai uz to, kas ir absolūti nepieciešams konkrēta noziedzīga nodarījuma izmeklēšanai.

Ja atļauja, kas pieprasīta, ievērojot pirmo daļu, netiek piešķirta, ar minēto pieprasīto atļauju saistīto vēlāklaika biometriskās identifikācijas sistēmas lietošanu nekavējoties pārtrauc un personas datus, kas saistīti ar tādu augsta riska MI sistēmas lietošanu, par kuru tika lūgta atļauja, dzēš.

Nekādā gadījumā šādu vēlāklaika biometriskās identifikācijai paredzētu augsta riska MI sistēmu nelieto tiesībsardzības nolūkos nemērķorientētā veidā, bez kādas saistības ar noziedzīgu nodarījumu, kriminālprocesu, reāliem un pašreizējiem vai reāliem un paredzamiem noziedzīga nodarījuma draudiem vai konkrētas pazudušas personas meklēšanu. Nodrošina, ka lēmumu, kas personai rada nelabvēlīgas tiesiskas sekas, tiesībsardzības iestādes nevar pieņemt, balstoties vienīgi uz šādu vēlāklaika biometriskās tālidentifikācijas sistēmu sniegto iznākumu.

Šis punkts neskar Regulas (ES) 2016/679 9. pantu un Direktīvas (ES) 2016/680 10. pantu attiecībā uz biometrisku datu apstrādi.

Neatkarīgi no nolūka vai uzturētāja katru šādu augsta riska MI sistēmu lietošanu dokumentē attiecīgā policijas datnē un pēc pieprasījuma dara pieejamu attiecīgajai tirgus uzraudzības iestādei un valsts datu aizsardzības iestādei, izņemot ar tiesībsardzību saistītu sensitīvu operatīvo datu izpaušanu. Šī daļa neskar pilnvaras, kas ar Direktīvu (ES) 2016/680 piešķirtas uzraudzības iestādēm.

Uzturētāji iesniedz attiecīgajai tirgus uzraudzības iestādei un valsts datu aizsardzības iestādei gada ziņojumus par gadījumiem, kad tie lietojuši vēlāklaika biometriskās tālidentifikācijas sistēmas, izņemot ar tiesībsardzību saistītu sensitīvu operatīvo datu izpaušanu. Ziņojumus var agregēt, lai vienā operācijā aptvertu vairāk nekā vienu ieviešanu.

Dalībvalstis saskaņā ar Savienības tiesību aktiem var ieviest ierobežojošākus tiesību aktus par vēlāklaika biometriskās tālidentifikācijas sistēmu lietošanu.

11. Neskarot šīs regulas 50. pantu, III pielikumā minēto augsta riska MI sistēmu uzturētāji, kas pieņem lēmumus vai palīdz pieņemt lēmumus saistībā ar fiziskām personām, informē fiziskas personas, ka uz tām attiecas augsta riska MI sistēmas lietošana. Augsta riska MI sistēmām, ko izmanto tiesībsardzības nolūkos, piemēro Direktīvas (ES) 2016/680 13. pantu.

12. Uzturētāji sadarbojas ar attiecīgajām kompetentajām iestādēm visās darbībās, ko minētās iestādes šīs regulas īstenošanas nolūkā veic saistībā ar augsta riska MI sistēmu.

27. pants

Augsta riska MI sistēmu ietekmes uz pamattiesībām novērtējums

1. Pirms tiek lietota augsta riska MI sistēma, kas minēta 6. panta 2. punktā, izņemot augsta riska MI sistēmas, ko paredzēts lietot III pielikuma 2. punktā uzskaitītā jomā, uzturētāji, kas ir publisko tiesību subjekti vai privātas vienības, kas sniedz sabiedriskos pakalpojumus, un III pielikuma 5. punkta b) un c) apakšpunktos minēto augsta riska MI sistēmu uzturētāji, veic novērtējumu par ietekmi uz pamattiesībām, kādu var radīt šādas sistēmas lietošana. Minētajā nolūkā uzturētāji veic novērtējumu, kurā ietver

a) to uzturētāja procesu aprakstu, kuros augsta riska MI sistēma tiks lietota saskaņā ar tai paredzēto nolūku;

b) laikposma un biežuma aprakstu, kādā paredzēts lietot katru augsta riska MI sistēmu;

c) to fizisku personu un grupu kategorijas, kuras, iespējams, skartu sistēmas izmantošana konkrētā kontekstā;

d) konkrētus kaitējuma riskus, kam, iespējams, būtu ietekme uz to fizisku personu vai personu grupu kategorijām, kas noteiktas, ievērojot šā punkta c) apakšpunktu, ņemot vērā informāciju, ko nodrošinātājs sniedzis, ievērojot 13. pantu;

e) aprakstu par cilvēka virsvadības pasākumu īstenošanu saskaņā ar lietošanas instrukciju;

f) pasākumus, kas veicami, ja minētie riski materializējas, tostarp iekšējās pārvaldības kārtību un sūdzību mehānismus.

2. Šā panta 1. punktā paredzētais pienākums attiecas uz augsta riska MI sistēmas pirmo lietošanu. Uzturētājs līdzīgos gadījumos var izmantot iepriekš veiktus novērtējumus par ietekmi uz pamattiesībām vai esošu novērtējumu, ko veicis nodrošinātājs. Ja augsta riska MI sistēmas lietošanas laikā uzturētājs uzskata, ka kāds no 1. punktā uzskaitītajiem elementiem ir mainījies vai ir novecojis, uzturētājs veic nepieciešamos pasākumus, lai atjauninātu informāciju.
3. Pēc tam, kad ir veikts šā panta 1. punktā minētais novērtējums, uzturētājs paziņo tirgus uzraudzības iestādei tā rezultātus, iesniedz kā paziņojuma daļu aizpildīto veidni, kas minēta šā panta 5. punktā. Gadījumā, kas minēts 46. panta 1. punktā, uzturētāji var tikt atbrīvoti no minētā paziņošanas pienākuma.
4. Ja kāds no šajā pantā paredzētajiem pienākumiem jau ir izpildīts ar novērtējumu par ietekmi uz datu aizsardzību, ko veic, ievērojot Regulas (ES) 2016/679 35. pantu vai Direktīvas (ES) 2016/680 27. pantu, šā panta 1. punktā minētais novērtējums par ietekmi uz pamattiesībām papildina šo novērtējumu par ietekmi uz datu aizsardzību.
5. MI birojs izstrādā anketas veidni, tostarp, izmantojot automatizētu rīku, lai atvieglotu uzturētājiem šajā pantā paredzēto pienākumu pildīšanu vienkāršotā veidā.

4. IEDAĻA

Paziņojošās iestādes un paziņotās struktūras

28. pants

Paziņojošās iestādes

1. Katra dalībvalsts izraugās vai izveido vismaz vienu paziņojošo iestādi, kas atbild par vajadzīgo procedūru izveidi un izpildi atbilstības novērtēšanas struktūru novērtēšanai, izraudzīšanai un paziņošanai, kā arī to pārraudzībai. Minētās procedūras izstrādā, sadarbojoties visu dalībvalstu paziņojošajām iestādēm.
2. Dalībvalstis var nolemt, ka 1. punktā minēto novērtēšanu un pārraudzību jāveic valsts akreditācijas struktūrai Regulas (EK) Nr. 765/2008 nozīmē un saskaņā ar to.
3. Paziņojošās iestādes tiek izveidotas, organizētas un darbojas tā, lai nerastos interešu konflikts ar atbilstības novērtēšanas struktūrām un tiktu garantēta to darbību objektivitāte un neitralitāte.
4. Paziņojošās iestādes tiek organizētas tā, lai lēmumus saistībā ar atbilstības novērtēšanas struktūru paziņošanu pieņemtu kompetentās personas, kas nav tās pašas, kuras veikušas minēto struktūru novērtēšanu.
5. Paziņojošās iestādes nepiedāvā un neveic darbības, ko veic atbilstības novērtēšanas struktūras, vai komerciālus vai uz konkurenci balstītus konsultāciju pakalpojumus.
6. Paziņojošās iestādes nodrošina to iegūtās informācijas konfidencialitāti saskaņā ar 78. pantu.
7. To uzdevumu pienācīgai izpildei paziņojošo iestāžu rīcībā ir pietiekams skaits kompetentu darbinieku. Kompetentajam personālam attiecīgā gadījumā ir to funkcijai nepieciešamās speciālās zināšanas tādās jomās kā informācijas tehnoloģijas, MI un tiesības, tostarp pamattiesību uzraudzība.

29. pants

Atbilstības novērtēšanas struktūras pieteikums paziņošanai

1. Atbilstības novērtēšanas struktūras iesniedz paziņošanas pieteikumu paziņojošajai iestādei tajā dalībvalstī, kurā tās izveidotas.

2. Paziņošanas pieteikumam pievieno aprakstu par atbilstības novērtēšanas darbībām, atbilstības novērtēšanas moduli vai moduļiem un MI sistēmu veidiem, attiecībā uz kuriem atbilstības novērtēšanas struktūra apliecina savu kompetenci, kā arī valsts akreditācijas struktūras izsniegtu akreditācijas sertifikātu, ja tāds ir, kas apliecina, ka atbilstības novērtēšanas struktūra atbilst 31. pantā noteiktajām prasībām.

Pievieno derīgus dokumentus, kas saistīti ar pieteikuma iesniedzējas paziņotās struktūras esošu izraudzīšanos saskaņā ar citiem Savienības saskaņošanas tiesību aktiem.

3. Ja attiecīgā atbilstības novērtēšanas struktūra nevar iesniegt akreditācijas sertifikātu, tā iesniedz paziņojošajai iestādei visus dokumentāros pierādījumus, kas vajadzīgi, lai pārbaudītu, atzītu un regulāri pārbaudītu tās atbilstību 31. pantā noteiktajām prasībām.

4. Attiecībā uz paziņotajām struktūrām, kuras ir izraudzītas saskaņā ar citiem Savienības saskaņošanas tiesību aktiem, visus dokumentus un sertifikātus, kas saistīti ar minēto izraudzīšanos, var izmantot, lai vajadzības gadījumā atbalstītu to izraudzīšanās procedūru, kura paredzēta šajā regulā. Paziņotā struktūra atjaunina šā panta 2. un 3. punktā minēto dokumentāciju katru reizi, kad notiek attiecīgas izmaiņas, lai par paziņotajām struktūrām atbildīgā iestāde varētu pārbaudīt un pārbaudīt, vai tiek pastāvīgi nodrošināta atbilstība visām 31. pantā norādītajām prasībām.

30. pants

Paziņošanas procedūra

1. Paziņojošās iestādes var paziņot tikai tādas atbilstības novērtēšanas struktūras, kas atbilst 31. pantā noteiktajām prasībām.

2. Paziņojošās iestādes paziņošanu Komisijai un pārējām dalībvalstīm veic, izmantojot Komisijas izstrādāto un pārvaldīto elektronisko paziņošanas rīku, par katru 1. punktā minēto atbilstības novērtēšanas struktūru.

3. Šā panta 2. punktā minētajā paziņojumā iekļauj sīkas ziņas par atbilstības novērtēšanas darbībām, atbilstības novērtēšanas moduli vai moduļiem, attiecīgajiem MI sistēmu veidiem, kā arī attiecīgo kompetences apliecinājumu. Ja paziņošana netiek balstīta uz 29. panta 2. punktā minēto akreditācijas sertifikātu, paziņojošā iestāde iesniedz Komisijai un pārējām dalībvalstīm dokumentārus pierādījumus, kuri apliecina atbilstības novērtēšanas struktūras kompetenci un ieviestos pasākumus, ar ko nodrošina, ka minētā struktūra tiks regulāri pārbaudīta un ka tā pastāvīgi atbildīs 31. pantā noteiktajām prasībām.

4. Attiecīgā atbilstības novērtēšanas struktūra var veikt paziņotās struktūras darbības tikai tad, ja Komisija vai pārējās dalībvalstis nav paidušas iebildumus divu nedēļu laikā no paziņojošās iestādes iesniegta paziņojuma, ja tajā ir iekļauts 29. panta 2. punktā minētais akreditācijas sertifikāts, vai divu mēnešu laikā no paziņojošās iestādes iesniegta paziņojuma, ja tajā ir iekļauti 29. panta 3. punktā minētie dokumentārie pierādījumi.

5. Ja tiek celti iebildumi, Komisija nekavējoties sāk apspriešanos ar attiecīgajām dalībvalstīm un atbilstības novērtēšanas struktūru. To ņemot vērā, Komisija lemj, vai atļauja ir pamatota. Komisija savu lēmumu adresē attiecīgajai dalībvalstij un attiecīgajai atbilstības novērtēšanas struktūrai.

31. pants

Prasības attiecībā uz paziņotajām struktūrām

1. Paziņoto struktūru izveido saskaņā ar dalībvalsts valsts tiesību aktiem, un tā ir juridiska persona.

2. Paziņotās struktūras atbilst organizatoriskajām, kvalitātes vadības, resursu un procesa prasībām, kas nepieciešamas to uzdevumu veikšanai, kā arī atbilstīgām kibernetikas prasībām.

3. Paziņoto struktūru uzbūve, pienākumu sadalījums, pārskatu sniegšanas kārtība un darbība nodrošina uzticēšanos paziņoto struktūru sniegtam un veikto atbilstības novērtēšanas darbību rezultātiem.

4. Paziņotās struktūras ir neatkarīgas no augsta riska MI sistēmas nodrošinātāja, attiecībā uz kuru tās veic atbilstības novērtēšanas darbības. Paziņotās struktūras ir neatkarīgas arī no citiem operatoriem, kuriem ir ekonomiskā ieinteresētība novērtējamajās augsta riska MI sistēmās, kā arī no visiem nodrošinātāja konkurentiem. Tas nedrīkst lietot novērtētās augsta riska MI sistēmas, kas ir vajadzīgas atbilstības novērtēšanas struktūras darbībām, vai lietot šādas augsta riska MI sistēmas personīgām vajadzībām.
5. Ne atbilstības novērtēšanas struktūra, tās augstākā līmeņa vadība, ne darbinieki, kas atbild par tai paredzēto atbilstības novērtēšanas uzdevumu veikšanu, nav tieši iesaistīti augsta riska MI sistēmu projektēšanā, izstrādē, tirdzniecībā vai lietošanā un nepārstāv minētajās darbībās iesaistītas personas. Viņi neiesaistās darbībās, kas varētu būt konfliktā ar viņu spriedumu neatkarību vai godprātību saistībā ar atbilstības novērtēšanas darbībām, attiecībā uz kurām viņi ir paziņotā struktūra. Tas jo īpaši attiecas uz konsultāciju pakalpojumiem.
6. Paziņotās struktūras ir organizētas un darbojas tā, lai nodrošinātu savu darbību neatkarību, objektivitāti un neitralitāti. Paziņotās struktūras dokumentē un ievieš struktūru un procedūras, kas vajadzīgas, lai garantētu objektivitāti un veicinātu un piemērotu objektivitātes principus attiecībā uz visu to organizāciju, personālu un novērtēšanas darbībām.
7. Paziņotās struktūras ievieš dokumentētas procedūras, lai nodrošinātu, ka to personāls, komitejas, meitasuzņēmumi, apakšuzņēmēji un jebkura saistītā struktūra vai ārējo struktūru darbinieki saskaņā ar 78. pantu ievēro tās informācijas konfidencialitāti, kas nonāk viņu rīcībā, veicot atbilstības novērtēšanas darbības, izņemot gadījumus, kad tās izpaušana tiek prasīta tiesību aktos. Paziņoto struktūru personālam ir pienākums ievērot dienesta noslēpumu attiecībā uz visu informāciju, kas iegūta, veicot šajā regulā paredzētos uzdevumus, izņemot attiecībā uz tās dalībvalsts paziņojošajām iestādēm, kurā tiek veiktas viņu darbības.
8. Paziņotajām struktūrām ir procedūras darbību veikšanai, kurās pienācīgi ņem vērā nodrošinātāja lielumu, nozari, kurā tas darbojas, struktūru un attiecīgās MI sistēmas sarežģītības pakāpi.
9. Paziņotajām struktūrām ir pienācīgi apdrošināta civiltiesiskā atbildība attiecībā uz savām atbilstības novērtēšanas darbībām, ja vien dalībvalsts, kurā tās ir iedibinātas, neuzņemas atbildību saskaņā ar šīs valsts tiesību aktiem vai ja dalībvalsts pati tieši neatbild par atbilstības novērtēšanu.
10. Paziņotās struktūras spēj veikt visus uzdevumus, kas tām noteikti šajā regulā, ar visaugstāko profesionālo godaprātu un nepieciešamo kompetenci konkrētajā jomā, neatkarīgi no tā, vai šos uzdevumus veic paziņotās struktūras pašas vai cita persona to uzdevumā un atbildībā.
11. Paziņotajām struktūrām ir pietiekamas iekšējās kompetences, lai tās varētu efektīvi izvērtēt uzdevumus, ko to vārdā veic ārējās personas. Paziņotajai struktūrai ir pastāvīgi pieejams pietiekams administratīvais, tehniskais, juridiskais un zinātniskais personāls, kam ir pieredze un zināšanas par attiecīgajiem MI sistēmu veidiem, datiem un datojumu, kā arī par 2. iedaļā noteiktajām prasībām.
12. Paziņotās struktūras piedalās 38. pantā minētajās koordinācijas darbībās. Tās arī tiešā veidā piedalās vai ir pārstāvētas Eiropas standartizācijas organizācijās, vai nodrošina, ka ir informētas un regulāri atjaunina zināšanas par attiecīgajiem standartiem.

32. pants

Pieņemums par atbilstību prasībām attiecībā uz paziņotajām struktūrām

Ja atbilstības novērtēšanas struktūra apliecina savu atbilstību kritērijiem, kas noteikti attiecīgajos saskaņotajos standartos vai to daļās, uz kuriem atsaucas publicētas Eiropas Savienības Oficiālajā Vēstnesī, pieņem, ka tā atbilst 31. pantā noteiktajām prasībām, ciktāl piemērojamie saskaņotie standarti aptver minētās prasības.

33. pants

Paziņoto struktūru meitasuzņēmumi un apakšuzņēmuma līgumu slēgšana

1. Ja paziņotā struktūra par konkrētu ar atbilstības novērtēšanu saistītu uzdevumu veikšanu slēdz apakšuzņēmuma līgumus vai to veikšanai izmanto meitasuzņēmumu, tā pārliecinās, ka apakšuzņēmējs vai meitasuzņēmums atbilst 31. panta prasībām, un attiecīgi informē paziņojošo iestādi.
2. Paziņotās struktūras uzņemas pilnu atbildību par uzdevumiem, ko veic jebkuri apakšuzņēmēji vai filiāles.
3. Par darbībām var slēgt apakšuzņēmuma līgumu vai tās var veikt meitasuzņēmums tikai tad, ja nodrošinātājs tam piekrīt. Paziņotās struktūras publisko savu filiāļu sarakstu.
4. Attiecīgos dokumentus par apakšuzņēmēja vai meitasuzņēmuma kvalifikācijas un darba, ko tie veikuši atbilstīgi šai regulai, novērtēšanu glabā paziņojošajai iestādei pieejamus piecus gadus no dienas, kad ir izbeigts apakšuzņēmuma līgums.

34. pants

Paziņoto struktūru pienākumi to darbības laikā

1. Paziņotās struktūras pārbauda augsta riska MI sistēmu atbilstību saskaņā ar 43. pantā noteiktajām atbilstības novērtēšanas procedūrām.
2. Paziņotās struktūras, veicot savas darbības, izvairās no nevajadzīga sloga nodrošinātājiem un pienācīgi ņem vērā nodrošinātāja lielumu, nozari, kurā tas darbojas, tā struktūru un attiecīgās augsta riska MI sistēmas sarežģītības pakāpi, jo īpaši nolūkā samazināt administratīvo slogu un atbilstības nodrošināšanas izmaksas mikrouzņēmumiem un mazajiem uzņēmumiem Komisijas lēmuma 2003/361/EK nozīmē. Paziņotā struktūra tomēr ievēro tādu stingrības pakāpi un aizsardzības līmeni, kāds ir vajadzīgs, lai augsta riska MI sistēma atbilstu šīs regulas prasībām.
3. Paziņotās struktūras dara pieejamu un pēc pieprasījuma iesniedz visu attiecīgo dokumentāciju, ieskaitot nodrošinātāju dokumentāciju, paziņojošajai iestādei, kas minēta 28. pantā, lai minētā iestāde varētu veikt novērtēšanas, izraudzīšanās, paziņošanas un pārraudzības darbības un lai atvieglotu šajā iedaļā izklāstīto novērtēšanu.

35. pants

Paziņoto struktūru identifikācijas numuri un saraksti

1. Komisija piešķir vienotu identifikācijas numuru katrai paziņotajai struktūrai, arī tad, ja struktūra ir paziņota saskaņā ar vairāk nekā vienu Savienības tiesību aktu.
2. Komisija dara publiski pieejamu to struktūru sarakstu, kas paziņotas saskaņā ar šo regulu, tostarp to identifikācijas numurus un darbības, attiecībā uz kurām tās ir paziņotas. Komisija nodrošina saraksta regulāru atjaunināšanu.

36. pants

Izmaiņas paziņojumos

1. Paziņojošā iestāde, izmantojot 30. panta 2. punktā minēto elektronisko paziņošanas rīku, paziņo Komisijai un pārējām dalībvalstīm par visām attiecīgām izmaiņām paziņojumā par paziņoto struktūru.
2. Procedūras, kas noteiktas 29. un 30. pantā, piemēro gadījumos, kad tiek paplašināts paziņojuma tvērums.

Ja paziņojumā tiek izdarītas citas izmaiņas, kuras nav tā tvēruma paplašināšana, piemēro 3. līdz 9. punktos noteiktās procedūras.

3. Ja paziņotā struktūra nolemj pārtraukt savas atbilstības novērtēšanas darbības, tā pēc iespējas drīz un plānotas pārtraukšanas gadījumā – vismaz vienu gadu pirms savu darbību pārtraukšanas informē paziņojošo iestādi un attiecīgos nodrošinātājus. Paziņotās struktūras sertifikāti var palikt derīgi deviņus mēnešus ilgu laikposmu pēc paziņotās struktūras darbību pārtraukšanas ar nosacījumu, ka kāda cita paziņotā struktūra ir rakstiski apliecinājusi, ka tā uzņemsies pienākumus attiecībā uz augsta riska MI sistēmām, uz kurām attiecas minētie sertifikāti. Pēdējā minētā paziņotā struktūra līdz tāda deviņu mēnešu laikposma beigām pabeidz skarto augsta riska MI sistēmu pilnīgu novērtēšanu pirms jaunu sertifikātu izdošanas minētajām sistēmām. Ja paziņotā struktūra savu darbību ir pārtraukusi, paziņojošā iestāde izraudzīšanos atsauc.

4. Ja paziņojošajai iestādei ir pietiekams pamats uzskatīt, ka paziņotā struktūra vairs neatbilst 31. pantā noteiktajām prasībām vai ka tā nepilda savus pienākumus, paziņojošā iestāde nekavējoties ar vislielāko rūpību izskata šo jautājumu. Šajā sakarā tā informē attiecīgo paziņoto struktūru par celtajiem iebildumiem un dod tai iespēju darīt zināmu savu viedokli. Ja paziņojošā iestāde secina, ka paziņotā struktūra vairs neatbilst 31. pantā noteiktajām prasībām vai ka tā nepilda savus pienākumus, paziņojošā iestāde attiecīgi ierobežo, aptur vai atsauc izraudzīšanos, atkarībā no tā, cik nopietna ir neatbilstība minētajām prasībām vai minēto pienākumu nepildīšana. Tā nekavējoties informē Komisiju un pārējās dalībvalstis.

5. Ja paziņotās struktūras izraudzīšanās ir apturēta, ierobežota vai pilnīgi vai daļēji atsaukta, tā 10 dienu laikā informē attiecīgos nodrošinātājus.

6. Ja izraudzīšanās tiek ierobežota, apturēta vai atsaukta, paziņojošā iestāde veic attiecīgos pasākumus, lai nodrošinātu, ka attiecīgās paziņotās struktūras datnes tiek glabātas, un pēc pieprasījuma darītu tās pieejamas paziņojošajām iestādēm citās dalībvalstīs un tirgus uzraudzības iestādēm.

7. Ja izraudzīšanos ierobežo, aptur vai atsauc, paziņojošā iestāde:

- a) novērtē ietekmi uz sertifikātiem, ko izdevusi paziņotā struktūra;
 - b) triju mēnešu laikā pēc tam, kad tā ir paziņojusi par izmaiņām saistībā ar izraudzīšanos, Komisijai un pārējām dalībvalstīm iesniedz ziņojumu par saviem konstatējumiem;
 - c) prasa paziņotajai struktūrai saprātīgā laikposmā, kuru nosaka iestāde, apturēt vai atsaukt jebkādos neatbilstīgi izdotus sertifikātus, lai nodrošinātu tirgū esošo augsta riska MI sistēmu nepārtrauktu atbilstību;
 - d) informē Komisiju un dalībvalstis par sertifikātiem, kurus tā ir pieprasījusi apturēt vai atsaukt;
 - e) sniedz tās dalībvalsts valsts kompetentajām iestādēm, kurā ir nodrošinātāja juridiskā adrese, visu attiecīgo informāciju par sertifikātiem, kurus tā ir pieprasījusi apturēt vai atsaukt; minētā iestāde vajadzības gadījumā veic pienācīgos pasākumus, lai izvairītos no potenciāla riska veselībai, drošībai vai pamattiesībām.
8. Izņemot neatbilstīgi izdotus sertifikātus un gadījumus, kad izraudzīšanās ir apturēta vai ierobežota, sertifikāti paliek derīgi kādos no šādiem apstākļiem:
- a) paziņojošā iestāde viena mēneša laikā pēc apturēšanas vai ierobežošanas ir apliecinājusi, ka saistībā ar sertifikātiem, kurus skar apturēšana vai ierobežošana, nepastāv risks veselībai, drošībai vai pamattiesībām, un paziņojošā iestāde ir izstrādājusi grafiku darbībām, ar kurām labot apturēšanas vai ierobežošanas iemeslus; vai
 - b) paziņojošā iestāde ir apliecinājusi, ka apturēšanas vai ierobežošanas laikā netiks izdoti, grozīti vai atkārtoti izdoti nekādi ar apturēšanu saistīti sertifikāti, un tā norāda, vai paziņotajai struktūrai ir spējas turpināt pārraudzību un saglabāt atbildību par spēkā esošajiem izdotajiem sertifikātiem apturēšanas vai ierobežošanas laikposmā; ja paziņojošā iestāde lemj, ka paziņotajai struktūrai nav spēju uzturēt spēkā esošos izdotos sertifikātus, tās sistēmas nodrošinātājs, uz kuru attiecas sertifikāts, trīs mēnešu laikā pēc apturēšanas vai ierobežošanas rakstiski apliecina tās dalībvalsts valsts kompetentajām iestādēm, kurā ir tā juridiskā adrese, ka cita kvalificēta paziņotā struktūra pagaidu kārtā uzņemas paziņotās struktūras funkcijas, lai pārraudzītu un saglabātu atbildību par sertifikātiem apturēšanas vai ierobežošanas laikposmā.

9. Izņemot neatbilstīgi izdotus sertifikātus un gadījumus, kad izraudzīšanās ir atsaukta, sertifikāti paliek derīgi uz deviņu mēnešu laikposmu šādos apstākļos:

- a) tās dalībvalsts valsts kompetentā iestāde, kurā ir sertifikātā aptvertās augsta riska MI sistēmas nodrošinātāja juridiskā adrese, ir apliecinājusi, ka saistībā ar attiecīgajām augsta riska MI sistēmām nepastāv risks veselībai, drošībai vai pamattiesībām; un
- b) cita paziņotā struktūra ir rakstiski apliecinājusi, ka tā nekavējoties uzņemsies atbildību par minēto MI sistēmu novērtēšanu, un pabeidz novērtēšanu divpadsmit mēnešu laikā pēc izraudzīšanās atsaukšanas.

Pirmajā daļā minētajos apstākļos tās dalībvalsts valsts kompetentā iestāde, kurā ir sertifikātā aptvertās sistēmas nodrošinātāja juridiskā adrese, var pagarināt sertifikātu pagaidu derīgumu uz papildu trīs mēnešu laikposmiem, kuri kopumā nepārsniedz 12 mēnešus.

Valsts kompetentā iestāde vai paziņotā struktūra, kas uzņemas tās paziņotās struktūras funkcijas, kuru skar izraudzīšanās izmaiņas, par to nekavējoties informē Komisiju, pārējās dalībvalstis un citas paziņotās struktūras.

37. pants

Paziņoto struktūru kompetences apstrīdēšana

1. Vajadzības gadījumā Komisija izmeklē visus gadījumus, kuros ir pamats šaubīties par paziņotās struktūras kompetenci vai par to, ka paziņotā struktūra joprojām pilda 31. pantā noteiktās prasības un tai piemērojamos pienākumus.
2. Paziņojošā iestāde pēc pieprasījuma sniedz Komisijai visu attiecīgo informāciju, kas saistīta ar attiecīgās paziņotās struktūras paziņošanu vai tās kompetences saglabāšanu.
3. Komisija nodrošina, ka ar visu sensitīvo informāciju, kas izmeklēšanas gaitā iegūta, ievērojot šo pantu, rīkojas konfidenciāli saskaņā ar 78. pantu.
4. Ja Komisija noskaidro, ka paziņotā struktūra neatbilst vai vairs neatbilst uz tās paziņošanu attiecīgajām prasībām, tā attiecīgi informē paziņojošo dalībvalsti un lūdz to veikt nepieciešamos korektīvos pasākumus, tostarp vajadzības gadījumā apturēt vai atsaukt paziņošanu. Ja dalībvalsts neveic nepieciešamos korektīvos pasākumus, Komisija ar īstenošanas aktu var apturēt, ierobežot vai atsaukt izraudzīšanos. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

38. pants

Paziņoto struktūru koordinācija

1. Komisija nodrošina, ka attiecībā uz augsta riska MI sistēmām tiek izveidota atbilstoša koordinācija un sadarbība starp paziņotajām struktūrām, kas, ievērojot šo regulu, darbojas atbilstības novērtēšanas procedūrās, un pienācīgi notiek paziņoto struktūru nozares grupas veidā.
2. Katra paziņojošā iestāde nodrošina, ka tās paziņotās struktūras tieši vai ar izraudzītu pārstāvju starpniecību piedalās 1. punktā minētās grupas darbā.
3. Komisija nodrošina zināšanu un paraugprakses apmaiņu starp paziņojošajām iestādēm.

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 paziņoto struktūru darbības saskaņā ar šo regulu, ar noteikumu, ka tās atbilst 31. pantā noteiktajām prasībām vai nodrošina līdzvērtīgu atbilstības līmeni.

5. IEDAĻA

Standarti, atbilstības novērtēšana, sertifikāti, reģistrācija

40. pants

Saskaņoti standarti un standartizācijas nodevumi

1. Tiek uzskatīts, ka augsta riska MI sistēmas, kas atbilst saskaņotiem standartiem vai to daļām, kuru atsaucies ir publicētas Eiropas Savienības Oficiālajā Vēstnesī saskaņā ar Regulu (ES) Nr. 1025/2012, izpilda šīs nodaļas 2. iedaļā izklāstītās prasības vai – attiecīgā gadījumā – šīs regulas V nodaļas 2. un 3. iedaļā noteiktos pienākumus, ciktāl minētie standarti aptver minētās prasības vai pienākumus.

2. Komisija bez liekas kavēšanās saskaņā ar Regulas (ES) Nr. 1025/2012 10. pantu izdod standartizācijas pieprasījumus, kas aptver visas šīs nodaļas 2. iedaļā noteiktās prasības, un attiecīgā gadījumā standartizācijas pieprasījumus, kas aptver šīs regulas V nodaļas 2. un 3. iedaļā noteiktos pienākumus. Standartizācijas pieprasījumos pieprasa arī nodevumus par ziņošanas un dokumentēšanas procesiem nolūkā panākt lielāku MI sistēmu resursefektivitāti, piemēram, augsta riska MI sistēmas enerģijas patēriņa un citu resursu patēriņa samazināšanu tās darbmuža laikā, un par vispārīga lietojuma MI modeļu energoefektīvu izstrādi. Sagatavojot standartizācijas pieprasījumu, Komisija apspriežas ar MI padomi un attiecīgām ieinteresētajām personām, tostarp konsultatīvo forumu.

Izdodot standartizācijas pieprasījumu Eiropas standartizācijas organizācijām, Komisija konkrēti norāda, ka standartiem ir jābūt skaidriem, saskaņotiem, tostarp ar standartiem, kas izstrādāti dažādās nozarēs produktiem, uz kuriem attiecas I pielikumā uzskaitītie esošie Savienības saskaņošanas tiesību akti, un tiem jābūt vērīgiem uz to, lai nodrošinātu, ka augsta riska MI sistēmas vai vispārīga lietojuma MI modeļi, kas laisti tirgū vai nodoti ekspluatācijā Savienībā, atbilst attiecīgajām šajā regulā noteiktajām prasībām vai pienākumiem.

Komisija pieprasa Eiropas standartizācijas organizācijām saskaņā ar Regulas (ES) Nr. 1025/2012 24. pantu sniegt pierādījumus par to, ka tās dara visu iespējamo, lai sasniegtu šā punkta pirmajā un otrajā daļā minētos mērķus.

3. Standartizācijas procesa dalībnieki cenšas sekmēt investīcijas un inovāciju MI jomā, tostarp uzlabojot juridisko noteiktību, kā arī Savienības tirgus konkurētspēju un izaugsmi, un sekmē globālās sadarbības standartizācijas jomā stiprināšanu un to, ka tiek ņemti vērā pastāvošie starptautiskie standarti MI jomā, kas atbilst Savienības vērtībām, pamattiesībām un interesēm, un stiprina daudzpusēju ieinteresēto personu pārvaldību, nodrošinot līdzsvarotu interešu pārstāvību un visu attiecīgo ieinteresēto personu efektīvu līdzdalību saskaņā ar Regulas (ES) Nr. 1025/2012 5., 6. un 7. pantu.

41. pants

Kopīgās specifikācijas

1. Komisija var pieņemt īstenošanas aktus, ar kuriem nosaka kopīgās specifikācijas šīs nodaļas 2. iedaļā noteiktajām prasībām vai – attiecīgā gadījumā – V nodaļas 2. un 3. iedaļā noteiktajiem pienākumiem, ja ir izpildīti šādi nosacījumi:

a) Komisija, ievērojot Regulas (ES) Nr. 1025/2012 10. panta 1. punktu, ir pieprasījusi vienai vai vairākām Eiropas standartizācijas organizācijām izstrādāt saskaņota standarta projektu attiecībā uz šīs nodaļas 2. iedaļā noteiktajām prasībām, vai attiecīgā gadījumā attiecībā uz V nodaļas 2. un 3. iedaļā noteiktajiem pienākumiem un:

i) pieprasījumu nav akceptējusi neviena Eiropas standartizācijas organizācija; vai

ii) saskaņotie standarti, reaģējot uz minēto pieprasījumu, nav iesniegti termiņā, kas noteikts saskaņā ar Regulas (ES) Nr. 1025/2012 10. panta 1. punktu; vai

iii) attiecīgie saskaņotie standarti nepietiekami risina problemātiskos pamattiesību jautājumus; vai

iv) saskaņotie standarti neatbilst pieprasījumam; un

b) *Eiropas Savienības Oficiālajā Vēstnesī* nav publicēta atsauce saskaņā ar Regulu (ES) Nr. 1025/2012 uz saskaņotiem standartiem, kuri attiecas uz šīs nodaļas 2. iedaļā minētajām prasībām, vai attiecīgā gadījumā uz V nodaļas 2. un 3. iedaļā minētajiem pienākumiem, un nav sagaidāms, ka šāda atsauce tiks publicēta saprātīgā laikposmā.

Izstrādājot kopīgās specifikācijas, Komisija apspriežas ar 67. pantā minēto konsultatīvo forumu.

Šā punkta pirmajā daļā minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

2. Pirms īstenošanas akta projekta sagatavošanas Komisija informē Regulas (ES) Nr. 1025/2012 22. pantā minēto komiteju, ka tās ieskatā šā panta 1. punkta nosacījumi ir izpildīti.

3. Pieņem, ka augsta riska MI sistēmas vai vispārīga lietojuma MI modeļi, kas atbilst 1. punktā minētajām kopīgajām specifikācijām vai minēto specifikāciju daļām, atbilst 2. iedaļā noteiktajām prasībām vai attiecīgā gadījumā atbilst V nodaļas 2. un 3. iedaļā minētajiem pienākumiem, ciktāl uz minētajām prasībām vai pienākumiem attiecas minētās kopīgās specifikācijas vai minētie pienākumi.

4. Ja saskaņotu standartu ir pieņēmusi kāda Eiropas standartizācijas organizācija, un Komisijai ir ierosināts atsauci uz to publicēt *Eiropas Savienības Oficiālajā Vēstnesī*, Komisija saskaņoto standartu novērtē saskaņā ar Regulu (ES) Nr. 1025/2012. Kad atsauci uz saskaņoto standartu publicē *Eiropas Savienības Oficiālajā Vēstnesī*, Komisija atceļ 1. punktā minētos īstenošanas aktus vai to daļas, kas attiecas uz tām pašām prasībām, kuras minētas šīs nodaļas 2. iedaļā vai attiecīgā gadījumā tiem pašiem pienākumiem, kas minēti V nodaļas 2. un 3. iedaļā.

5. Ja augsta riska MI sistēmu vai vispārīga lietojuma MI modeļu nodrošinātāji neatbilst 1. punktā minētajām kopīgajām specifikācijām, tie pienācīgi pamato, ka viņi ir pieņēmuši tehniskos risinājumus, kas atbilst šīs nodaļas 2. iedaļā minētajām prasībām vai attiecīgā gadījumā atbilst V nodaļas 2. un 3. iedaļā minētajiem pienākumiem vismaz tām līdzvērtīgā līmenī.

6. Ja dalībvalsts uzskata, ka kopīgā specifikācija pilnībā neatbilst 2. iedaļā noteiktajām prasībām vai attiecīgā gadījumā atbilst V nodaļas 2. un 3. iedaļā minētajiem pienākumiem, tā par to informē Komisiju, iesniedzot detalizētu skaidrojumu. Komisija minēto informāciju novērtē un attiecīgā gadījumā groza īstenošanas aktu, ar ko nosaka attiecīgo kopīgo specifikāciju.

42. pants

Pieņemums par atbilstību dažām prasībām

1. Uzskata, ka augsta riska MI sistēmas, kuras ir apmācītas un testētas ar datiem, kas atspoguļo konkrēto ģeogrāfisko, uzvedības, kontekstuālo vai funkcionālo vidi, kurā tās paredzēts lietot, atbilst attiecīgajām prasībām, kas noteiktas 10. panta 4. punktā.

2. Pieņem, ka augsta riska MI sistēmas, kuras ir sertificētas vai kurām saskaņā ar kiberdrošības shēmu ir izsniegts atbilstības apliecinājums, ievērojot Regulu (ES) 2019/881, un kuru atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, atbilst šīs regulas 15. pantā noteiktajām kiberdrošības prasībām, ciktāl uz minētajām prasībām attiecas kiberdrošības sertifikāts vai atbilstības apliecinājums vai tā daļas.

43. pants

Atbilstības novērtēšana

1. Attiecībā uz augsta riska MI sistēmām, kas uzskaitītas III pielikuma 1. punktā, ja nodrošinātājs, apliecinot augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām, ir piemērojis 40. pantā minētos saskaņotos standartus vai, attiecīgā gadījumā, 41. pantā minētās kopīgās specifikācijas, nodrošinātājs izvēlas vienu no šīm atbilstības novērtēšanas procedūrām, kas balstītas uz:

- a) VI pielikumā minēto iekšējo kontroli; vai
- b) VII pielikumā minēto kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtēšanu, iesaistot paziņoto struktūru.

Apliecinot augsta riska MI sistēmas atbilstību 2. iedaļā noteiktajām prasībām, nodrošinātājs ievēro VII pielikumā noteikto atbilstības novērtēšanas procedūru, ja:

- a) 40. pantā minētie saskaņotie standarti nepastāv un 41. pantā minētās kopīgās specifikācijas nav pieejamas;
- b) nodrošinātājs saskaņoto standartu nav piemērojis vai ir piemērojis tikai tā daļu;
- c) a) apakšpunktā minētās kopīgās specifikācijas pastāv, bet nodrošinātājs tās nav piemērojis;
- d) viens vai vairāki no a) apakšpunktā minētajiem saskaņotajiem standartiem ir publicēti ar ierobežojumu, un tikai attiecībā uz to standarta daļu, uz kuru attiecas ierobežojums.

VII pielikumā minētās atbilstības novērtēšanas procedūras nolūkos nodrošinātājs var izvēlēties jebkuru no paziņotajām struktūrām. Tomēr, ja augsta riska MI sistēmu paredzēts nodot ekspluatācijā tiesībaizsardzības, imigrācijas vai patvēruma iestādēm vai Savienības iestādēm, struktūrām, birojiem vai aģentūrām, kā paziņotā struktūra darbojas tirgus uzraudzības iestāde, kas minēta, attiecīgi, 74. panta 8. vai 9. punktā.

2. Attiecībā uz augsta riska MI sistēmām, kas minētas III pielikuma 2. līdz 8. punktā, nodrošinātāji ievēro VI pielikumā minēto atbilstības novērtēšanas procedūru uz iekšējās kontroles pamata, kas neparedz paziņotās struktūras iesaistīšanos.

3. Attiecībā uz augsta riska MI sistēmām, uz kurām attiecas I pielikuma A iedaļā uzskaitītie Savienības saskaņošanas tiesību akti, nodrošinātājs ievēro attiecīgu atbilstības novērtēšanas procedūru, kā prasīts minētajos tiesību aktos. Uz minētajām augsta riska MI sistēmām attiecas šīs nodaļas 2. iedaļā noteiktās prasības, un tās ir daļa no minētās novērtēšanas. Piemēro arī VII pielikuma 4.3., 4.4., 4.5. punktu un 4.6. punkta piekto daļu.

Paziņotajām struktūrām, kuras paziņotas, kā paredzēts minētajos tiesību aktos, tādas novērtēšanas nolūkos ir tiesības kontrolēt augsta riska MI sistēmu atbilstību 2. iedaļā noteiktajām prasībām, ar noteikumu, ka minēto paziņoto struktūru atbilstība prasībām, kuras noteiktas 31. panta 4., 5., 10. un 11. punktā, ir novērtēta saistībā ar paziņošanas procedūru, kas paredzēta minētajos tiesību aktos.

Ja tiesību akts, kas uzskaitīts I pielikuma A iedaļā, ļauj produkta ražotājam atteikties no trešās personas veiktas atbilstības novērtēšanas, ar noteikumu, ka šis ražotājs ir piemērojis visus saskaņotos standartus, kas aptver visas attiecīgās prasības, minētais ražotājs var izmantot šo iespēju tikai tad, ja tas ir piemērojis arī saskaņotos standartus vai, attiecīgā gadījumā, 41. pantā minētās kopīgās specifikācijas, kas attiecas uz šīs nodaļas 2. iedaļā noteiktajām prasībām.

4. Augsta riska MI sistēmas, kam jau ir veikta atbilstības novērtēšanas procedūra, pakļauj jaunai atbilstības novērtēšanas procedūrai būtiskas modifikācijas gadījumā neatkarīgi no tā, vai modificēto sistēmu paredzēts izplatīt tālāk jeb vai to turpinās lietot pašreizējais uzturētājs.

Attiecībā uz augsta riska MI sistēmām, kuras pēc laišanas tirgū vai nodošanas ekspluatācijā turpina mācīties, tādas izmaiņas augsta riska MI sistēmā un tās veiktspējā, ko sākotnējās atbilstības novērtēšanas brīdī ir iepriekš noteicis nodrošinātājs un kas ir norādītas informācijā, kura ietverta tehniskajā dokumentācijā, kas minēta IV pielikuma 2. punkta f) apakšpunktā, nav būtiskas modifikācijas.

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu VI un VII pielikumu, tos atjauninot, ņemot vērā tehnikas attīstību.

6. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu šā panta 1. un 2. punktu nolūkā uz III pielikuma 2. līdz 8. punktā minētajām augsta riska MI sistēmām attiecināt VII pielikumā minēto atbilstības novērtēšanas procedūru vai tās daļas. 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 aizsardzība, kā arī pienācīgu spēju un resursu pieejamība paziņoto struktūru starpā.

44. pants

Sertifikāti

1. Sertifikātus, ko saskaņā ar VII pielikumu izdod paziņotās struktūras, sagatavo valodā, kas ir viegli saprotama attiecīgajām iestādēm dalībvalstī, kurā ir izveidota paziņotā struktūra.

2. Sertifikāti ir derīgi tajos norādītajā laikposmā, kas nepārsniedz piecus gadus MI sistēmām, uz kurām attiecas I pielikums, un četrus gadus MI sistēmām, uz kurām attiecas III pielikums. Pēc nodrošinātāja pieteikuma sertifikāta derīgumu var pagarināt uz turpmākiem laikposmiem, kas katrs nepārsniedz piecus gadus MI sistēmām, uz kurām attiecas I pielikums, un četrus gadus MI sistēmām, uz kurām attiecas III pielikums, pamatojoties uz atkārtotu novērtēšanu saskaņā ar piemērojamām atbilstības novērtēšanas procedūrām. Jebkurš sertifikāta papildinājums ir joprojām derīgs ar noteikumu, ka derīgs ir sertifikāts, kuru tas papildina.

3. Ja paziņotā struktūra konstatē, ka MI sistēma vairs neatbilst 2. iedaļā noteiktajām prasībām, tā, ņemot vērā samērīguma principu, aptur vai atsauc izdoto sertifikātu vai uzliek tam ierobežojumus, ja vien atbilstība šīm prasībām nav nodrošināta ar pienācīgu korektīvu darbību, ko sistēmas nodrošinātājs veic paziņotās struktūras noteiktajā termiņā. Paziņotā struktūra savu lēmumu pamato.

Ir pieejama paziņoto struktūru lēmumu pārsūdzēšanas procedūra, tostarp par izdotiem atbilstības sertifikātiem.

45. pants

Paziņoto struktūru pienākumi informēt

1. Paziņotās struktūras informē paziņojošo iestādi par:

- a) katru Savienības tehniskās dokumentācijas novērtējuma sertifikātu, sertifikātu papildinājumiem un visiem kvalitātes vadības sistēmas apstiprinājumiem, kas izsniegti saskaņā ar VII pielikuma prasībām;
- b) katru atteikumu, ierobežojumu, apturēšanu vai atsaukšanu, kas attiecas uz Savienības tehniskās dokumentācijas novērtējuma sertifikātu vai kvalitātes vadības sistēmas apstiprinājumu, kas izdots saskaņā ar VII pielikuma prasībām;
- c) apstākļiem, kas ietekmē paziņojuma 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 paziņotas, un visām citām darbībām, tostarp pārrobežu darbībām un apakšuzņēmuma līgumu slēgšanu (pēc pieprasījuma).

2. Katra paziņotā struktūra informē pārējās paziņotās struktūras par:

- a) kvalitātes vadības sistēmas apstiprinājumiem, kurus tā ir atteikusi, apturējusi vai atsaukusi, un pēc pieprasījuma arī par kvalitātes sistēmas apstiprinājumiem, kurus tā ir izdevusi;
- b) Savienības tehniskās dokumentācijas novērtējuma sertifikātiem vai to papildinājumiem, kurus tā ir atteikusi, atsaukusi, apturējusi vai kā citādi ierobežojusi, un pēc pieprasījuma arī par tās izsniegtiem sertifikātiem un/vai to papildinājumiem.

3. Katra paziņotā struktūra sniedz pārējām paziņotajām struktūrām, kas veic līdzīgas atbilstības novērtēšanas darbības, kuras attiecas uz to pašu veidu MI sistēmām, attiecīgu informāciju par jautājumiem, kas saistīti ar negatīviem un pēc pieprasījuma – pozitīviem atbilstības novērtēšanas rezultātiem.
4. Paziņojošās iestādes nodrošina to iegūtās informācijas konfidencialitāti saskaņā ar 78. pantu.

46. pants

Atkāpe no atbilstības novērtēšanas procedūras

1. Atkāpjoties no 43. panta un pēc pienācīgi pamatota pieprasījuma tirgus uzraudzības iestāde var atļaut konkrētu augsta riska MI sistēmu laišanu tirgū vai nodošanu ekspluatācijā attiecīgās dalībvalsts teritorijā ārkārtēju sabiedriskās drošības iemeslu dēļ vai personu dzīvības un veselības aizsardzības, vides aizsardzības vai svarīgu rūpniecības un infrastruktūras aktīvu aizsardzības iemeslu dēļ. Minētā atļauja ir uz ierobežotu laikposmu, kamēr tiek veiktas nepieciešamās atbilstības novērtēšanas procedūras, ņemot vērā ārkārtējos apstākļus, kas pamato atkāpi. Šīs procedūras pabeidz bez liekas kavēšanās.
2. Pienācīgi pamatotā steidzamā situācijā ārkārtēju sabiedriskās drošības iemeslu dēļ vai konkrēta, būtiska un nenovēršama apdraudējuma fizisku personu dzīvībai vai fiziskai drošībai gadījumā tiesībaizsardzības iestādes vai civilās aizsardzības iestādes var nodot ekspluatācijā konkrētu augsta riska MI sistēmu bez 1. punktā minētās atļaujas ar noteikumu, ka šāda atļauja bez liekas kavēšanās tiek pieprasīta lietošanas laikā vai pēc tās. Ja 1. punktā minētā atļauja tiek atteikta, šādas augsta riska MI sistēmas lietošanu nekavējoties aptur un visus šādas lietošanas rezultātus un iznākumus nekavējoties atmet.
3. Atļauju, kas minēta 1. punktā, izsniedz tikai tad, ja tirgus uzraudzības iestāde secina, ka augsta riska MI sistēma atbilst 2. iedaļas prasībām. Par visām atļaujām, kas izsniegtas, ievērojot 1. un 2. punktu, tirgus uzraudzības iestāde nekavējoties informē Komisiju un pārējās dalībvalstis. Šis pienākums neattiecas uz sensitīviem operatīvajiem datiem saistībā ar tiesībaizsardzības iestāžu darbībām.
4. Ja 15 kalendāro dienu laikā pēc 3. 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.
5. Ja 15 kalendāro dienu laikā pēc 3. punktā minētā paziņojuma saņemšanas kāda dalībvalsts ceļ iebildumus pret citas dalībvalsts tirgus uzraudzības iestādes izdoto atļauju vai Komisija uzskata, ka atļauja ir pretrunā Savienības tiesību aktiem vai 3. punktā minētais dalībvalstu secinājums par attiecīgās sistēmas atbilstību nav pamatots, Komisija nekavējoties sāk apspriešanos ar attiecīgo dalībvalsti. Notiek apspriešanās ar attiecīgajiem operatoriem, un viņiem ir iespēja izklāstīt savu viedokli. To ņemot vērā, Komisija lemj, vai atļauja ir pamatota. Komisija savu lēmumu adresē attiecīgajai dalībvalstij un attiecīgiem operatoriem.
6. Ja Komisija atļauju uzskata par nepamatotu, attiecīgās dalībvalsts tirgus uzraudzības iestāde to atsauc.
7. Augsta riska MI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas I pielikuma A iedaļā minētie Savienības saskaņošanas tiesību akti, piemēro tikai minētajos Savienības saskaņošanas tiesību aktos noteiktās atkāpes no atbilstības novērtēšanas.

47. pants

ES atbilstības deklarācija

1. Nodrošinātājs sagatavo rakstisku, mašīnlasāmu, fiziski vai elektroniski parakstītu ES atbilstības deklarāciju katrai augsta riska MI sistēmai un glabā to valsts kompetentajām iestādēm pieejamu 10 gadus pēc augsta riska MI sistēmas laišanas tirgū vai nodošanas ekspluatācijā. ES atbilstības deklarācijā norāda tās augsta riska MI sistēmas identitāti, kurai deklarācija ir sagatavota. ES atbilstības deklarācijas kopiju pēc pieprasījuma iesniedz attiecīgajām valsts kompetentajām iestādēm.

2. ES atbilstības deklarācijā norāda, ka attiecīgā augsta riska MI sistēma atbilst 2. iedaļā noteiktajām prasībām. ES atbilstības deklarācijā iekļauj V pielikumā noteikto informāciju, un to tulko valodā, kura ir viegli saprotama valsts kompetentajām iestādēm dalībvalstīs, kurās attiecīgā augsta riska MI sistēma ir laista tirgū vai darīta pieejama.
3. Ja uz augsta riska MI sistēmām attiecas citi Savienības saskaņošanas tiesību akti, kuriem arī vajadzīga ES atbilstības deklarācija, par visiem Savienības tiesību aktiem, kas piemērojami augsta riska MI 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, nodrošinātājs uzņemas atbildību par atbilstību 2. iedaļā noteiktajām prasībām. Vajadzības gadījumā nodrošinātājs ES atbilstības deklarāciju regulāri atjaunina.
5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai atjauninātu V pielikumā noteiktās ES atbilstības deklarācijas saturu ar mērķi ieviest elementus, kas kļūst nepieciešami, ņemot vērā tehnikas attīstību.

48. pants

CE zīme

1. Uz CE zīmi attiecas vispārīgie principi, kas paredzēti Regulas (EK) Nr. 765/2008 30. pantā.
2. Digitāli nodrošinātām augsta riska MI sistēmām digitālu CE zīmi izmanto tikai tad, ja tai var viegli piekļūt, izmantojot minētās sistēmas piekļuves saskarni vai viegli pieejamu mašīnlasāmu kodu, vai citus elektroniskus līdzekļus.
3. CE zīmi augsta riska MI sistēmām uzliek tā, lai tā būtu redzama, salasāma un neizdzēšama. Ja augsta riska MI sistēmas specifika dēļ tas nav iespējams vai netiek prasīts, zīmi uzliek uz iepakojuma vai, attiecīgā gadījumā, uz pievienotās dokumentācijas.
4. Attiecīgā gadījumā CE zīmei seko tās paziņotās struktūras identifikācijas numurs, kura ir atbildīga par 43. pantā noteikto atbilstības novērtēšanas procedūru. Paziņotās struktūras identifikācijas numuru uzliek pati struktūra, vai arī pēc tās norādījumiem to uzliek nodrošinātājs vai nodrošinātāja pilnvarotais pārstāvis. Identifikācijas numuru norāda arī visos reklāmas materiālos, kuros minēts, ka augsta riska MI sistēma atbilst CE zīmes prasībām.
5. Ja augsta riska MI sistēmas reglamentē arī citi Savienības tiesību akti, kas arī paredz CE zīmes uzlikšanu, CE zīme norāda, ka šī augsta riska MI sistēma atbilst arī šo citu tiesību aktu prasībām.

49. pants

Reģistrācija

1. Pirms tiek laista tirgū vai nodota ekspluatācijā augsta riska MI sistēma, kas uzskaitīta III pielikumā, izņemot augsta riska MI sistēmas, kas minētas III pielikuma 2. punktā, nodrošinātājs vai, attiecīgā gadījumā, pilnvarotais pārstāvis reģistrējas pats un reģistrē savu sistēmu 71. pantā minētajā ES datubāzē.
2. Pirms tiek laista tirgū vai nodota ekspluatācijā MI sistēma, par kuru nodrošinātājs saskaņā ar 6. panta 3. punktu ir secinājis, ka tā nav augsta riska MI sistēma, minētais nodrošinātājs vai, attiecīgā gadījumā, pilnvarotais pārstāvis reģistrējas pats un reģistrē savu sistēmu 71. pantā minētajā ES datubāzē.
3. Pirms tiek nodota ekspluatācijā vai lietota augsta riska MI sistēma, kas uzskaitīta III pielikumā, izņemot augsta riska MI sistēmas, kas uzskaitītas III pielikuma 2. punktā, uzturētāji, kas ir publiskas iestādes, Savienības iestādes, struktūras, biroji vai aģentūras vai personas, kas rīkojas to vārdā, reģistrējas, atlasa sistēmu un reģistrē tās lietošanu 71. pantā minētajā ES datubāzē.

4. Attiecībā uz augsta riska MI sistēmām, kas minētas III pielikuma 1., 6. un 7. punktā, tiesībaizsardzības, migrācijas, patvēruma un robežkontroles jomās šā panta 1., 2. un 3. punktā minēto reģistrāciju veic ES datubāzes drošā, publiski nepieejamā sadaļā, kas minēta 71. pantā, un attiecīgi iekļauj tikai šādu informāciju, kas minēta:

- a) VIII pielikuma A iedaļas 1. līdz 10. punktā, izņemot 6., 8. un 9. punktu;
- b) VIII pielikuma B iedaļas 1. līdz 5. punktu un 8. un 9. punktu;
- c) VIII pielikuma C iedaļas 1. līdz 3. punktu;
- d) IX pielikuma 1., 2., 3. un 5. punktu.

Vienīgi Komisijai un 74. panta 8. punktā minētajām valsts iestādēm ir piekļuve šā punkta pirmajā daļā uzskaitītajām attiecīgajām ES datubāzes ierobežotas piekļuves sadaļām.

- 5. III pielikuma 2. punktā minētās augsta riska MI sistēmas reģistrē valsts līmenī.

IV NODAĻA

DAŽU MI SISTĒMU NODROŠINĀTĀJU UN UZTURĒTĀJU PIENĀKUMI ATTIECĪBĀ UZ PĀRREDZAMĪBU

50. pants

Dažu MI sistēmu nodrošinātāju un uzturētāju pienākums nodrošināt pārredzamību

1. Nodrošinātāji nodrošina, ka MI sistēmas, kas paredzētas tiešai mijiedarbībai ar fiziskām personām, projektē un izstrādā tā, lai attiecīgās fiziskās personas tiktu informētas par to, ka tās mijiedarbojas ar MI sistēmu, ja vien tas nav pašsaprotams no tādas fiziskas personas viedokļa, kura ir samērā labi informēta, vērota un apdomīga, ņemot vērā apstākļus un lietošanas kontekstu. Šis pienākums neattiecas uz MI sistēmām, kuras ir likumiski atļautas noziedzīgu nodarījumu atklāšanai, novēršanai, izmeklēšanai vai kriminālvajāšanai, ievērojot atbilstošus trešo personu tiesību un brīvību aizsardzības pasākumus, ja vien minētās sistēmas nav pieejamas sabiedrībai ziņošanai par noziedzīgu nodarījumu.

2. MI sistēmu, tostarp vispārīga lietojuma MI sistēmu, kuras ģenerē sintētisku audio, attēla, video vai teksta saturu, nodrošinātāji nodrošina, ka MI sistēmas iznākumi ir mašīnlasāmā formātā un ir iespējams atklāt, ka tie ir mākslīgi ģenerēti vai manipulēti. Nodrošinātāji nodrošina, ka viņu tehniskie risinājumi ir efektīvi, sadarbībspēji, robusti un uzticami, ciktāl tas ir tehniski iespējams, ņemot vērā dažādo satura veidu specifiku un ierobežojumus, īstenošanas izmaksas un vispārējā jaunākos sasniegumus, kā tas var būt atspoguļots attiecīgajos tehniskajos standartos. Šo pienākumu nepiemēro, ciktāl MI sistēma pilda palīgfunkciju standarta rediģēšanai vai būtiski nemaina uzturētāja sniegtos ievaddatus vai to semantiku, vai ja tā ir likumiski atļauta noziedzīgu nodarījumu atklāšanai, novēršanai, izmeklēšanai vai kriminālvajāšanai.

3. Emociju atpazīšanas sistēmas vai biometriskās kategorizācijas sistēmas uzturētāji informē par sistēmas darbību fiziskas personas, uz kurām tā attiecas, un personas datus apstrādā saskaņā ar, attiecīgi, Regulām (ES) 2016/679 un (ES) 2018/1725 un Direktīvu (ES) 2016/680. Šis pienākums neattiecas uz biometriskai kategorizācijai un emociju atpazīšanai izmantotām MI sistēmām, kuras ir likumiski atļautas, lai atklātu, novērstu vai izmeklētu noziedzīgus nodarījumus, ievērojot atbilstošus trešo personu tiesību un brīvību aizsardzības pasākumus un saskaņā ar Savienības tiesību aktiem.

4. Tādas MI sistēmas uzturētāji, kura ģenerē vai manipulē attēla, audio vai video saturu, kas ir dziļviltojums, izpauž, ka saturs ir mākslīgi ģenerēts vai manipulēts. Šo pienākumu nepiemēro, ja lietošana ir likumiski atļauta noziedzīga nodarījuma atklāšanai, novēršanai, izmeklēšanai vai kriminālvajāšanai. Ja saturs ir daļa no acīmredzami mākslinieciska, radoša, satīriskā, fikcionāla vai analoga darba vai programmas, šajā punktā paredzētie pārredzamības pienākumi ietver vienīgi šāda ģenerēta vai manipulēta satura esamības izpaušanu piemērotā veidā, kas netraucē izrādīt vai baudīt darbu.

Tādas MI sistēmas uzturētāji, kura ģenerē vai manipulē tekstu, ko publicē nolūkā informēt sabiedrību par sabiedrības interešu jautājumiem, izpauž, ka teksts ir mākslīgi ģenerēts vai manipulēts. Šo pienākumu nepiemēro, ja lietošana ir likumiski atļauta noziedzīga nodarījuma atklāšanai, novēršanai, izmeklēšanai vai kriminālvajāšanai vai ja MI ģenerētu saturu ir pārskatījis cilvēks vai tam ir veikta redakcionāla kontrole un ja fiziska vai juridiska persona ir redakcionāli atbildīga par satura publikāciju.

5. Šā panta 1. līdz 4. punktā minēto informāciju attiecīgām fiziskām personām sniedz skaidrā un atšķiramā veidā, vēlākais, pirmās mijiedarbības vai eksponēšanas laikā. Informācija atbilst piemērojamām pieklūstamības prasībām.

6. Šā panta 1. līdz 4. punkts neietekmē III nodaļā noteiktās prasības un pienākumus un neskar citus Savienības vai valsts tiesību aktos noteiktus MI sistēmu uzturētāju pienākumus attiecībā uz pārredzamību.

7. MI birojs rosina un sekmē prakses kodeksu izstrādi Savienības līmenī, lai sekmētu ar mākslīgi ģenerēta vai manipulēta satura atklāšanu un marķēšanu saistītu pienākumu efektīvu īstenošanu. Komisija var pieņemt īstenošanas aktus, lai apstiprinātu minētos prakses kodeksus saskaņā ar 56. panta 6. punktā noteikto procedūru. Ja tā uzskata, ka kodekss nav atbilstīgs, Komisija var pieņemt īstenošanas aktu, ar ko nosaka kopīgus noteikumus minēto pienākumu īstenošanai saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

V NODAĻA

VISPĀRĪGA LIETOJUMA MI MODEĻI

1. IEDAĻA

Klasificēšanas noteikumi

51. pants

Vispārīga lietojuma MI modeļu klasificēšana par vispārīga lietojuma MI modeļiem ar sistēmisku risku

1. Vispārīga lietojuma MI modeli klasificē par vispārīga lietojuma MI modeli ar sistēmisku risku, ja tas atbilst kādai no šādiem nosacījumiem:

- a) tam ir augstas ietekmes spējas, kas novērtētas, pamatojoties uz piemērotiem tehniskiem rīkiem un metodikām, tostarp rādītājiem un kritērijiem;
- b) pamatojoties uz Komisijas lēmumu, *ex officio* vai pēc zinātniskās grupas kvalificēta brīdinājuma tam ir spējas vai ietekme, kas ir līdzvērtīga a) punktā noteiktajām, ņemot vērā XIII pielikumā noteiktos kritērijus.

2. Tiek pieņemts, ka vispārīga lietojuma MI modelim ir augstas ietekmes spējas saskaņā ar 1. punkta a) apakšpunktu, ja kumulatīvais tā apmācībai izmantotais skaitļošanas apjoms, mērīts peldošā komata operācijā, ir lielāks nekā 10^{25} .

3. Komisija pieņem deleģētos aktus saskaņā ar 97. pantu, lai grozītu šā panta 1. un 2. punktā uzskaitītās maksimālās vērtības, kā arī lai nepieciešamības gadījumā papildinātu kritērijus un rādītājus, ņemot vērā tehnoloģiju attīstību, piemēram, algoritmiskos uzlabojumus vai lielāku aparatūras efektivitāti, lai šīs robežvērtības atspoguļotu jaunākos sasniegumus.

52. pants

Procedūra

1. Ja vispārīga lietojuma MI modelis atbilst 51. panta 1. punkta a) apakšpunktā minētajam nosacījumam attiecīgais nodrošinātājs paziņo Komisijai nekavējoties un jebkurā gadījumā divu nedēļu laikā pēc tam, kad minētā prasība ir izpildīta vai kļūst zināms, ka tā tiks izpildīts. Minētajā paziņojumā iekļauj informāciju, kas nepieciešama, lai apliecinātu, ka attiecīgā prasība ir izpildīta. Ja Komisijai kļūst zināms par vispārīga lietojuma MI modeli, kas rada sistēmiskus riskus, par kuru tai nav paziņots, tā var nolemt to atzīt par modeli ar sistēmisku risku.

2. Tāda vispārīga lietojuma MI modeļa nodrošinātājs, kurš atbilst 51. panta 1. punkta a) apakšpunktā minētajiem nosacījumiem, var līdz ar paziņojumu iesniegt pietiekami pamatotus argumentus, lai apliecinātu, ka izņēmuma kārtā, lai arī tas atbilst minētajai prasībai, vispārīga lietojuma MI modelis savas konkrētās specifikas dēļ nerada sistēmiskus riskus un tādēļ nebūtu jākvalificē kā vispārīga lietojuma MI modelis ar sistēmisku risku.

3. Ja Komisija secina, ka argumenti, kas iesniegti, ievērojot 2. punktu, nav pietiekami pamatoti un attiecīgais nodrošinātājs nav spējis apliecināt, ka vispārīga lietojuma MI modelis savas konkrētās specifikas dēļ nerada sistēmiskus riskus, tā noraida minētos argumentus, un vispārīga lietojuma MI modeli uzskata par vispārīga lietojuma MI modeli ar sistēmisku risku.

4. Komisija var atzīt, ka vispārīga lietojuma MI modelis rada sistēmiskus riskus, *ex officio* vai pēc zinātniskās grupas kvalificēta brīdinājuma, ievērojot 90. panta 1. punkta a) apakšpunktu, balstoties uz kritērijiem, kas noteikti XIII pielikumā.

Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai grozītu XIII pielikumu, precizējot un atjauninot minētajā pielikumā noteiktos kritērijus.

5. Pēc nodrošinātāja, kura modelis, ievērojot 4. punktu, ir atzīts par vispārīga lietojuma MI modeli ar sistēmisku risku, pamatota pieprasījuma Komisija pieprasījumu ņem vērā un var lemt atkārtoti vērtēt, vai, pamatojoties uz XIII pielikumā noteiktajiem kritērijiem, joprojām var uzskatīt, ka vispārīga lietojuma MI modelis rada sistēmiskus riskus. Šādā pieprasījumā ietver objektīvus, detalizētus un jaunus iemeslus, kas radušies pēc lēmuma par atzīšanu. Nodrošinātāji var pieprasīt atkārtotu novērtēšanu agrākais sešus mēnešus pēc lēmuma par atzīšanu. Ja Komisija pēc atkārtotās novērtēšanas nolemj saglabāt atzīšanu par vispārīga lietojuma MI modeli ar sistēmisku risku, nodrošinātāji var pieprasīt atkārtotu novērtēšanu agrākais sešus mēnešus pēc minētā lēmuma.

6. Komisija nodrošina, ka tiek publicēts vispārīga lietojuma MI modeļu ar sistēmisku risku saraksts, un pastāvīgi atjaunina minēto sarakstu, neskarot nepieciešamību ievērot un aizsargāt intelektuālā īpašuma tiesības un konfidencialu uzņēmējdarbības informāciju vai komercnoslēpumus saskaņā ar Savienības un valsts tiesību aktiem.

2. IEDAĻA

Vispārīga lietojuma MI modeļu nodrošinātāju pienākumi

53. pants

Vispārīga lietojuma MI modeļu nodrošinātāju pienākumi

1. Vispārīga lietojuma MI modeļu nodrošinātāji:

a) sastāda un pastāvīgi atjaunina modeļa tehnisko dokumentāciju, iekļaujot tā apmācības un testēšanas procesu un tā izvērtēšanas rezultātus, kas ietver vismaz XI pielikumā paredzēto informāciju, lai to pēc pieprasījuma iesniegtu MI birojam un valsts kompetentajām iestādēm;

b) sastāda, pastāvīgi atjaunina un dara pieejamu informāciju un dokumentāciju MI sistēmu nodrošinātājiem, kuri ir iecerējuši integrēt konkrēto vispārīga lietojuma MI modeli savās MI sistēmās. Neskarot nepieciešamību ievērot un aizsargāt intelektuālā īpašuma tiesības un konfidencialu uzņēmējdarbības informāciju vai komercnoslēpumus saskaņā ar Savienības un valsts tiesību aktiem, informācija un dokumentācija

i) dod MI sistēmu nodrošinātājiem iespēju labi izprast konkrētā vispārīga lietojuma MI modeļa spējas un ierobežojumus un izpildīt savus pienākumus, ievērojot šo regulu; un

ii) ietver vismaz XII pielikumā izklāstītos elementus;

c) ievieš politiku, lai panāktu atbilstību Savienības tiesību aktiem autortiesību un blakustiesību jomā un jo īpaši lai identificētu un pildītu, tostarp ar modernām tehnoloģijām, tiesību rezervāciju, kas pausta, ievērojot Direktīvas (ES) 2019/790 4. panta 3. punktu;

d) saskaņā ar MI biroja nodrošināto veidni sagatavo un publisko pietiekami detalizētu kopsavilkumu par vispārīga lietojuma MI modeļa apmācībā izmantoto saturu.

2. Šā panta 1. punkta a) un b) apakšpunktā paredzētos pienākumus nepiemēro to MI modeļu nodrošinātājiem, kuri ir laisti apgrozībā ar bezmaksas un atvērtas piekļuves licenci, kura ļauj modeļim piekļūt, to lietot, modificēt un izplatīt, un kuru parametri, tostarp svāri, informācija par modeļa arhitektūru un informācija par modeļa lietošanu, ir darīti publiski pieejami. Šo izņēmumu nepiemēro vispārīga lietojuma MI modeļiem ar sistēmiskiem riskiem.
3. Vispārīga lietojuma MI modeļu nodrošinātāji savas kompetences un pilnvaru īstenošanā, ievērojot šo regulu, vajadzības gadījumā sadarbojas ar Komisiju un valsts kompetentajām iestādēm.
4. Vispārīga lietojuma MI modeļu nodrošinātāji var palauties uz prakses kodeksiem 56. panta nozīmē, lai apliecinātu šā panta 1. punktā noteikto pienākumu ievērošanu, līdz laikam, kamēr tiek publicēts saskaņots standarts. Atbilstība Eiropas saskaņotajiem standartiem sniedz nodrošinātājiem atbilstības prezumpciju, ciktāl minētie standarti attiecas uz minētajiem pienākumiem. Vispārīga lietojuma MI modeļu nodrošinātāji, kas neievēro apstiprinātu prakses kodeksu vai neatbilst Eiropas saskaņotajam standartam, apliecina alternatīvus pienācīgus atbilstības nodrošināšanas līdzekļus, lai saņemtu Komisijas apstiprinājumu.
5. Lai veicinātu atbilstību XI pielikumam, jo īpaši tā 2. punkta d) un e) apakšpunktam, Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. pantu, lai sīki izklāstītu mērījumu un aprēķinu metodiku nolūkā panākt salīdzināmu un pārbaudāmu dokumentāciju.
6. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 97. panta 2. punktu, lai grozītu XI un XII pielikumu, ņemot vērā tehnoloģijas attīstību.
7. Ar informāciju vai dokumentāciju, kas iegūta, ievērojot šā panta noteikumus, tostarp komercnoslēpumiem, rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.

54. pants

Vispārīga lietojuma MI modeļu nodrošinātāju pilnvarotie pārstāvji

1. Nodrošinātāji, kas iedibināti trešās valstīs, pirms vispārīga lietojuma MI modeli dara pieejamu Savienības tirgū, ar rakstisku pilnvaru ieceļ pilnvarotu pārstāvi, kurš iedibināts Savienībā.
2. Nodrošinātājs ļauj savam pilnvarotajam pārstāvim pildīt uzdevumus, kas norādīti no nodrošinātāja saņemtajā pilnvarojumā.
3. Pilnvarotais pārstāvis veic uzdevumus, kas norādīti no nodrošinātāja saņemtajā pilnvarojumā. Tas pēc pieprasījuma iesniedz MI birojam pilnvarojuma kopiju kādā no Savienības iestāžu oficiālajām valodām. Šīs regulas nolūkos pilnvarojums dod pilnvarotajam pārstāvim tiesības veikt šādus uzdevumus:
 - a) pārliecināties, ka nodrošinātājs ir sagatavojis XI pielikumā norādīto tehnisko dokumentāciju un izpildījis visus pienākumus, kas minēti 53. pantā un, attiecīgā gadījumā, 55. pantā;
 - b) glabāt MI birojam un valsts kompetentajām iestādēm pieejamu XI pielikumā norādītās tehniskās dokumentācijas kopiju 10 gadus pēc vispārīga lietojuma MI modeļa laišanas tirgū un pastāvīgi atjaunināt tā nodrošinātāja kontaktinformāciju, kurš ir iecēlis pilnvaroto pārstāvi;
 - c) pēc pamatota pieprasījuma sniegt MI birojam visu informāciju un dokumentāciju, tostarp b) apakšpunktā minēto, kura ir nepieciešama, lai apliecinātu šīs nodaļas pienākumu izpildi;
 - d) pēc pamatota pieprasījuma sadarboties ar MI biroju un ar kompetentajām iestādēm visās darbībās, ko tās veic saistībā ar vispārīga lietojuma MI modeli, tostarp, ja modelis ir integrēts MI sistēmās, kuras ir laistas tirgū vai nodotas ekspluatācijā Savienībā.
4. Pilnvarojums ļauj MI birojam vai kompetentajām iestādēm visos jautājumos, kas saistīti ar atbilstības nodrošināšanu šai regulai, vērsties pie pilnvarotā pārstāvja, nevis pie nodrošinātāja, vai papildus nodrošinātājam.

5. Pilnvarotais pārstāvis izbeidz pilnvarojumu, ja tas uzskata vai tam ir pamats uzskatīt, ka nodrošinātājs rīkojas pretēji saviem pienākumiem, kas noteikti šajā regulā. Šādā gadījumā tas arī nekavējoties informē MI biroju par pilnvarojuma izbeigšanu un tās iemesliem.

6. Šajā pantā paredzēto pienākumu nepiemēro to vispārīga lietojuma MI modeļu nodrošinātājiem, kuri ir laisti apgrozībā ar bezmaksas un atvērta pirmkoda licenci, kas ļauj modeļiem piekļūt, to lietot, modificēt un izplatīt, un kuru parametri, tostarp svāri, informācija par modeļa arhitektūru un informācija par modeļa lietošanu, ir darīti publiski pieejami, ja vien vispārīga lietojuma MI modeļi nerada sistēmiskus riskus.

3. IEDAĻA

Vispārīga lietojuma MI modeļu ar sistēmisku risku nodrošinātāju pienākumi

55. pants

Vispārīga lietojuma MI modeļu ar sistēmisku risku nodrošinātāju pienākumi

1. Papildus 53. un 54. pantā uzskaitītajiem pienākumiem vispārīga lietojuma MI modeļu ar sistēmisku risku nodrošinātāji:

- a) veic modeļa izvērtēšanu saskaņā ar standartizētiem protokoliem un rīkiem, kas atspoguļo jaunākos sasniegumus, tostarp veicot un dokumentējot modeļa pretestības testēšanu nolūkā identificēt un mazināt sistēmiskus riskus;
- b) novērtē un mazina iespējamās sistēmiskās riskus Savienības līmenī, tostarp to avotus, kas var izrietēt no vispārīga lietojuma MI modeļu ar sistēmisku risku izstrādes, laišanas tirgū vai lietošanas;
- c) uzskaita, dokumentē un bez liekas kavēšanās ziņo MI birojam un, attiecīgā gadījumā, valsts kompetentajām iestādēm attiecīgo informāciju par nopietniem incidentiem un iespējamām korektīviem pasākumiem, ar ko tos risināt;
- d) nodrošina pienācīga līmeņa kibernetiskās aizsardzību vispārīga lietojuma MI modeļiem ar sistēmisku risku un modeļa fiziskajai infrastruktūrai.

2. Vispārīga lietojuma MI modeļu ar sistēmisku risku nodrošinātāji var paļauties uz prakses kodeksiem 56. panta nozīmē, lai apliecinātu šā panta 1. punktā noteikto pienākumu pildīšanu, līdz laikam, kamēr tiek publicēts saskaņots standarts. Atbilstība Eiropas saskaņotajiem standartiem sniedz nodrošinātājiem atbilstības prezumpciju, ciktāl minētie standarti attiecas uz minētajiem pienākumiem. Vispārīga lietojuma MI modeļu ar sistēmiskiem riskiem nodrošinātāji, kas neievēro apstiprinātu prakses kodeksu vai neatbilst Eiropas saskaņotajam standartam, apliecina alternatīvus pienācīgus atbilstības nodrošināšanas līdzekļus, lai saņemtu Komisijas novērtējumu.

3. Ar informāciju vai dokumentāciju, kas iegūta, ievērojot šo pantu, tostarp komercnoslēpumiem, rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.

4. IEDAĻA

Prakses kodeksi

56. pants

Prakses kodeksi

1. MI birojs rosina un sekmē prakses kodeksu izstrādi Savienības līmenī, lai veicinātu šīs regulas pareizu piemērošanu, ņemot vērā starptautiskās pieejas.

2. MI birojs un MI padome tiecas nodrošināt, ka prakses kodeksi aptver vismaz 53. un 55. pantā paredzētos pienākumus, tostarp šādus jautājumus:

- a) līdzekļi, ar ko nodrošināt, ka 53. panta 1. punkta a) un b) apakšpunktā minētā informācija tiek pastāvīgi atjaunināta, ņemot vērā tirgus un tehnoloģiju attīstību;
- b) pienācīga detalizācijas pakāpe kopsavilkumam par apmācībā izmantoto saturu;
- c) sistēmisko risku veida un rakstura identifikācija Savienības līmenī, tostarp, attiecīgā gadījumā, to avotu identifikācija;
- d) pasākumi, procedūras un kārtība sistēmisko risku novērtēšanai un pārvaldībai Savienības līmenī, tostarp to dokumentācija, kas ir samērīgi ar riskiem, apsver to smagumu un iespējamību un ņem vērā konkrētos izaicinājumus rīcībā ar minētajiem riskiem saistībā ar to, kādos veidos šādi riski varētu rasties un materializēties MI vērtības ķēdē.

3. MI birojs var prakses kodeksu izstrādē uzaicināt piedalīties visus vispārīga lietojuma MI modeļu nodrošinātājus, kā arī attiecīgās valstu kompetentās iestādes. Procesu var atbalstīt pilsoniskās sabiedrības organizācijas, nozare, akadēmiskās aprindas un citas ieinteresētās personas, piemēram, lejasposma nodrošinātāji un neatkarīgi eksperti.

4. MI birojs un MI padome tiecas nodrošināt, ka prakses kodeksos ir skaidri izklāstīti to konkrētie mērķi un ir ietvertas saistības vai pasākumi, tostarp, attiecīgā gadījumā, galvenie snieguma rādītāji, lai nodrošinātu minēto mērķu sasniegšanu un lai Savienības līmenī pienācīgi ņemtu vērā visu ieinteresēto personu, tostarp skarto personu, vajadzības un intereses.

5. MI birojs tiecas nodrošināt, ka prakses kodeksu dalībnieki regulāri ziņo MI birojam par saistību īstenošanu un veiktajiem pasākumiem un to rezultātiem, tostarp, attiecīgā gadījumā, tos mērojot ar galvenajiem snieguma rādītājiem. Galvenajos snieguma rādītājos un ziņošanas saistībās atspoguļo lieluma un spēju atšķirības starp dažādiem dalībniekiem.

6. MI birojs un MI padome regulāri uzrauga un izvērtē to, kā dalībnieki sasniedz prakses kodeksu mērķus, un to ieguldījumu šīs regulas pareizā piemērošanā. MI birojs un MI padome novērtē, vai prakses kodeksi aptver 53. un 55. pantā paredzētos pienākumus, un regulāri uzrauga un izvērtē to mērķu sasniegšanu. Tie publicē prakses kodeksu piemērotības novērtējumu.

Komisija var ar īstenošanas aktu apstiprināt prakses kodeksu un piešķirt tam vispārēju spēkā esību Savienībā. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

7. MI birojs var uzaicināt visus vispārīga lietojuma MI modeļu nodrošinātājus ievērot prakses kodeksus. Attiecībā uz to vispārīga lietojuma MI modeļu nodrošinātājiem, kuri nerada sistēmiskus riskus, šāda ievērošana būtu jāattiecina vienīgi uz 53. pantā paredzētajiem pienākumiem, ja vien viņi nepārprotami nepauz interesi pievienoties pilnajam kodeksam.

8. MI birojs attiecīgā gadījumā arī rosina un sekmē prakses kodeksu pārskatīšanu un pielāgošanu, jo īpaši, ņemot vērā jaunpienākušos standartus. MI birojs palīdz pieejamo standartu novērtēšanā.

9. Prakses kodeksi ir gatavi vēlākais līdz 2025. gada 2. maijam. MI birojs veic vajadzīgos pasākumus, tostarp uzaicina nodrošinātājus, ievērojot 7. punktu.

Ja līdz 2025. gada 2. augustam prakses kodeksu nevar pabeigt vai ja MI birojs pēc šā panta 6. punktā paredzētās novērtēšanas uzskata, ka tas nav piemērots, Komisija var ar īstenošanas aktiem sniegt kopīgus noteikumus 53. un 55. pantā paredzēto pienākumu, tostarp šā panta 2. punktā izklāstīto jautājumu, īstenošanai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

VI NODAĻA
INOVĀCIJAS ATBALSTA PASĀKUMI

57. pants

MI “regulatīvās smilškastēs”

1. Dalībvalstis nodrošina, ka to kompetentās iestādes izveido vismaz vienu MI “regulatīvo smilškastī” valsts līmenī, kura sāk darboties līdz 2026. gada 2. augustam. Minēto “smilškastī” var arī izveidot kopīgi ar citu dalībvalstu kompetentajām iestādēm. Komisija var sniegt tehnisku atbalstu, konsultācijas un rīkus MI “regulatīvo smilškastu” izveidei un darbībai.

Pirmajā daļā paredzēto pienākumu var pildīt arī, piedaloties esošā “smilškastē”, ciktāl tāda dalība nodrošina līdzvērtīgu valsts tvēruma līmeni dalībvalstīm, kuras piedalās.

2. Var izveidot arī papildu MI “regulatīvās smilškastēs” reģionālā vai vietējā līmenī vai kopīgi ar citu dalībvalstu kompetentajām iestādēm.

3. Eiropas Datu aizsardzības uzraudzītājs arī var izveidot MI “regulatīvo smilškastī” Savienības iestādēm, struktūrām, birojiem un aģentūrām un var pildīt valstu kompetento iestāžu lomas un uzdevumus saskaņā ar šo nodaļu.

4. Dalībvalstis nodrošina, ka 1. un 2. punktā minētās kompetentās iestādes piešķir pietiekamus resursus, lai efektīvi un savlaicīgi panāktu atbilstību šim pantam. Attiecīgā gadījumā valsts kompetentās iestādes sadarbojas ar citām attiecīgajām iestādēm un var ļaut MI ekosistēmā iesaistīt citus dalībniekus. Šis pants neskar citas regulatīvās smilškastes, kas izveidotas saskaņā ar Savienības vai valsts tiesību aktiem. Dalībvalstis nodrošina pienācīgu sadarbības līmeni starp iestādēm, kas uzrauga minētās citas “smilškastes”, un valstu kompetentajām iestādēm.

5. Saskaņā ar 1. punktu izveidotās MI “regulatīvās smilškastēs” nodrošina kontrolētu vidi, kas rosina inovāciju un sekmē inovatīvu MI sistēmu izstrādi, apmācību, testēšanu un validēšanu ierobežotu laikposmu pirms to laišanas tirgū vai nodošanas ekspluatācijā atbilstīgi konkrētam “smilškastēs” plānam, par kuru vienojušies nodrošinātāji un potenciālie nodrošinātāji un kompetentā iestāde. Šādas “smilškastes” var ietvert testēšanu reālos apstākļos, ko pārtrauga “smilškastē”.

6. Kompetentās iestādes attiecīgā gadījumā nodrošina norādījumus, uzraudzību un atbalstu MI “regulatīvās smilškastēs” ietvaros saistībā ar risku identificēšanu, jo īpaši attiecībā uz pamattiesībām, veselību un drošību, saistībā ar testēšanu, seku mazināšanas pasākumiem un to efektivitāti attiecībā uz šajā regulā un, attiecīgā gadījumā, citos Savienības un valstu tiesību aktos paredzētajiem pienākumiem un prasībām, ko uzrauga “smilškastēs” ietvaros.

7. Kompetentās iestādes sniedz nodrošinātājiem un potenciālajiem nodrošinātājiem, kas piedalās MI “regulatīvajā smilškastē”, norādījumus par to, ko sagaida regulatīvi, un to, kā pildīt šajā regulā noteiktās prasības un pienākumus.

Pēc MI sistēmas nodrošinātāja vai potenciālā nodrošinātāja pieprasījuma kompetentā iestāde sniedz rakstisku apliecinājumu par smilškastē sekmīgi veiktajām darbībām. Kompetentā iestāde sniedz arī noslēguma ziņojumu, kurā sīki izklāsta smilškastē veiktās darbības un saistītos rezultātus, un mācīšanās rezultātus. Nodrošinātāji var izmantot šādu dokumentāciju, lai apliecinātu savu atbilstību šai regulai, izmantojot atbilstības novērtēšanas procesu vai attiecīgās tirgus uzraudzības darbības. Šajā sakarā tirgus uzraudzības iestādes un paziņotās struktūras pozitīvi ņem vērā noslēguma ziņojumus un rakstiskus pierādījumus, ko sniedz valsts kompetentās iestādes, lai saprātīgā mērā paātrinātu atbilstības novērtēšanas procedūras.

8. Ievērojot 78. panta konfidencialitātes noteikumus un ar nodrošinātāja vai potenciālā nodrošinātāja piekrišanu Eiropas Komisija un MI padome ir pilnvarotas piekļūt noslēguma ziņojumiem un attiecīgā gadījumā tos ņem vērā, pildot savus šajā regulā paredzētos uzdevumus. Ja gan nodrošinātājs vai potenciālais nodrošinātājs, gan valsts kompetentā iestāde tam nepārprotami piekrīt, noslēguma ziņojumu var darīt publiski pieejamu, izmantojot šajā pantā minēto vienoto informācijas platformu.

9. Ar MI “regulatīvo smilškastu” izveidi tiecas sekmēt šādu mērķu sasniegšanu:

a) uzlabot juridisko noteiktību, lai panāktu regulatīvu atbilstību šai regulai vai, attiecīgā gadījumā, citiem piemērojamiem Savienības un valsts tiesību aktiem;

- b) atbalstīt paraugprakses apmaiņu, izmantojot sadarbību ar iestādēm, kas iesaistītas MI “regulatīvajā smilškastē”;
- c) veicināt inovāciju un konkurētspēju un sekmēt MI ekosistēmas attīstību;
- d) veicināt uz pierādījumiem balstītu regulatīvo mācīšanos;
- e) sekmēt un paātrināt MI sistēmu piekļuvi Savienības tirgum, jo īpaši, ja tās nodrošina MVU, tostarp jaunuzņēmumi.

10. Valsts kompetentās iestādes nodrošina, ka tādā mērā, kādā inovatīvās MI sistēmas ietver personas datu apstrādi vai citādi ir tādu citu valsts iestāžu vai kompetento iestāžu uzraudzībā, kas dod vai atbalsta piekļuvi datiem, valsts datu aizsardzības iestādes un minētās citas valsts vai kompetentās iestādes ir saistītas ar MI “regulatīvās smilškastēs” darbību un ir iesaistītas minēto aspektu uzraudzībā, ciktāl to paredz to attiecīgie uzdevumi un pilnvaras.

11. MI “regulatīvās smilškastēs” neietekmē kompetento iestāžu, kuras uzrauga “smilškastēs”, tostarp reģionālā vai vietējā līmenī, uzraudzības vai korekcijas pilnvaras. Būtiski riski veselībai un drošībai un pamattiesībām, kas konstatēti šādu MI sistēmu izstrādes un testēšanas laikā, tiek pienācīgi mazināti. Valsts kompetentās iestādes ir pilnvarotas uz laiku vai pastāvīgi apturēt testēšanas procesu vai dalību “smilškastē”, ja efektīva mazināšana nav iespējama, un par šādu lēmumu informē MI biroju. Valsts kompetentās iestādes īsteno savas uzraudzības pilnvaras attiecīgo tiesību aktu robežās un, īstenojot tiesību normas attiecībā uz konkrētu MI “regulatīvās smilškastēs” projektu, izmanto savu rīcības brīvību ar mērķi atbalstīt inovāciju MI jomā Savienībā.

12. Nodrošinātāji un potenciālie nodrošinātāji MI “regulatīvajā smilškastē” saskaņā ar piemērojamiem atbildību reglamentējošiem Savienības un valsts tiesību aktiem atbild par jebkādu kaitējumu, kas nodarīts trešām personām “smilškastē” notiekošo eksperimentu rezultātā. Tomēr, ja potenciālie nodrošinātāji ievēro konkrēto plānu un dalības noteikumus un labticīgi ievēro valsts kompetentās iestādes sniegtos norādījumus, iestādes nepiemēro administratīvus naudas sodus par šīs regulas noteikumu pārkāpumiem. Ja citas kompetentās iestādes, kas ir atbildīgas par citiem Savienības un valsts tiesību aktiem, ir bijušas aktīvi iesaistītas MI sistēmas uzraudzībā “smilškastē” un ir sniegušas norādījumus par atbilstību, attiecībā uz minētajiem tiesību aktiem administratīvos naudas sodus nepiemēro.

13. MI “regulatīvās smilškastēs” izstrādā un īsteno tā, lai attiecīgā gadījumā tās sekmētu pārrobežu sadarbību starp valstu kompetentajām iestādēm.

14. Valsts kompetentās iestādes koordinē savas darbības un sadarbojas MI padomes satvarā.

15. Valsts kompetentās iestādes informē MI biroju un MI padomi par “regulatīvās smilškastēs” izveidi un var lūgt tām atbalstu un norādījumus. MI birojs dara publiski pieejamu plānoto un esošo “smilškastu” sarakstu un pastāvīgi atjaunina to, lai veicinātu lielāku mijiedarbību MI “regulatīvajās smilškastēs” un pārrobežu sadarbību.

16. Valsts kompetentās iestādes iesniedz MI birojam un MI padomei ikgadējus ziņojumus, sākot no viena gada pēc MI “regulatīvās smilškastēs” izveides un pēc tam katru gadu līdz tās darbības beigām un galīgajam ziņojumam. Minētajos ziņojumos sniedz informāciju par minēto “regulatīvo smilškastu” darbības gaitu un rezultātiem, ieskaitot paraugpraksi, incidentus, gūtās atziņas un ieteikumus par to struktūru un, attiecīgā gadījumā, par šīs regulas, tostarp tās deleģēto un īstenošanas aktu, piemērošanu un iespējamu pārskatīšanu un citu Savienības tiesību aktu piemērošanu, ko “smilškastēs” ietvaros uzrauga kompetentās iestādes. Valstu kompetentās iestādes minētos gada ziņojumus vai to kopsavilkumus dara publiski pieejamus tiešsaistē. Komisija attiecīgā gadījumā gada ziņojumus ņem vērā, pildot savus šajā regulā paredzētos uzdevumus.

17. Komisija izstrādā vienotu un specializētu saskarni, kas ietver visu attiecīgo informāciju saistībā ar MI “regulatīvajām smilškastēm”, lai ļautu ieinteresētajām personām mijiedarboties ar MI “regulatīvajām smilškastēm” un uzdot jautājumus kompetentajām iestādēm un lūgt nesaistošus norādījumus par tādu inovatīvu produktu, pakalpojumu un uzņēmējdarbības modeļu atbilstību, kuros integrētas MI tehnoloģijas, saskaņā ar 62. panta 1. punkta c) apakšpunktu. Komisija attiecīgā gadījumā proaktīvi koordinē darbības ar valsts kompetentajām iestādēm.

58. pants

Sīki izstrādāta MI "regulatīvo smilškastu" kārtība un to darbība

1. Lai nepieļautu sadrumstalotību Savienībā, Komisija pieņem īstenošanas aktus, kuros sīki norāda MI "regulatīvo smilškastu" izveides, izstrādes, īstenošanas, darbības un uzraudzības kārtību. Īstenošanas aktos iekļauj kopīgus principus šādos jautājumos:

- a) atbilstības un atlases kritēriji dalībai MI "regulatīvajā smilškastē";
- b) procedūras, kas nosaka pieteikšanos MI "regulatīvajai smilškaitei", dalību tajā, tās uzraudzību, iziešanu no tās un tās izbeigšanu, tostarp "smilškaite" plāns un noslēguma ziņojums;
- c) dalībniekiem piemērojamie noteikumi.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

2. Īstenošanas akti, kas minēti 1. punktā, nodrošina, ka:

- a) MI "regulatīvās smilškaite" ir atvērtas jebkuram nodrošinātājam vai potenciālam MI sistēmas nodrošinātājam, kas uz tām piesakās un izpilda atbilstības un atlases kritērijus, kuri ir pārredzami un taisnīgi, un valsts kompetentās iestādes par savu lēmumu informē pieteikumu iesniedzējus trīs mēnešu laikā pēc pieteikuma iesniegšanas;
- b) MI "regulatīvās smilškaite" nodrošina plašu un vienlīdzīgu piekļuvi un atbilst dalības pieprasījumam; nodrošinātāji vai potenciālie nodrošinātāji var arī iesniegt pieteikumus partnerībās ar nodrošinātājiem un citām attiecīgām trešām personām;
- c) sīki izstrādāta kārtība un nosacījumi attiecībā uz MI "regulatīvajām smilškastēm" cik vien iespējams atbalsta valsts kompetento iestāžu elastīgas iespējas izveidot un darbināt savas MI "regulatīvās smilškaite";
- d) piekļuve MI "regulatīvajām smilškastēm" ir bez maksas MVU, tostarp jaunuzņēmumiem, neskarot ārkārtas izmaksas, ko valsts kompetentās iestādes var atgūt taisnīgā un samērīgā veidā;
- e) tās ļauj nodrošinātājiem vai potenciālajiem nodrošinātājiem, izmantojot MI "regulatīvo smilškastu" mācīšanās iznākumus, izpildīt šajā regulā noteiktos atbilstības novērtēšanas pienākumus un brīvprātīgi piemērot 95. pantā minētos rīcības kodeksus;
- f) MI "regulatīvās smilškaite" atvieglo citu MI ekosistēmas attiecīgo dalībnieku, piemēram, pazīnoto struktūru un standartizācijas organizāciju, MVU, tostarp jaunuzņēmumu, uzņēmumu, novatoru, testēšanas un eksperimentēšanas struktūru, pētniecības un eksperimentēšanas laboratoriju un Eiropas Digitālās inovācijas centru, izcilības centru un individuālu pētnieku iesaisti, lai ļautu īstenot un atvieglotu sadarbību ar publisko un privāto sektoru;
- g) procedūras, procesi un administratīvās prasības attiecībā uz pieteikšanos dalībai MI "regulatīvajā smilškastē", atlasi, dalību un iziešanu no "smilškaite" ir vienkāršas un viegli saprotamas un tiek skaidri darītas zināmas, lai atvieglotu dalību MVU, tostarp jaunuzņēmumiem, ar ierobežotām juridiskajām un administratīvajām iespējām, un tās ir racionalizētas visā Savienībā, lai nepieļautu sadrumstalotību un lai dalība MI "regulatīvā smilškastē", ko izveidojusi kāda dalībvalsts vai Eiropas Datu aizsardzības uzraudzītājs, tiktu savstarpēji un vienādi atzīta un tai būtu tādas pašas juridiskās sekas visā Savienībā;
- h) dalība MI "regulatīvajā smilškastē" ir ierobežota uz projekta sarežģītībai un mērogam piemērotu laikposmu, un kuru valsts kompetentā iestāde var pagarināt;
- i) MI "regulatīvās smilškaite" veicina rīku un infrastruktūras izstrādi MI sistēmu testēšanai, salīdzinošai novērtēšanai un to MI sistēmu aspektu izvērtēšanai un izskaidrošanai, kas ir būtiski saistībā ar regulatīvu mācīšanos, piemēram, precizitāte, robustums un kiberdrošība, kā arī pasākumu izstrādi nolūkā mazināt riskus pamattiesībām un sabiedrībai kopumā.

3. Potenciālos nodrošinātājus MI "regulatīvajās smilškastēs", jo īpaši MVU un jaunuzņēmumus, attiecīgā gadījumā novirza uz pirmsieviešanas pakalpojumiem, piemēram, norādījumiem par šīs regulas īstenošanu, citiem papildvērtības pakalpojumiem, piemēram, palīdzību ar standartizācijas dokumentiem un sertifikāciju, testēšanas un eksperimentēšanas struktūrām, Eiropas Digitālās inovācijas centriem un izcilības centriem.

4. Ja valsts kompetentās iestādes apsver iespēju atļaut veikt testēšanu reālos apstākļos, kuru uzrauga saskaņā ar šo pantu izveidojamas MI “regulatīvās smilškastēs” ietvaros, tās konkrēti vienojas ar dalībniekiem par šādas testēšanas noteikumiem un jo īpaši par atbilstošiem aizsardzības pasākumiem nolūkā aizsargāt pamattiesības, veselību un drošību. Attiecīgā gadījumā tās sadarbojas ar citām valstu kompetentajām iestādēm, lai nodrošinātu konsekventu praksi visā Savienībā.

59. pants

Personas datu turpmāka apstrāde dažu MI sistēmu izstrādei sabiedrības interesēs MI “regulatīvajā smilškastē”

1. MI “regulatīvajā smilškastē” personas datus, kas likumīgi savākti citiem mērķiem, var apstrādāt tikai, lai izstrādātu, apmācītu un testētu dažas MI sistēmas “smilškastē”, ja ir izpildīti visi šādi nosacījumi:

- a) MI sistēmas izstrādā publiska iestāde vai cita fiziska vai juridiska persona nolūkā aizsargāt būtiskas sabiedrības intereses un vienā vai vairākās no šādām jomām:
 - i) sabiedrības drošība un sabiedrības veselība, tostarp slimību atklāšana, diagnostika, profilakse, kontrole un ārstēšana un veselības aprūpes sistēmu uzlabošana;
 - ii) vides augsta līmeņa aizsardzība un kvalitātes uzlabošana, bioloģiskās daudzveidības aizsardzība, aizsardzība pret piesārņojumu, zaļās pārkārtošanās pasākumi, klimata pārmaiņu mazināšanas un pielāgošanās pasākumi;
 - iii) enerģētiskā ilgtspēja;
 - iv) transporta sistēmu un mobilitātes, kritiskās infrastruktūras un tīklu drošība un noturība;
 - v) publiskās pārvaldes un sabiedrisko pakalpojumu efektivitāte un kvalitāte;
- b) apstrādātie dati ir nepieciešami, lai izpildītu vienu vai vairākas III nodaļas 2. iedaļā minētās prasības, ja šīs prasības nevar efektīvi izpildīt, apstrādājot anonimizētus, sintētiskus vai citādus nepersondatus;
- c) ir efektīvi pārraudzības mehānismi, lai varētu noteikt, vai “smilškastēs” eksperimentēšanas laikā var rasties kāds augsts risks datu subjektu tiesībām un brīvībām, kā minēts Regulas (ES) 2016/679 35. pantā un Regulas (ES) 2018/1725 39. pantā, kā arī reaģēšanas mehānismi, lai šos riskus ātri mazinātu un vajadzības gadījumā apturētu datu apstrādi;
- d) personas dati, ko paredzēts apstrādāt “smilškastēs” kontekstā, atrodas funkcionāli nodalītā, izolētā un aizsargātā datu apstrādes vidē potenciālā nodrošinātāja pārziņā, un piekļuve minētajiem datiem ir tikai pilnvarotām personām;
- e) nodrošinātāji sākotnēji savāktos datus var kopīgēt tālāk tikai saskaņā ar Savienības tiesību aktiem datu aizsardzības jomā; “smilškastē” radītos personas datus nevar kopīgēt ārpus “smilškastēs”;
- f) personas datu apstrāde “smilškastēs” kontekstā neraisa pasākumus vai lēmumus, kas ietekmē datu subjektus, un tā neietekmē viņu tiesību piemērošanu, kas noteiktas Savienības tiesību aktos par personas datu aizsardzību;
- g) personas dati, kurus apstrādā “smilškastēs” kontekstā, tiek aizsargāti, izmantojot pienācīgus tehniskus un organizatoriskus pasākumus, un tiek dzēsti, tiklīdz dalība “smilškastē” ir beigusies vai pienākušas personas datu glabāšanas perioda beigas;
- h) žurnāldatnes par personas datu apstrādi “smilškastēs” kontekstā tiek glabātas visu dalības “smilškastē” laiku, ja vien Savienības vai valsts tiesību aktos nav noteikts citādi;
- i) pilnīgu un detalizētu procesa aprakstu un pamatojumu MI sistēmas apmācībai, testēšanai un validēšanai glabā kopā ar testēšanas rezultātiem kā daļu no tehniskās dokumentācijas, kas minēta IV pielikumā;

- j) kompetento iestāžu tīmekļa vietnē tiek publicēts šis kopsavilkums par “smilškastē” izstrādāto MI projektu, tā mērķiem un gaidāmiem rezultātiem; šis pienākums neattiecas uz sensitīviem operatīvajiem datiem saistībā ar tiesībaizsardzības, robežkontroles, imigrācijas vai patvēruma iestāžu darbībām.
2. Lai, darbojoties tiesībaizsardzības iestāžu kontrolē un atbildībā, novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai veiktu kriminālvajāšanu par tiem, vai izpildītu kriminālsodus, tostarp, lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, personas datu apstrāde MI “regulatīvajās smilškastēs” notiek, pamatojoties uz konkrētiem Savienības vai valsts tiesību aktiem, un uz to attiecas tie paši kumulatīvie nosacījumi, kas minēti 1. punktā.
3. Šā panta 1. punkts neskar Savienības vai valsts tiesību aktus, kas izslēdz personas datu apstrādi citiem mērķiem nekā tie, kas nepārprotami minēti attiecīgajā tiesību aktā, kā arī Savienības vai valsts tiesību aktus, ar kuriem nosaka pamatu personas datu apstrādei, kas ir nepieciešama inovatīvu MI sistēmu izstrādei, testēšanai vai apmācībai, vai jebkādu citu juridisko pamatu saskaņā ar Savienības tiesību aktiem par personas datu aizsardzību.

60. pants

Augsta riska MI sistēmu testēšana reālos apstākļos ārpus MI “regulatīvajām smilškastēm”

1. Augsta riska MI sistēmu testēšanu reālos apstākļos ārpus MI “regulatīvajām smilškastēm” var veikt III pielikumā uzskaitīto augsta riska MI sistēmu nodrošinātāji vai potenciālie nodrošinātāji saskaņā ar šo pantu un šajā pantā minēto testēšanas reālos apstākļos plānu, neskarot 5. pantā paredzētos aizliegumus.

Komisija ar īstenošanas aktiem precizē testēšanas reālos apstākļos plāna detalizētus elementus. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

Šis punkts neskar Savienības vai valsts tiesību aktus par tādu augsta riska MI sistēmu testēšanu reālos apstākļos, kas saistītas ar produktiem, uz kuriem attiecas I pielikumā uzskaitītie Savienības saskaņošanas tiesību akti.

2. Nodrošinātāji vai potenciālie nodrošinātāji III pielikumā minēto augsta riska MI sistēmu testēšanu reālos apstākļos var veikt jebkurā laikā pirms MI sistēmas laišanas tirgū vai nodošanas ekspluatācijā paši vai partnerībā ar vienu vai vairākiem uzturētājiem vai potenciālajiem uzturētājiem.

3. Augsta riska MI sistēmu testēšana reālos apstākļos saskaņā ar šo pantu neskar jebkādu ētiskuma izvērtēšanu, kas prasīta Savienības vai valsts tiesību aktos.

4. Nodrošinātāji vai potenciālie nodrošinātāji var veikt testēšanu reālos apstākļos tikai tad, ja ir izpildīti visi turpmāk minētie nosacījumi:

- a) nodrošinātājs vai potenciālais nodrošinātājs ir izstrādājis testēšanas reālos apstākļos plānu un iesniedzis to tirgus uzraudzības iestādei dalībvalstī, kurā paredzēts veikt testēšanu reālos apstākļos;
- b) tirgus uzraudzības iestāde dalībvalstī, kurā paredzēts veikt testēšanu reālos apstākļos, ir apstiprinājusi testēšanu reālos apstākļos un testēšanas reālos apstākļos plānu; ja tirgus uzraudzības iestāde nav sniegusi atbildi 30 dienu laikā, uzskata, ka testēšana reālos apstākļos un testēšanas reālos apstākļos plāns ir apstiprināts; ja valsts tiesību akti neparedz automātisku apstiprinājumu, testēšanai reālos apstākļos aizvien ir nepieciešama atļauja;
- c) nodrošinātājs vai potenciālais nodrošinātājs, izņemot III pielikuma 1., 6. un 7. punktā minēto augsta riska MI sistēmu tiesībaizsardzības, migrācijas, patvēruma un robežkontroles pārvaldības jomā un III pielikuma 2. punktā minēto augsta riska MI sistēmu nodrošinātājus vai potenciālos nodrošinātājus, ir reģistrējis testēšanu reālos apstākļos saskaņā ar 71. panta 4. punktu ar unikālu Savienības mēroga vienoto identifikācijas numuru un iesniedzis IX pielikumā norādīto informāciju; III pielikuma 1., 6. un 7. punktā minēto augsta riska MI sistēmu nodrošinātājs vai potenciālais nodrošinātājs tiesībaizsardzības, migrācijas, patvēruma un robežkontroles pārvaldības jomā ir reģistrējis testēšanu reālos apstākļos ES datubāzes drošajā nepublicajā iedaļā saskaņā ar 49. panta 4. punkta d) apakšpunktu ar unikālu Savienības mēroga vienoto identifikācijas numuru un tajā norādīto informāciju; III pielikuma 2. punktā minētais augsta riska AI sistēmu nodrošinātājs vai potenciālais nodrošinātājs ir reģistrējis testēšanu reālos apstākļos saskaņā ar 49. panta 5. punktu;

- d) nodrošinātājs vai potenciālais nodrošinātājs, kas veic testēšanu reālos apstākļos, ir iedibināts Savienībā vai ir iecēlis juridisko pārstāvi, kurš ir iedibināts Savienībā;
- e) datus, kas savākti un apstrādāti testēšanas vajadzībām reālos apstākļos, pārsūta uz trešām valstīm tikai tad, ja ir īstenoti atbilstīgi un piemērojami aizsardzības pasākumi, kas paredzēti Savienības tiesību aktos;
- f) testēšana reālos apstākļos neilgst ilgāk, kā nepieciešams, lai sasniegtu tās mērķus, un jebkurā gadījumā ne ilgāk kā sešus mēnešus, ko var pagarināt vēl par sešiem mēnešiem, ja nodrošinātājs vai potenciālais nodrošinātājs par to iepriekš paziņo tirgus uzraudzības iestādei, pievienojot paskaidrojumu, kādēļ nepieciešams šāds pagarinājums;
- g) testēšanas reālos apstākļos subjekti, kas ir personas, kuras pieder pie neaizsargātas grupām to vecuma vai garīgās invaliditātes dēļ, ir pienācīgi aizsargāti;
- h) ja nodrošinātājs vai potenciālais nodrošinātājs organizē testēšanu reālos apstākļos sadarbībā ar vienu vai vairākiem uzturētājiem vai potenciālajiem uzturētājiem, pēdējie minētie ir informēti par visiem testēšanas aspektiem, kas ir būtiski, pieņemot lēmumu par dalību, un tiem ir sniegta attiecīgā MI sistēmas lietošanas instrukcija, kas minēta 13. pantā; nodrošinātājs vai potenciālais nodrošinātājs un potenciālais uzturētājs noslēdz vienošanos, kurā precizē savas lomas un pienākumus, lai nodrošinātu atbilstību noteikumiem par testēšanu reālos apstākļos saskaņā ar šo regulu un citiem piemērojamiem Savienības un valsts tiesību aktiem;
- i) subjekti, kas piedalās testēšanā reālos apstākļos, ir devuši informētu piekrišanu saskaņā ar 61. pantu, vai tiesībaizsardzības gadījumos, ja informētas piekrišanas iegūšana kavētu MI sistēmas testēšanu, pašai testēšanai un testēšanas rezultātiem reālos apstākļos nav nekādas negatīvas ietekmes uz subjektiem un pēc testa veikšanas viņu personas datus dzēš;
- j) testēšanu reālos apstākļos efektīvi pārbauga nodrošinātājs vai potenciālais nodrošinātājs, kā arī uzturētājs vai potenciālais uzturētājs ar tādu personu starpniecību, kuras ir atbilstoši kvalificētas attiecīgajā jomā un kurām ir vajadzīgās spējas, apmācība un pilnvaras savu uzdevumu veikšanai;
- k) MI sistēmas prognozes, ieteikumus vai lēmumus var faktiski reversēt un neņemt vērā.

5. Subjekti, kas piedalās testēšanā reālos apstākļos, vai attiecīgi to likumiski izraudzītais pārstāvis var bez jebkādam nelabvēlīgām sekām un nesniedzot nekādu pamatojumu jebkurā laikā izstāties no testēšanas, atsaucot savu informēto piekrišanu, un var prasīt savu personas datu tūlītēju un neatgriezenisku dzēšanu. Informētas piekrišanas atsaukšana neietekmē jau veiktās darbības.

6. Saskaņā ar 75. pantu dalībvalstis piešķir savām tirgus uzraudzības iestādēm pilnvaras pieprasīt, lai nodrošinātāji un potenciālie nodrošinātāji sniegtu informāciju, veikt neizziņotas attālinātas vai uz vietas veiktas inspekcijas un veikt pārbaudes par testēšanas veikšanu reālos apstākļos un ar to saistītajām augsta riska MI sistēmām. Tirgus uzraudzības iestādes izmanto minētās pilnvaras, lai nodrošinātu testēšanas reālos apstākļos drošu izstrādi.

7. Par jebkuru nopietnu incidentu, kas identificēts testēšanas reālos apstākļos gaitā, ziņo valsts tirgus uzraudzības iestādei saskaņā ar 73. pantu. Nodrošinātājs vai potenciālais nodrošinātājs pieņem tūlītējus ietekmes mazināšanas pasākumus vai, ja tas nav iespējams, aptur testēšanu reālos apstākļos līdz brīdim, kad notiek šāda mazināšana, vai citādi to izbeidz. Nodrošinātājs vai potenciālais nodrošinātājs izveido procedūru MI sistēmas tūlītējai atsaukšanai pēc šādas testēšanas reālos apstākļos pabeigšanas.

8. Nodrošinātāji vai potenciālie nodrošinātāji paziņo valsts tirgus uzraudzības iestādei dalībvalstī, kurā paredzēts veikt testēšanu reālos apstākļos, par testēšanas reālos apstākļos apturēšanu vai izbeigšanu un par galīgajiem iznākumiem.

9. Nodrošinātājs vai potenciālais nodrošinātājs saskaņā ar piemērojamiem atbildību reglamentējošiem Savienības un valsts tiesību aktiem ir atbildīgi par jebkādu kaitējumu, kas nodarīts to testēšanā reālos apstākļos.

61. pants

Informēta piekrišana piedalīties testēšanā reālos apstākļos ārpus MI “regulatīvajām smilškastēm”

1. Lai veiktu testēšanu reālos apstākļos, kas paredzēta 60. pantā, no testēšanas subjektiem saņem brīvi dotu informētu piekrišanu pirms to dalības šādā testēšanā un pēc tam, kad tie ir pienācīgi informēti, tiem sniedzot kodolīgu, skaidru, būtisku un saprotamu informāciju par:
 - a) testēšanas reālos apstākļos veidu un mērķi un iespējamām neērtībām, kas var būt saistītas ar viņu dalību;
 - b) apstākļiem, kādos tiks veikta testēšana reālos apstākļos, tostarp paredzamo subjekta vai subjektu dalības ilgumu;
 - c) viņu tiesībām un garantijām attiecībā uz viņu dalību, jo īpaši viņu tiesībām atteikties piedalīties un tiesībām bez jebkādam nelabvēlīgām sekām un nesniedzot nekādu pamatojumu jebkurā laikā izstāties no testēšanas reālos apstākļos;
 - d) kārtību, kādā pieprasa MI sistēmas prognožu, ieteikumu vai lēmumu reversēšanu vai neņemšanu vērā;
 - e) unikālu Savienības mēroga vienoto identifikācijas numuru testēšanai reālos apstākļos saskaņā ar 60. panta 4. punkta c) apakšpunktu un tā nodrošinātāja vai viņa juridiskā pārstāvja kontaktinformāciju, no kura var iegūt sīkāku informāciju.
2. Informētu piekrišanu datē un dokumentē, un testēšanas subjektiem vai to juridiskajam pārstāvim izsniedz kopiju.

62. pants

Pasākumi nodrošinātājiem un uzturētājiem, jo īpaši MVU, tostarp jaunuzņēmumiem

1. Dalībvalstis veic šādas darbības:
 - a) dod MVU, tostarp jaunuzņēmumiem, kuriem ir juridiskā adrese vai filiāle Savienībā, prioritāru piekļuvi MI “regulatīvajām smilškastēm”, ciktāl tie atbilst atbilstības nosacījumiem un atlases kritērijiem; prioritārā piekļuve neliedz citiem MVU, tostarp jaunuzņēmumiem, kuri nav tie, kas minēti šajā punktā, piekļūt MI “regulatīvajai smilškaitei” ar noteikumu, ka tie arī atbilst atbilstības nosacījumiem un atlases kritērijiem;
 - b) organizē konkrētas izpratnes veicināšanas un apmācības darbības par šīs regulas piemērošanu, kas pielāgotas MVU, tostarp jaunuzņēmumu, uzturētāju un, attiecīgā gadījumā, vietējo publisko iestāžu vajadzībām;
 - c) izmanto esošos īpašos kanālus un, attiecīgā gadījumā, izveido jaunus saziņai ar MVU, tostarp jaunuzņēmumiem, uzturētājiem, citiem novatoriem un, attiecīgā gadījumā, vietējām publiskajām iestādēm, lai sniegtu konsultācijas un atbildētu uz jautājumiem par šīs regulas īstenošanu, tostarp par dalību MI “regulatīvajās smilškastēs”;
 - d) sekmē MVU un citu attiecīgo ieinteresēto personu līdzdalību standartizācijas izstrādes procesā.
2. Nosakot maksas par atbilstības novērtēšanu saskaņā ar 43. pantu, ņem vērā nodrošinātāju, kuri ir MVU, tostarp jaunuzņēmumi, konkrētās intereses un vajadzības, samazinot šīs maksas proporcionāli to lielumam, tirgus lielumam un citiem attiecīgiem rādītājiem.
3. MI birojs veic šādas darbības:
 - a) nodrošina standartizētas veidnes jomām, uz kurām attiecas šī regula, kā MI padome norāda savā pieprasījumā;
 - b) izstrādā un uztur vienotu informācijas platformu, kas visiem operatoriem visā Savienībā sniedz viegli izmantojamu informāciju saistībā ar šo regulu;

- c) rīko atbilstīgas komunikācijas kampaņas, lai palielinātu informētību par pienākumiem, kas izriet no šīs regulas;
- d) izvērtē un veicina paraugprakses konvergenci publiskā iepirkuma procedūrās saistībā ar MI sistēmām.

63. pants

Atkāpes konkrētiem operatoriem

1. Mikrouzņēmumi Komisijas Ieteikuma 2003/361/EK nozīmē var dažus šīs regulas 17. pantā prasītās kvalitātes vadības sistēmas elementus pildīt vienkāršotā veidā ar noteikumu, ka tiem nav partneruzņēmumu vai saistītu uzņēmumu minētā ieteikuma nozīmē. Minētajā nolūkā Komisija izstrādā pamatnostādnes par kvalitātes vadības sistēmas elementiem, ko var pildīt vienkāršotā veidā, kurā ņem vērā mikrouzņēmumu vajadzības, neietekmējot aizsardzības līmeni vai vajadzību ievērot prasības attiecībā uz augsta riska MI sistēmām.
2. Šā panta 1. punktu neinterpretē kā tādu, kas atbrīvo minētos operatorus no citu šajā regulā noteikto prasību vai pienākumu izpildes, tostarp to prasību un pienākumu izpildes, kas noteikti 9., 10., 11., 12., 13., 14., 15., 72. un 73. pantā.

VII NODAĻA

PĀRVALDĪBA

1. IEDAĻA

Pārvaldība Savienības līmenī

64. pants

MI birojs

1. Komisija attīsta Savienības speciālās zināšanas un spējas MI jomā, izmantojot MI biroju.
2. Dalībvalstis sekmē MI birojam uzticētos uzdevumus, kā atspoguļots šajā regulā.

65. pants

Eiropas Mākslīgā intelekta padomes izveide un struktūra

1. Ar šo tiek izveidota Eiropas mākslīgā intelekta padome ("MI padome").
2. MI padomē ir pa vienam pārstāvim no katras dalībvalsts. Eiropas datu aizsardzības uzraudzītājs piedalās kā novērotājs. MI padomes sanāksmēs piedalās arī MI birojs, nepiedaloties balsošanā. MI padome var uzaicināt uz sanāksmēm citas valstu un Savienības iestādes, struktūras vai ekspertus, katru gadījumu izskatot atsevišķi, ja apspriestie jautājumi tiem ir būtiski.
3. Katru pārstāvi izraugās attiecīgā dalībvalsts uz trīs gadu laikposmu, kas ir vienu reizi atjaunojams.
4. Dalībvalstis nodrošina, ka to pārstāvji MI padomē:
 - a) tiem ir attiecīgās kompetences un pilnvaras savā dalībvalstī, lai aktīvi sekmētu 66. pantā minēto MI padomes uzdevumu izpildi;
 - b) ir izraudzīti par vienoto kontaktpunktu saziņai ar MI padomi un attiecīgā gadījumā, ņemot vērā dalībvalstu vajadzības, par vienoto kontaktpunktu ieinteresētajām personām;

c) ir pilnvaroti veicināt konsekveni un koordināciju starp valsts kompetentajām iestādēm savā dalībvalstī attiecībā uz šīs regulas īstenošanu, tostarp, vācot attiecīgus datus un informāciju, lai tās varētu pildīt savus uzdevumus MI padomē.

5. Dalībvalstu izraudzītie pārstāvji ar divu trešdaļu balsu vairākumu pieņem MI padomes reglamentu. Reglamentā jo īpaši nosaka procedūras atlases procesam, priekšsēdētāja pilnvaru ilgumu un tā uzdevumu specifikācijas, detalizētu balsošanas kārtību un MI padomes un tās apakšgrupu darbības organizāciju.

6. MI padome izveido divas pastāvīgas apakšgrupas, lai nodrošinātu platformu sadarbībai un apmaiņai starp tirgus uzraudzības iestādēm un paziņotu iestādēm par jautājumiem, kas saistīti attiecīgi ar tirgus uzraudzību un paziņotajām struktūrām.

Tirgus uzraudzības pastāvīgajai apakšgrupai būtu jādarbojas kā šīs regulas administratīvās sadarbības grupai (ADCO) Regulas (ES) 2019/1020 30. panta nozīmē.

MI padome vajadzības gadījumā var izveidot citas pastāvīgas vai pagaidu apakšgrupas konkrētu jautājumu izskatīšanai. Attiecīgā gadījumā uz šādām apakšgrupām vai minēto apakšgrupu konkrētām sanāksmēm kā novērotājus var uzaicināt 67. pantā minētā konsultatīvā foruma pārstāvjus.

7. MI padome ir organizēta un darbojas tā, lai nodrošinātu savas darbības neatkarību, objektivitāti un neitralitāti.

8. MI padomi vada viens no dalībvalstu pārstāvjiem. MI birojs nodrošina MI padomes sekretariātu, pēc priekšsēdētāja pieprasījuma sasauc sanāksmes un sagatavo darba kārtību saskaņā ar MI padomes uzdevumiem, ievērojot šo regulu un MI padomes reglamentu.

66. pants

MI padomes uzdevumi

MI padome konsultē Komisiju un dalībvalstis un palīdz tām, lai veicinātu šīs regulas konsekventu un efektīvu piemērošanu. Minētajā nolūkā MI padome var jo īpaši:

- a) sekmēt koordināciju starp valstu kompetentajām iestādēm, kuras ir atbildīgas par šīs regulas piemērošanu, un, sadarbībā ar attiecīgajām tirgus uzraudzības iestādēm un ja ir vienošanās ar tām, atbalstīt 74. panta 11. punktā minētos tirgus uzraudzības iestāžu kopīgos pasākumus;
- b) apkopot un kopīgot tehniskās un regulatīvās speciālās zināšanas un paraugpraksi dalībvalstu starpā;
- c) sniegt konsultācijas par šīs regulas īstenošanu, jo īpaši attiecībā uz noteikumu par vispārīga lietojuma MI modeļiem izpildes panākšanu;
- d) veicināt administratīvās prakses saskaņošanu dalībvalstīs, tostarp attiecībā uz atkāpi no 46. pantā minētajām atbilstības novērtēšanas procedūrām, MI "regulatīvo smilškastu" darbību un testēšanu reālos apstākļos, kā minēts 57., 59. un 60. pantā;
- e) pēc Komisijas pieprasījuma vai pēc savas iniciatīvas sniegt ieteikumus un rakstiskus atzinumus par visiem attiecīgajiem jautājumiem, kas saistīti ar šīs regulas īstenošanu un tās konsekventu un efektīvu piemērošanu, tostarp:
 - i) par rīcības kodeksu un prakses kodeksu izstrādi un piemērošanu, ievērojot šo regulu, kā arī par Komisijas pamatnostādņu izstrādi un piemērošanu;
 - ii) par šīs regulas izvērtēšanu un pārskatīšanu, ievērojot 112. pantu, tostarp attiecībā uz 73. pantā minētajiem ziņojumiem par nopietniem incidentiem un 71. pantā minētās ES datubāzes darbību, deleģēto un īstenošanas aktu sagatavošanu un attiecībā uz šīs regulas iespējamu pieskaņošanu I pielikumā uzskaitītajiem Savienības saskaņošanas tiesību aktiem;
 - iii) par tehniskajām specifikācijām vai esošajiem standartiem attiecībā uz III nodaļas 2. iedaļā noteiktajām prasībām;

- iv) par 40. un 41. pantā minēto saskaņoto standartu vai kopīgo specifikāciju izmantošanu;
- v) tādām tendencēm kā Eiropas konkurētspēja MI jomā pasaulē, MI ieviešana Savienībā un digitālo prasmju attīstība;
- vi) tendencēm MI vērtības ķēžu mainīgajā tipoloģijā, jo īpaši par no tā izrietošām sekām attiecībā uz pārskatatbildību;
- vii) par iespējamo vajadzību grozīt III pielikumu saskaņā ar 7. pantu un iespējamo vajadzību pārskatīt 5. pantu, ievērojot 112. pantu, ņemot vērā attiecīgos pieejamos pierādījumus un jaunākās norises tehnoloģiju jomā;
- f) atbalstīt Komisiju MI pratības un sabiedrības informētības veicināšanā un izpratnes veicināšanā par ieguvumiem, riskiem, aizsardzības pasākumiem, tiesībām un pienākumiem saistībā ar MI sistēmu lietošanu;
- g) veicināt kopīgu kritēriju izstrādi un tirgus dalībnieku un kompetento iestāžu vienotu izpratni par šajā regulā paredzētajiem attiecīgajiem jēdzieniem, tostarp sekmējot kritēriju izstrādi;
- h) attiecīgā gadījumā sadarboties ar citām Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī ar attiecīgajām Savienības ekspertu grupām un tīkliem, jo īpaši tādās jomās kā produktu drošība, kiberdrošība, konkurence, digitālie un mediju pakalpojumi, finanšu pakalpojumi, patērētāju aizsardzība, datu un pamattiesību aizsardzība;
- i) veicināt efektīvu sadarbību ar trešo valstu kompetentajām iestādēm un starptautiskajām organizācijām;
- j) palīdzēt valstu kompetentajām iestādēm un Komisijai organizatorisko un tehnisko speciālo zināšanu izstrādē, kas vajadzīgas šīs regulas īstenošanai, tostarp, dodot ieguldījumu šīs regulas īstenošanā iesaistītā dalībvalstu personāla apmācības vajadzību novērtēšanā;
- k) palīdzēt MI birojam sniegt atbalstu valstu kompetentajām iestādēm MI “regulatīvo smilškastu” izveidē un izstrādē un sekmēt sadarbību un informācijas apmaiņu starp MI “regulatīvajām smilškastēm”;
- l) sniegt ieguldījumu un attiecīgas konsultācijas norādījumu dokumentu izstrādē;
- m) konsultēt Komisiju saistībā ar starptautiskiem jautājumiem MI jomā;
- n) sniegt atzinumus Komisijai par kvalificētiem brīdinājumiem attiecībā uz vispārīga lietojuma MI modeļiem;
- o) saņemt dalībvalstu atzinumus par kvalificētiem brīdinājumiem attiecībā uz vispārīga lietojuma MI modeļiem un par valstu pieredzi un praksi saistībā ar MI sistēmu, jo īpaši sistēmu, kurās integrē vispārīga lietojuma MI modeļus, pārraudzību un ieviešanu.

67. pants

Konsultatīvais forums

1. Izveido konsultatīvu forumu, lai sniegtu tehniskas speciālās zināšanas un konsultācijas MI padomei un Komisijai un sekmētu to uzdevumus, kas paredzēti šajā regulā.
2. Konsultatīvā foruma dalībnieki pārstāv līdzsvarotu ieinteresēto personu loku, tostarp nozari, jaunuzņēmumus, MVU, pilsonisko sabiedrību un akadēmiskās aprindas. Konsultatīvā foruma sastāvs ir līdzsvarots attiecībā uz komerciālām un nekomerciālām interesēm un – komerciālo interešu kategorijā – attiecībā uz MVU un citiem uzņēmumiem.
3. Komisija saskaņā ar 2. punktā noteiktajiem kritērijiem ieceļ konsultatīvā foruma locekļus no ieinteresēto personu vidus, kurām ir atzītas speciālās zināšanas MI jomā.

4. Konsultatīvā foruma locekļu pilnvaru termiņš ir divi gadi, un to var pagarināt par laikposmu, kas nepārsniedz četrus gadus.
5. Pamattiesību aģentūra, ENISA, Eiropas Standartizācijas komiteja (CEN), Eiropas Elektrotehnikas standartizācijas komiteja (CENELEC) un Eiropas Telesakaru standartu institūts (ETSI) ir konsultatīvā foruma pastāvīgie locekļi.
6. Konsultatīvais forums izstrādā savu reglamentu. Tas ievēlē divus līdzpriekšsēdētājus no savu locekļu vidus saskaņā ar 2. punktā noteiktajiem kritērijiem. Līdzpriekšsēdētāju amata pilnvaru termiņš ir divi gadi, un to var vienreiz atjaunot.
7. Konsultatīvais forums rīko sanāksmes vismaz divas reizes gadā. Konsultatīvais forums uz savām sanāksmēm var uzaicināt ekspertus un citas ieinteresētās personas.
8. Konsultatīvais forums var pēc MI padomes vai Komisijas pieprasījuma sagatavot atzinumus, ieteikumus un rakstiskus komentārus.
9. Lai izskatītu konkrētus jautājumus, kas saistīti ar šīs regulas mērķiem, konsultatīvais forums vajadzības gadījumā var izveidot pastāvīgas vai pagaidu apakšgrupas.
10. Konsultatīvais forums sagatavo gada ziņojumu par savām darbībām. Minēto ziņojumu publicē.

68. pants

Neatkarīgu ekspertu zinātniskā grupa

1. Komisija ar īstenošanas aktu paredz noteikumus par neatkarīgu ekspertu zinātniskās grupas ("zinātniskā grupa") izveidi nolūkā sniegt atbalstu šajā regulā paredzētajiem izpildes panākšanas pasākumiem. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.
2. Zinātniskā grupa sastāv no ekspertiem, ko atlasījusi Komisija, pamatojoties uz jaunākajām zinātniskajām un tehniskajām speciālajām zināšanām MI jomā, kuras vajadzīgas 3. punktā minētajiem uzdevumiem, un tā spēj pierādīt, ka atbilst visiem šādiem kritērijiem:
 - a) tai ir īpašas speciālās zināšanas un kompetence un zinātniskās vai tehniskās speciālās zināšanas MI jomā;
 - b) neatkarība no jebkura MI sistēmu vai vispārīga lietojuma MI modeļu nodrošinātāja;
 - c) spēja darbības veikt rūpīgi, pareizi un objektīvi.

Komisija, apspriežoties ar MI padomi, lemj par ekspertu skaitu grupā saskaņā ar prasītajām vajadzībām un nodrošina taisnīgu dzimumu un ģeogrāfisko pārstāvību.

3. Zinātniskā grupa sniedz konsultācijas un atbalstu MI birojam, jo īpaši attiecībā uz šādiem uzdevumiem:
 - a) sniegt atbalstu šīs regulas īstenošanā un izpildes panākšanā attiecībā uz vispārīga lietojuma MI modeļiem un sistēmām, jo īpaši
 - i) brīdinot MI biroju par vispārīga lietojuma MI modeļu iespējamiem sistēmiskiem riskiem Savienības līmenī saskaņā ar 90. pantu;
 - ii) dodot ieguldījumu vispārīga lietojuma MI modeļu un sistēmu spēju izvērtēšanas rīku un metodiku izstrādē, tostarp ar kritērijiem;
 - iii) sniedzot konsultācijas par vispārīga lietojuma MI modeļu ar sistēmisku risku klasifikāciju;
 - iv) sniedzot konsultācijas par dažādu vispārīga lietojuma MI modeļu un sistēmu klasifikāciju;

- v) dodot ieguldījumu rīku un veidņu izstrādē;
 - b) atbalstīt tirgus uzraudzības iestāžu darbu pēc minēto iestāžu lūguma;
 - c) atbalstīt pārrobežu tirgus uzraudzības darbības, kā minēts 74. panta 11. punktā, neskarot tirgus uzraudzības iestāžu pilnvaras;
 - d) atbalstīt MI biroju tā pienākumu izpildē saistībā ar Savienības drošības procedūru, ievērojot 81. pantu.
4. Zinātniskās grupas eksperti savus uzdevumus veic neatkarīgi un objektīvi un nodrošina uzdevumu un darbību izpildes gaitā iegūtās informācijas un datu konfidencialitāti. Pildot savus 3. punktā paredzētos uzdevumus, viņi nevienam nelūdz un ne no viena nepieņem norādījumus. Katrs eksperts sagatavo interešu deklarāciju, kuru publisko. MI birojs izstrādā sistēmas un procedūras, lai aktīvi pārvaldītu un novērstu iespējamus interešu konfliktus.
5. Šā panta 1. punktā minētajā īstenošanas aktā iekļauj noteikumus par nosacījumiem, procedūrām un sīki izstrādātu kārtību, kā zinātniskā grupa un tās locekļi izdod brīdinājumus un lūdz MI biroja palīdzību zinātniskās grupas uzdevumu pildīšanā.

69. pants

Dalībvalstu piekļuve ekspertu rezervei

1. Dalībvalstis var pieaicināt zinātniskās grupas ekspertus sniegt atbalstu to izpildes panākšanas pasākumiem, kas paredzēti šajā regulā.
2. Dalībvalstīm var prasīt maksu par ekspertu sniegtajām konsultācijām un atbalstu. Maksu struktūru un apmēru, kā arī atgūstamo izmaksu apmēru un struktūru nosaka 68. panta 1. punktā minētajā īstenošanas aktā, ņemot vērā šīs regulas pienācīgas īstenošanas mērķus, izmaksu lietderību un nepieciešamību nodrošināt visām dalībvalstīm efektīvu piekļuvi ekspertiem.
3. Komisija vajadzības gadījumā veicina dalībvalstu savlaicīgu piekļuvi ekspertiem un nodrošina, ka atbalsta darbību kombinācija, kuras veic Savienības MI testēšanas atbalsts, ievērojot 84. pantu, un eksperti, ievērojot šo pantu, tiek efektīvi organizēti un sniedz vislielāko iespējamo pievienoto vērtību.

2. IEDAĻA

Valsts kompetentās iestādes

70. pants

Valsts kompetento iestāžu un vienotā kontaktpunkta izraudzīšanās

1. Katra dalībvalsts šīs regulas nolūkos kā valsts kompetentās iestādes izveido vai izraugās vismaz vienu paziņojošo iestādi un vismaz vienu tirgus uzraudzības iestādi. Minētās valsts kompetentās iestādes īsteno savas pilnvaras neatkarīgi, objektīvi un bez aizspriedumiem, lai garantētu savu darbību un uzdevumu objektivitāti un nodrošinātu šīs regulas piemērošanu un īstenošanu. Minēto iestāžu locekļi atturas no jebkuras rīcības, kas nav saderīga ar viņu pienākumiem. Ar noteikumu, ka tiek ievēroti minētie principi, šādas darbības un uzdevumus var veikt viena vai vairākas izraudzītās iestādes saskaņā ar dalībvalsts organizatoriskajām vajadzībām.
2. Dalībvalstis dara zināmu Komisijai paziņojošo iestāžu un tirgus uzraudzības iestāžu identitāti un minēto iestāžu uzdevumus, kā arī turpmākas izmaiņas šajā sakarā. Dalībvalstis līdz 2025. gada 2. augustam publisko informāciju par to, kā sazināties ar kompetentajām iestādēm un vienotajiem kontaktpunktiem, izmantojot elektroniskās saziņas līdzekļus. Dalībvalstis izraugās tirgus uzraudzības iestādi, kas darbojas kā vienotais kontaktpunkts saistībā ar šo regulu, un paziņo Komisijai vienotā kontaktpunkta identitāti. Komisija vienoto kontaktpunktu sarakstu dara publiski pieejamu.

3. Dalībvalstis nodrošina, ka to valsts kompetentajām iestādēm tiek nodrošināti pienācīgi tehniskie, finanšu un cilvēkresursi, kā arī infrastruktūra, lai efektīvi pildītu uzdevumus, kas tām noteikti ar šo regulu. Jo īpaši, valsts kompetentajām iestādēm ir pietiekams skaits pastāvīgi pieejama personāla, kura kompetences un speciālās zināšanas ietver padziļinātu izpratni par MI tehnoloģijām, datiem un datošanu, personas datu aizsardzību, kiberdrošību, pamattiesībām, riskiem attiecībā uz veselību un drošību un zināšanas par esošajiem standartiem un juridiskajām prasībām. Dalībvalstis katru gadu novērtē un, ja vajadzīgs, atjaunina šajā punktā minētās kompetences un resursu prasības.
4. Valsts kompetentās iestādes veic atbilstošus pasākumus, lai nodrošinātu pienācīga līmeņa kiberdrošību.
5. Veicot savus pienākumus, valsts kompetentās iestādes rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.
6. Līdz 2025. gada 2. augustam un pēc tam reizi divos gados dalībvalstis ziņo Komisijai par valsts kompetento iestāžu finanšu un cilvēkresursu situāciju, novērtējot to atbilstību. Komisija šo informāciju nosūta MI padomei apspriešanai un iespējamai ieteikumu sniegšanai.
7. Komisija veicina pieredzes apmaiņu starp valstu kompetentajām iestādēm.
8. Valstu kompetentās iestādes var sniegt norādījumus un konsultācijas par šīs regulas īstenošanu, jo īpaši MVU, tostarp jaunuzņēmumiem, attiecīgi ņemot vērā MI padomes un Komisijas norādījumus un padomus. Kad valsts kompetentās iestādes plāno sniegt norādījumus un konsultācijas attiecībā uz MI sistēmu jomās, uz kurām attiecas citi Savienības tiesību akti, vajadzības gadījumā tās apspriežas ar attiecīgajām minētajos Savienības tiesību aktos paredzētajām valsts kompetentajām iestādēm.
9. Ja šīs regulas piemērošanas jomā ietilpst Savienības iestādes, struktūras, biroji un aģentūras, kā kompetentā iestāde to uzraudzības nolūkā darbojas Eiropas Datu aizsardzības uzraudzītājs.

VIII NODAĻA

ES DATUBĀZE PAR AUGSTA RISKĀ MI SISTĒMĀM

71. pants

ES datubāze par augsta riska MI sistēmām, kas uzskaitītas III pielikumā

1. Komisija sadarbībā ar dalībvalstīm izveido un uztur ES datubāzi, kas ietver šā panta 2. un 3. punktā minēto informāciju par 6. panta 2. punktā minētajām augsta riska MI sistēmām, kuras reģistrētas saskaņā ar 49. un 60. pantu un MI sistēmas, kas nav uzskatāmas par augsta riska sistēmām saskaņā ar 6. panta 3. punktu un ir reģistrētas saskaņā ar 6. panta 4. punktu un 49. pantu. Nosakot šādas datubāzes funkcionālās specifikācijas, Komisija apspriežas ar attiecīgajiem ekspertiem, un, atjauninot šādas datubāzes funkcionālās specifikācijas, Komisija apspriežas ar MI padomi.
2. VIII pielikuma A un B iedaļā uzskaitītos datus ES datubāzē ievada nodrošinātājs vai attiecīgā gadījumā pilnvarotais pārstāvis.
3. VIII pielikuma C iedaļā uzskaitītos datus ES datubāzē ievada uzturētājs, kas ir publiska iestāde, aģentūra vai struktūra vai darbojas to vārdā, saskaņā ar 49. panta 3. un 4. punktu.
4. Izņemot sadaļu, kas minēta 49. panta 4. punktā un 60. panta 4. punkta c) apakšpunktā, ES datubāzē iekļauta informācija, kas reģistrēta saskaņā ar 49. pantu, ir pieklūstama un publiski pieejama lietotājam ērtā veidā. Informācijai vajadzētu būt viegli pārlūkojamai un mašīnlasāmai. Informācija, kas reģistrēta saskaņā ar 60. pantu, ir pieklūstama tikai tirgus uzraudzības iestādēm un Komisijai, ja vien potenciālais nodrošinātājs vai nodrošinātājs nav devis piekrišanu darīt šo informāciju pieejamu arī sabiedrībai.
5. ES datubāze satur personas datus tikai tik daudz, cik nepieciešams informācijas vākšanai un apstrādei saskaņā ar šo regulu. Minētajā informācijā iekļauj to fizisku personu vārdus un kontaktinformāciju, kuras atbild par sistēmas reģistrēšanu un kurām ir juridiskas pilnvaras pārstāvēt, attiecīgi, nodrošinātāju vai uzturētāju.

6. Komisija ir ES datubāzes pārzine. Tā nodrošinātājiem, potenciālajiem nodrošinātājiem un uzturētājiem dara pieejamu pienācīgu tehnisko un administratīvo atbalstu. ES datubāze atbilst piemērojamajām pieklūstamības prasībām.

IX NODAĻA

PĒCTIRGUS PĀRRAUDZĪBA, INFORMĀCIJAS KOPĪĢOŠANA UN TIRGUS UZRAUDZĪBA

1. IEDAĻA

Pēctirgus pārraudzība

72. pants

Nodrošinātāju veikta pēctirgus pārraudzība un augsta riska MI sistēmu pēctirgus pārraudzības plāns

1. Nodrošinātāji izveido un dokumentē pēctirgus pārraudzības sistēmu tādā veidā, kas ir samērīgs MI tehnoloģiju raksturam un augsta riska MI sistēmas riskiem.

2. Pēctirgus pārraudzības sistēma aktīvi un sistemātiski vāc, dokumentē un analizē attiecīgos datus, kurus var sniegt uzturētāji vai kurus var savākt, izmantojot citus avotus, par augsta riska MI sistēmu veiktspēju visā to darbības laikā, un kuri ļauj nodrošinātājam izvērtēt MI sistēmu nepārtrauktu atbilstību III nodaļas 2. iedaļā noteiktajām prasībām. Attiecīgā gadījumā pēctirgus pārraudzība ietver analīzi par mijiedarbību ar citām MI sistēmām. Šis pienākums neattiecas uz uzturētāju, kas ir tiesībsardzības iestādes, sensitīviem operatīvajiem datiem.

3. Pēctirgus pārraudzības sistēmas pamatā ir pēctirgus pārraudzības plāns. Pēctirgus pārraudzības plāns ir IV pielikumā minētās tehniskās dokumentācijas daļa. Komisija līdz 2026. gada 2. februārim pieņem īstenošanas aktu, ar ko nosaka sīki izstrādātus noteikumus, ar kuriem izveido pēctirgus pārraudzības plāna veidni un plānā iekļaujamo elementu sarakstu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

4. Augsta riska MI sistēmām, uz kurām attiecas I pielikuma A iedaļā minētie Savienības saskaņošanas tiesību akti, ja saskaņā ar minētajiem tiesību aktiem jau ir izveidota pēctirgus pārraudzības sistēma un plāns, lai nodrošinātu konsekvenci, izvairītos no dublēšanās un samazinātu papildu slogu, nodrošinātājiem ir izvēle attiecīgā gadījumā, izmantojot 3. punktā minēto veidni, integrēt vajadzīgos 1., 2. un 3. punktā aprakstītos elementus jau esošās sistēmās un plānos, kas paredzēti minētajos tiesību aktos, ar noteikumu, ka tā tiek panākts līdzvērtīgs aizsardzības līmenis.

Pirmo daļu piemēro arī III pielikuma 5. punktā minētajām augsta riska MI sistēmām, ko laiž tirgū vai nodod ekspluatācijā finanšu iestādes, uz kurām attiecas Savienības finanšu pakalpojumu jomas tiesību aktos noteiktās prasības par to iekšējo pārvaldību, kārtību vai procesiem.

2. IEDAĻA

Informācijas kopīgošana par nopietniem incidentiem

73. pants

Ziņošana par nopietniem incidentiem

1. Savienības tirgū laistu augsta riska MI sistēmu nodrošinātāji par visiem nopietniem incidentiem ziņo tirgus uzraudzības iestādēm dalībvalstīs, kur šis incidents noticis.

2. Šā panta 1. punktā minēto ziņojumu sniedz tūlīt pēc tam, kad nodrošinātājs ir konstatējis cēloņsakarību starp MI sistēmu un nopietno incidentu vai šādas sakarības saprātīgu iespējamību, un jebkurā gadījumā ne vēlāk kā 15 dienas pēc tam, kad nodrošinātājs vai, attiecīgā gadījumā, uzturētājs ir uzzinājis par nopietno incidentu.

Nosakot pirmajā daļā minēto ziņošanas laikposmu, ņem vērā to, cik smags ir nopietnais incidents.

3. Neraugoties uz šā panta 2. punktu, plašas ietekmes pārkāpuma vai 3. panta 49. punkta b) apakšpunktā definētā nopietna incidenta gadījumā šā panta 1. punktā minēto ziņojumu sniedz nekavējoties un ne vēlāk kā divas dienas pēc tam, kad nodrošinātājs vai, attiecīgā gadījumā, uzturētājs ir uzzinājis par minēto incidentu.

4. Neraugoties uz 2. punktu, personas nāves gadījumā ziņojumu sniedz nekavējoties pēc tam, kad nodrošinātājs vai uzturētājs ir noskaidrojis cēloņsakarību starp augsta riska MI sistēmu un nopietno incidentu, vai tiklīdz tam par to ir aizdomas, bet ne vēlāk kā 10 dienas pēc dienas, kurā nodrošinātājs vai, attiecīgā gadījumā, uzturētājs ir uzzinājis par nopietno incidentu.

5. Ja tas ir nepieciešams, lai nodrošinātu savlaicīgu ziņošanu, nodrošinātājs vai, attiecīgā gadījumā, uzturētājs var iesniegt sākotnēju ziņojumu, kurš nav pilnīgs un kuram seko pilnīgs ziņojums.

6. Pēc tam, kad ir ziņots par nopietnu incidentu, ievērojot 1. punktu, nodrošinātājs nekavējoties veic vajadzīgo izmeklēšanu saistībā ar šo nopietno incidentu un attiecīgo MI sistēmu. Tā ietver incidenta riska novērtējumu un korektīvu darbību.

Pirmajā daļā minētās izmeklēšanas laikā nodrošinātājs sadarbojas ar kompetentajām iestādēm un, attiecīgā gadījumā, ar attiecīgo paziņoto struktūru un neveic nekādu izmeklēšanu, kuras gaitā attiecīgā MI sistēma tiek mainīta tādā veidā, kas var ietekmēt šā incidenta cēloņu turpmāku izvērtēšanu, iekams par šādu darbību tas nav informējis kompetentās iestādes.

7. Saņēmusi paziņojumu par nopietnu incidentu, kas minēts 3. panta 49. punkta c) apakšpunktā, attiecīgā tirgus uzraudzības iestāde informē 77. panta 1. punktā minētās valsts publiskās iestādes vai struktūras. Komisija izstrādā īpašus norādījumus, lai veicinātu šā panta 1. punktā noteikto pienākumu izpildi. Minētos norādījumus izdod līdz 2025. gada 2. augustam, un tos regulāri novērtē.

8. Tirgus uzraudzības iestāde septiņu dienu laikā no dienas, kurā tā saņēmusi šā panta 1. punktā minēto paziņojumu, veic pienācīgus pasākumus, kā paredzēts Regulas (ES) 2019/1020 19. pantā, un izpilda minētajā regulā paredzētās paziņošanas procedūras.

9. III pielikumā minētajām augsta riska MI sistēmām, kuras laiž tirgū vai nodod ekspluatācijā nodrošinātāji, uz kuriem attiecas Savienības legislatīvie instrumenti, kas nosaka ziņošanas pienākumus, kuri ir līdzvērtīgi šajā regulā paredzētajiem, paziņošana par nopietniem incidentiem attiecas tikai uz tiem, kas minēti 3. panta 49. punkta c) apakšpunktā.

10. Augsta riska MI sistēmām, kas ir ierīču drošības sastāvdaļas vai pašas ir ierīces, uz ko attiecas Regulas (ES) 2017/745 un (ES) 2017/746, paziņošana par nopietniem incidentiem attiecas tikai uz gadījumiem, kas minēti šīs regulas 3. panta 49. punkta c) apakšpunktā, un paziņojumu nosūta valsts kompetentajai iestādei, ko šim nolūkam izvēlējušās dalībvalstis, kurās noticis minētais incidents.

11. Valsts kompetentās iestādes nekavējoties paziņo Komisijai par visiem nopietniem incidentiem neatkarīgi no tā, vai tās ir rīkojušās saistībā ar to vai nē, saskaņā ar Regulas (ES) 2019/1020 20. pantu.

3. IEDAĻA

Izpildes panākšana

74. pants

Tirgus uzraudzība un MI sistēmu kontrole Savienības tirgū

1. MI sistēmām, uz kurām attiecas šī regula, piemēro Regulu (ES) 2019/1020. Šīs regulas efektīvas izpildes nolūkos:

- a) atsaucies uz Regulas (ES) 2019/1020 terminu “uzņēmējs” saprot kā tādas, kas ietver visus šīs regulas 2. panta 1. punktā norādītos operatorus;
- b) atsaucies uz Regulā (ES) 2019/1020 lietoto apzīmējumu “produkts” saprot kā tādas, kas ietver visas MI sistēmas, uz kurām attiecas šī regula.

2. Pildot savus ziņošanas pienākumus, kas paredzēti Regulas (ES) 2019/1020 34. panta 4. punktā, tirgus uzraudzības iestādes katru gadu ziņo Komisijai un attiecīgajām valsts konkurences iestādēm visu tirgus uzraudzības darbībās identificēto informāciju, kas tās varētu interesēt Savienības konkurences tiesību normu piemērošanā. Tās arī katru gadu ziņo Komisijai par aizliegtas prakses izmantošanu, kas notikusi minētā gada laikā, un par veiktajiem pasākumiem.

3. Augsta riska MI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas I pielikuma A iedaļā uzskaitītie Savienības saskaņošanas tiesību akti, tirgus uzraudzības iestāde šīs regulas nolūkos ir saskaņā ar minētajiem tiesību aktiem izraudzītā iestāde, kas atbild par tirgus uzraudzības darbībām.

Atkāpjoties no pirmās daļas un pamatotos apstākļos dalībvalstis var izraudzīties citu attiecīgu iestādi, lai tā rīkotos kā tirgus uzraudzības iestāde, ar noteikumu, ka tās nodrošina koordināciju ar attiecīgajām nozares tirgus uzraudzības iestādēm, kas ir atbildīgas par I pielikumā uzskaitīto Savienības saskaņošanas tiesību aktu izpildes panākšanu.

4. Šīs regulas 79. līdz 83. pantā minētās procedūras nepiemēro MI sistēmām, kas saistītas ar produktiem, uz kuriem attiecas I pielikuma A iedaļā uzskaitītie Savienības saskaņošanas tiesību akti, ja šādos tiesību aktos jau ir paredzētas procedūras, kuras nodrošina līdzvērtīgu aizsardzības līmeni un kurām ir tāds pats mērķis. Šādos gadījumos tā vietā piemēro attiecīgās nozares procedūras.

5. Neskarot tirgus uzraudzības iestāžu pilnvaras, kas paredzētas Regulas (ES) 2019/1020 14. pantā, lai panāktu šīs regulas efektīvu izpildi, minētās Regulas 14. panta 4. punkta d) un j) apakšpunktā minētās tirgus uzraudzības iestādes pilnvaras attiecīgā gadījumā var īstenot attālināti.

6. Augsta riska MI 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 valsts iestāde, kas saskaņā ar minētajiem tiesību aktiem atbild par šo iestāžu finanšu uzraudzību, ciktāl MI sistēmas laišana tirgū, nodošana ekspluatācijā vai lietošana ir tieši saistīta ar minēto finanšu pakalpojumu sniegšanu.

7. Atkāpjoties no 6. punkta, attiecīgos apstākļos un ar noteikumu, ka tiek nodrošināta koordinācija, dalībvalsts šīs regulas nolūkos par tirgus uzraudzības iestādi var noteikt citu attiecīgu iestādi.

Valstu tirgus uzraudzības iestādēm, kas uzrauga regulētās kredītiestādes, kuras tiek regulētas saskaņā ar Direktīvu 2013/36/ES un kuras piedalās vienotajā uzraudzības mehānismā, kas izveidots ar Regulu (ES) Nr. 1024/2013, būtu nekavējoties jāziņo Eiropas Centrālajai bankai visa tirgus uzraudzības darbību gaitā identificētā informācija, kas varētu būt noderīga Eiropas Centrālās bankas prudenciālās uzraudzības uzdevumu veikšanai, kā norādīts minētajā regulā.

8. Augsta riska MI sistēmām, kas uzskaitītas šīs regulas III pielikuma 1. punktā, ciktāl šīs sistēmas izmanto tiesībaizsardzības nolūkos, robežpārvaldības un tiesiskuma un demokrātijas nolūkos, un augsta riska MI sistēmām, kas uzskaitītas III pielikuma 6., 7. un 8. punktā, dalībvalstis šīs regulas nolūkos par tirgus uzraudzības iestādēm izraugās vai nu kompetentās datu aizsardzības uzraudzības iestādes, kas paredzētas Regulā (ES) 2016/679 vai Direktīvā (ES) 2016/680, vai jebkuru citu iestādi, kas izraudzīta, ievērojot tos pašus nosacījumus, kas paredzēti Direktīvas (ES) 2016/680 41.–44. pantā. Tirgus uzraudzības darbības nekādā veidā neietekmē tiesu iestāžu neatkarību vai kā citādi neiejaucas to darbībā, kad tās rīkojas tiesu varas ietvaros.

9. Ja šīs regulas piemērošanas jomā ietilpst Savienības iestādes, struktūras, biroji vai aģentūras, kā to tirgus uzraudzības iestāde darbojas Eiropas Datu aizsardzības uzraudzītājs, izņemot attiecībā uz Eiropas Savienības Tiesu, kas rīkojas tiesu varas ietvaros.

10. Dalībvalstis atbalsta koordināciju starp tirgus uzraudzības iestādēm, kas izraudzītas saskaņā ar šo regulu, un citām attiecīgām valsts iestādēm vai struktūrām, kuras uzrauga I pielikumā uzskaitīto Savienības saskaņošanas tiesību aktu vai citu tādu Savienības tiesību aktu piemērošanu, kuri varētu būt svarīgi attiecībā uz III pielikumā minētajām augsta riska MI sistēmām.

11. Tirgus uzraudzības iestādes un Komisija spēj ierosināt jaunas darbības, tostarp kopīgas izmeklēšanas, kas jāveic tirgus uzraudzības iestādēm vai tirgus uzraudzības iestādēm kopā ar Komisiju, nolūkā veicināt atbilstību, konstatēt neatbilstību, uzlabot informētību vai sniegt norādījumus saistībā ar šo regulu attiecībā uz konkrētām augsta riska MI sistēmu kategorijām, par kurām konstatēts, ka tās rada nopietnu risku divās vai vairāk dalībvalstīs, saskaņā ar Regulas (ES) 2019/1020 9. pantu. MI birojs sniedz koordinācijas atbalstu kopīgām izmeklēšanām.

12. Neskarot Regulā (ES) 2019/1020 paredzētās pilnvaras, un attiecīgā gadījumā un tiktāl, ciktāl tas ir nepieciešams tirgus uzraudzības iestāžu uzdevumu izpildei, nodrošinātāji tām piešķir pilnīgu piekļuvi dokumentācijai, kā arī apmācības, validēšanas un testēšanas datu kopām, ko izmanto augsta riska MI sistēmu izstrādei, tostarp – attiecīgā gadījumā un ievērojot drošības aizsardzības pasākumus –, izmantojot lietojumprogrammu saskarnes (API) vai citus attiecīgus tehniskos līdzekļus un rīkus, kas nodrošina attālinātu piekļuvi.

13. Tirgus uzraudzības iestādēm piekļuvi augsta riska MI sistēmas pirmkodam piešķir pēc pamatota pieprasījuma un tikai tad, ja ir izpildīti abi šādi nosacījumi:

- a) piekļuve pirmkodam ir nepieciešama, lai novērtētu augsta riska MI sistēmas atbilstību III nodaļas 2. iedaļā noteiktajām prasībām; un
- b) testēšanas vai revīzijas procedūras un verifikācijas, kuru pamatā ir nodrošinātāja sniegtie dati un dokumentācija, ir izsmeltas vai izrādījušās nepietiekamas.

14. Ar informāciju vai dokumentāciju, ko ieguvušas tirgus uzraudzības iestādes, rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.

75. pants

Savstarpējā palīdzība, tirgus uzraudzība un vispārīga lietojuma MI sistēmu kontrole

1. Ja MI sistēmas pamatā ir vispārīga lietojuma MI modelis un modeli un sistēmu izstrādā tas pats nodrošinātājs, MI birojam ir pilnvaras pārraudzīt un uzraudzīt minētās MI sistēmas atbilstību šajā regulā paredzētajiem pienākumiem. Lai pildītu pārraudzības un uzraudzības uzdevumus, MI birojam ir tirgus uzraudzības iestādes pilnvaras, kas paredzētas šajā sadaļā un Regulā (ES) 2019/1020.

2. Ja attiecīgajām tirgus uzraudzības iestādēm ir pietiekams pamats uzskatīt, ka vispārīga lietojuma MI sistēmas, kuras uzturētāji var tieši lietot vismaz vienam nolūkam, kas, ievērojot šo regulu, ir klasificēts kā augsta riska, neatbilst šajā regulā noteiktajām prasībām, tās sadarbojas ar MI biroju, lai veiktu atbilstības izvērtējumus, un attiecīgi informē MI padomi un citas tirgus uzraudzības iestādes.

3. Ja tirgus uzraudzības iestāde nespēj pabeigt izmeklēšanu par augsta riska MI sistēmu, jo tā nespēj piekļūt konkrētai informācijai, kas saistīta ar MI modeli, neraugoties uz to, ka tā ir darījusi visu iespējamo, lai iegūtu minēto informāciju, tā var iesniegt pamatotu pieprasījumu MI birojam, kas panāk piekļuves nodrošināšanu minētajai informācijai. Minētajā gadījumā MI birojs nekavējoties un jebkurā gadījumā 30 dienu laikā sniedz pieprasījuma iesniedzējai iestādei jebkuru informāciju, ko MI birojs uzskata par būtisku, lai noteiktu, vai augsta riska MI sistēma ir neatbilstīga. Tirgus uzraudzības iestādes nodrošina iegūtās informācijas konfidencialitāti saskaņā ar šīs regulas 78. pantu. Regulas (ES) 2019/1020 VI nodaļā paredzēto procedūru piemēro *mutatis mutandis*.

76. pants

Testēšanas reālos apstākļos uzraudzība, ko veic tirgus uzraudzības iestādes

1. Tirgus uzraudzības iestādēm ir kompetences un pilnvaras nodrošināt, ka testēšana reālos apstākļos tiek veikta atbilstoši šai regulai.

2. Ja tiek veikta tādu MI sistēmu testēšana reālos apstākļos, kuras tiek uzraudzītas MI "regulatīvajā smilškastē", kā paredzēts 58. pantā, tirgus uzraudzības iestādes savas uzraudzības funkcijas ietvaros attiecībā uz MI "regulatīvo smilškastī" pārbauda atbilstību 60. pantam. Minētās iestādes attiecīgā gadījumā var atļaut nodrošinātājam vai potenciālajam nodrošinātājam veikt testēšanu reālos apstākļos, atkāpjoties no 60. panta 4. punkta f) un g) apakšpunktā paredzētajiem nosacījumiem.

3. Ja tirgus uzraudzības iestāde ir saņēmusi informāciju no potenciālā nodrošinātāja, nodrošinātāja vai jebkuras trešās personas par nopietnu incidentu, vai ja tai ir cits pamats uzskatīt, ka 60. un 61. pantā noteiktie nosacījumi netiek izpildīti, tā savā teritorijā attiecīgā gadījumā var pieņemt jebkuru no šādiem lēmumiem:

a) apturēt vai izbeigt testēšanu reālos apstākļos;

b) pieprasīt nodrošinātājam vai potenciālajam nodrošinātājam un uzturētājam vai potenciālajam uzturētājam modificēt jebkuru testēšanas reālos apstākļos aspektu.

4. Ja tirgus uzraudzības iestāde ir pieņēmusi šā panta 3. punktā minēto lēmumu vai ir cēlusi iebildumu 60. panta 4. punkta b) apakšpunkta nozīmē, lēmumā vai iebildumā norāda tā pamatojumu un to, kā nodrošinātājs vai potenciālais nodrošinātājs var apstrīdēt lēmumu vai iebildumu.

5. Attiecīgā gadījumā, ja tirgus uzraudzības iestāde ir pieņēmusi 3. punktā minēto lēmumu, tā dara zināmu tā pamatojumu citu dalībvalstu tirgus uzraudzības iestādēm, kurās MI sistēma ir testēta saskaņā ar testēšanas plānu.

77. pants

Pamattiesību aizsardzības iestāžu pilnvaras

1. Valstu publiskām iestādēm vai struktūrām, kas uzrauga vai panāk to pienākumu izpildi, kuri noteikti Savienības tiesību aktos, kas aizsargā pamattiesības, tostarp tiesības uz nediskriminēšanu, saistībā ar III pielikumā minēto augsta riska MI sistēmu lietošanu ir tiesības pieprasīt un piekļūt jebkurai dokumentācijai, kas sagatavota vai tiek uzturēta saskaņā ar šo regulu, piekļūstamā valodā un formātā, ja piekļuve minētajai dokumentācijai ir nepieciešama, lai efektīvi izpildītu to pilnvaras to jurisdikcijas robežās. Attiecīgā publiskā iestāde vai struktūra par tādu pieprasījumu informē attiecīgās dalībvalsts tirgus uzraudzības iestādi.

2. Līdz 2024. gada 2. novembrim katra dalībvalsts identificē 1. punktā minētās publiskās iestādes vai struktūras un šo sarakstu dara publiski pieejamu. Dalībvalstis sarakstu paziņo Komisijai un pārējām dalībvalstīm un to regulāri atjaunina.

3. Ja 1. punktā minētā dokumentācija nav pietiekama, lai noskaidrotu, vai ir notikusi tādu pienākumu neizpilde, kas noteikti Savienības tiesību aktos, kuri aizsargā pamattiesības, 1. punktā minētā publiskā iestāde vai struktūra tirgus uzraudzības iestādei var iesniegt pamatotu pieprasījumu organizēt augsta riska MI sistēmas testēšanu ar tehniskiem līdzekļiem. Tirgus uzraudzības iestāde saprātīgā laikposmā pēc pieprasījuma organizē testēšanu, cieši iesaistot pieprasījuma iesniedzēju publisku iestādi vai struktūru.

4. Ar informāciju vai dokumentāciju, ko, ievērojot šo pantu, ieguvušas 1. punktā minētās valsts publiskās iestādes vai struktūras, rīkojas saskaņā ar 78. pantā noteiktajiem konfidencialitātes pienākumiem.

78. pants

Konfidencialitāte

1. Komisija, tirgus uzraudzības iestādes un paziņotās struktūras un jebkura cita fiziska vai juridiska persona, kas iesaistīta šīs regulas piemērošanā, saskaņā ar Savienības vai valsts tiesību aktiem ievēro to uzdevumu un darbību izpildes gaitā iegūtās informācijas un datu konfidencialitāti tādā veidā, lai aizsargātu jo īpaši:

- a) fiziskas vai juridiskas personas intelektuālā īpašuma tiesības un konfidencialu uzņēmējdarbības informāciju vai komercnoslēpumus, ieskaitot pirmkodu, izņemot gadījumus, kas minēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/943 ⁽⁵⁷⁾ 5. pantā;
- b) šīs regulas efektīvu īstenošanu, jo īpaši pārbaužu, izmeklēšanas vai revīzijas nolūkos;
- c) sabiedrības un valsts drošības intereses;
- d) kriminālprocesu vai administratīvo procesu norisi;
- e) informāciju, kas klasificēta, ievērojot Savienības vai valsts tiesību aktus.

2. Iestādes, kas ir iesaistītas šīs regulas piemērošanā, ievērojot 1. punktu, pieprasa tikai tādus datus, kas ir absolūti nepieciešami MI sistēmu radītā riska novērtējumam un to pilnvaru īstenošanai saskaņā ar šo regulu un Regulu (ES) 2019/1020. Tās ievieš pienācīgus un efektīvus kibernetikas drošības pasākumus, lai aizsargātu iegūtās informācijas un datu drošību un konfidencialitāti, un dzēs savāktos datus, tiklīdz tie vairs nav vajadzīgi nolūkam, kādā tie tika iegūti, saskaņā ar piemērojamiem Savienības vai valsts tiesību aktiem.

3. Neskarot 1. un 2. punktu, informāciju, ar kuru konfidenciali apmainās valstu kompetentās iestādes savā starpā vai valstu kompetentās iestādes un Komisija, neizpauž bez iepriekšējas apspriešanās ar izcelsmes valsts kompetento iestādi un uzturētāju, ja III pielikuma 1., 6. vai 7. punktā minētās augsta riska MI sistēmas lieto tiesībaizsardzības, robežkontroles, imigrācijas vai patvēruma iestādes un ja šāda izpaušana apdraudētu sabiedrības un valsts drošības intereses. Šī informācijas apmaiņa neattiecas uz sensitīviem operatīvajiem datiem saistībā ar tiesībaizsardzības, robežkontroles, imigrācijas vai patvēruma iestāžu darbībām.

Ja tiesībaizsardzības, imigrācijas vai patvēruma iestādes ir III pielikuma 1., 6. vai 7. punktā minēto augsta riska MI sistēmu nodrošinātāji, IV pielikumā minētā tehniskā dokumentācija glabājas minēto iestāžu telpās. Minētās iestādes nodrošina, ka tirgus uzraudzības iestādes, kas attiecīgi minētas 74. panta 8. un 9. 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.

4. Šā panta 1., 2. un 3. punkts neietekmē Komisijas, dalībvalstu un to attiecīgo iestāžu, kā arī paziņoto struktūru tiesības un pienākumus attiecībā uz informācijas apmaiņu un brīdinājumu izplatīšanu, tostarp pārrobežu sadarbības kontekstā, kā arī neietekmē attiecīgo pušu pienākumus sniegt informāciju, kā paredzēts dalībvalstu krimināltiesībās.

5. Komisija un dalībvalstis var vajadzības gadījumā un saskaņā ar attiecīgajiem starptautisko un tirdzniecības nolīgumu noteikumiem 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.

79. pants

Valsts līmeņa procedūra rīcībai ar MI sistēmām, kas rada risku

1. MI sistēmas, kas rada risku, ir “produkts, kas rada risku”, kā definēts Regulas (ES) 2019/1020 3. panta 19. punktā, ciktāl tās rada risku personu veselībai vai drošībai, vai pamattiesībām.
2. Ja dalībvalsts tirgus uzraudzības iestādei ir pietiekams pamats uzskatīt, ka MI sistēma rada risku, kā minēts šā panta 1. punktā, tā veic attiecīgās MI sistēmas izvērtēšanu attiecībā uz tās atbilstību visām prasībām un pienākumiem, kas noteikti šajā regulā. Īpašu uzmanību pievērš MI sistēmām, kas rada risku neaizsargātām grupām. Ja ir identificēti riski pamattiesībām, tirgus uzraudzības iestāde informē arī attiecīgās publiskās iestādes vai struktūras, kas minētas 77. panta 1. punktā, un pilnībā sadarbojas ar tām. Attiecīgie operatori pēc vajadzības sadarbojas ar tirgus uzraudzības iestādi un ar citām 77. panta 1. punktā minētajām publiskām iestādēm vai struktūrām.

⁽⁵⁷⁾ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/943 (2016. gada 8. jūnijs) par zinātnības un darījumdarbības neizpaužamas informācijas (komercnoslēpumu) aizsardzību pret nelikumīgu iegūšanu, izmantošanu un izpaušanu (OV L 157, 15.6.2016., 1. lpp.).

Ja minētajā izvērtēšanā tirgus uzraudzības iestāde vai, attiecīgā gadījumā, tirgus uzraudzības iestāde sadarbībā ar valsts publisku iestādi, kas minēta 77. panta 1. punktā, konstatē, ka augsta riska MI sistēma neatbilst šajā regulā noteiktajām prasībām un pienākumiem, tā bez liekas kavēšanās pieprasa attiecīgajam operatoram veikt visas pienācīgās korektīvās darbības, lai panāktu MI sistēmas atbilstību, vai MI sistēmu izņemt no tirgus vai atsaukt termiņā, ko tirgus uzraudzības iestāde var noteikt, un jebkurā gadījumā ne vēlāk kā 15 darba dienu laikā vai, kā attiecīgi paredzēts piemērojamajos Savienības saskaņošanas tiesību aktos.

Tirgus uzraudzības iestāde attiecīgi informē attiecīgo paziņoto struktūru. Uz šā punkta otrajā daļā minētajiem pasākumiem attiecas Regulas (ES) 2019/1020 18. pants.

3. Ja tirgus uzraudzības iestāde uzskata, ka neatbilstība neaprobežojas tikai ar tās valsts teritoriju, tā bez liekas kavēšanās informē Komisiju un pārējās dalībvalstis par izvērtēšanas rezultātiem un par darbībām, ko tā operatoram pieprasījusi veikt.

4. Operators nodrošina, ka visas pienācīgās korektīvās darbības tiek veiktas attiecībā uz visām attiecīgajām MI sistēmām, kuras tas darījis pieejamas Savienības tirgū.

5. Ja MI sistēmas operators neveic pienācīgu korektīvu darbību 2. punktā minētajā termiņā, tirgus uzraudzības iestāde veic visus vajadzīgos provizoriskos pasākumus, lai aizliegtu vai ierobežotu to, ka MI sistēma tiek darīta pieejama tās valsts tirgū vai nodota ekspluatācijā, izņemtu produktu vai savrupo MI sistēmu no minētā tirgus vai atsauktu to. Minētā iestāde bez liekas kavēšanās paziņo Komisijai un pārējām dalībvalstīm par minētajiem pasākumiem.

6. Šā panta 5. punktā minētajā paziņojumā iekļauj visas pieejamās ziņas, jo īpaši informāciju, kas vajadzīga neatbilstīgās MI sistēmas identificēšanai, datus par MI sistēmas izcelsmi un piegādes ķēdi, norādītās iespējamās neatbilstības un saistītā riska raksturu, veikto valsts pasākumu raksturu un ilgumu, kā arī attiecīgā operatora izvirzītos argumentus. Tirgus uzraudzības iestādes jo īpaši norāda, vai neatbilstība ir saistīta ar vienu vai vairākiem šādiem aspektiem:

a) 5. pantā minētās MI prakses aizlieguma neievērošana;

b) augsta riska MI sistēmas neatbilstība III nodaļas 2. iedaļā noteiktajām prasībām;

c) trūkumi 40. un 41. pantā minētajos saskaņotajos standartos vai kopīgajās specifikācijās, uz kuru pamata piešķir pieņemumu par atbilstību;

d) neatbilstība 50. pantam.

7. Tirgus uzraudzības iestādes, kas nav procedūru sākušās dalībvalsts tirgus uzraudzības iestāde, bez liekas kavēšanās informē Komisiju un pārējās dalībvalstis par visiem pieņemtajiem pasākumiem un visu savā rīcībā esošo papildu informāciju par attiecīgās MI sistēmas neatbilstību un – ja tās nepiekrīt paziņotajam valsts pasākumam – informē par saviem iebildumiem.

8. Ja trīs mēnešu laikā no šā panta 5. punktā minētā paziņojuma saņemšanas ne kādas dalībvalsts tirgus uzraudzības iestāde, ne Komisija nav cēlusi iebildumus pret citas dalībvalsts tirgus uzraudzības iestādes veiktu provizorisku pasākumu, minēto pasākumu uzskata par pamatotu. Tas neskar attiecīgā operatora procesuālās tiesības saskaņā ar Regulas (ES) 2019/1020 18. pantu. Šīs regulas 5. pantā minētās MI prakses aizlieguma neievērošanas gadījumā šajā punktā minēto trīs mēnešu termiņu samazina līdz 30 dienām.

9. Tirgus uzraudzības iestādes nodrošina, ka attiecībā uz attiecīgo produktu vai MI sistēmu bez liekas kavēšanās tiek veikti pienācīgi ierobežojoši pasākumi, piemēram, produkta vai MI sistēmas izņemšana no to tirgus.

80. pants

Procedūra rīcībai ar MI sistēmām, ko nodrošinātājs, piemērojot III pielikumu, klasificējis kā tādas, kas nav augsta riska MI sistēmas

1. Ja tirgus uzraudzības iestādei ir pietiekams pamats uzskatīt, ka MI sistēma, ko nodrošinātājs, piemērojot 6. panta 3. punktu, klasificējis kā tādu, kas nav augsta riska MI sistēma, patiesībā ir augsta riska MI sistēma, tirgus uzraudzības iestāde veic attiecīgās MI sistēmas izvērtēšanu attiecībā uz tās klasificēšanu par augsta riska MI sistēmu, pamatojoties uz 6. panta 3. punktā izklāstītajiem nosacījumiem un Komisijas pamatnostādnēm.

2. Ja minētās izvērtēšanas gaitā tirgus uzraudzības iestāde konstatē, ka attiecīgā MI sistēma ir augsta riska sistēma, tā bez liekas kavēšanās pieprasa attiecīgajam nodrošinātājam veikt visas nepieciešamās darbības, lai panāktu MI sistēmas atbilstību šajā regulā noteiktajām prasībām un pienākumiem, kā arī veikt pienācīgas korektīvas darbības termiņā, kuru tirgus uzraudzības iestāde var noteikt.
3. Ja tirgus uzraudzības iestāde uzskata, ka attiecīgās MI sistēmas lietošana neaprobežojas tikai ar tās valsts teritoriju, tā bez liekas kavēšanās informē Komisiju un pārējās dalībvalstis par izvērtēšanas rezultātiem un par darbībām, ko tā nodrošinātājam pieprasījusi veikt.
4. Nodrošinātājs nodrošina, ka tiek veiktas visas nepieciešamās darbības, lai panāktu MI sistēmas atbilstību šajā regulā noteiktajām prasībām un pienākumiem. Ja attiecīgās MI sistēmas nodrošinātājs šā panta 2. punktā minētajā termiņā nenodrošina MI sistēmas atbilstību minētajām prasībām un pienākumiem, nodrošinātājam piemēro naudas sodus saskaņā ar 99. pantu.
5. Nodrošinātājs nodrošina, ka visas pienācīgās korektīvās darbības tiek veiktas attiecībā uz visām attiecīgajām MI sistēmām, kuras tas darījis pieejamas Savienības tirgū.
6. Ja attiecīgās MI sistēmas nodrošinātājs šā panta 2. punktā minētajā termiņā neveic pienācīgu korektīvo darbību, piemēro 79. panta 5.–9. punkta noteikumus.
7. Ja izvērtēšanas, ko veic, ievērojot šā panta 1. punktu, gaitā tirgus uzraudzības iestāde konstatē, ka nodrošinātājs ir nepareizi klasificējis MI sistēmu kā tādu, kas nav augsta riska MI sistēma, lai apietu III nodaļas 2. iedaļas prasību piemērošanu, nodrošinātājam piemēro naudas sodus saskaņā ar 99. pantu.
8. Īstenojot savas pilnvaras pārraudzīt šā panta piemērošanu un saskaņā ar Regulas (ES) 2019/1020 11. pantu tirgus uzraudzības iestādes var veikt pienācīgas pārbaudes, ņemot vērā jo īpaši informāciju, kas tiek glabāta šīs regulas 71. pantā minētajā ES datubāzē.

81. pants

Savienības drošības procedūra

1. Ja trīs mēnešu laikā pēc 79. panta 5. punktā minētā paziņojuma saņemšanas vai 30 dienu laikā, ja runa ir par 5. pantā minētās MI prakses aizlieguma neievērošanu, kādas dalībvalsts tirgus uzraudzības iestāde ceļ iebildumus pret citas dalībvalsts tirgus uzraudzības iestādes veiktu pasākumu vai ja Komisija uzskata, ka pasākums ir pretrunā Savienības tiesību aktiem, Komisija bez liekas kavēšanās uzsāk apspriešanos ar attiecīgās dalībvalsts tirgus uzraudzības iestādi un operatoru vai operatoriem un izvērtē valsts pasākumu. Pamatojoties uz minētā izvērtējuma rezultātiem, Komisija sešu mēnešu laikā pēc 79. panta 5. punktā minētā paziņojuma saņemšanas vai 60 dienu laikā pēc tās, ja runa ir par 5. pantā minētās MI prakses aizlieguma neievērošanu, izlemj, vai valsts pasākums ir pamatots, un šo lēmumu paziņo attiecīgās dalībvalsts tirgus uzraudzības iestādei. Komisija par savu lēmumu paziņo arī visām pārējām tirgus uzraudzības iestādēm.
2. Ja Komisija uzskata, ka attiecīgās dalībvalsts veiktais pasākums ir pamatots, visas dalībvalstis nodrošina, ka attiecībā uz attiecīgo MI sistēmu tās veic pienācīgus ierobežojošus pasākumus, piemēram, pieprasa MI sistēmas izņemšanu no to tirgus bez liekas kavēšanās, un attiecīgi informē Komisiju. Ja Komisija uzskata, ka valsts pasākums nav pamatots, attiecīgā dalībvalsts atceļ pasākumu un attiecīgi informē Komisiju.
3. Ja valsts pasākums tiek uzskatīts par pamatotu un MI sistēmas neatbilstība tiek saistīta ar trūkumiem šīs regulas 40. un 41. pantā minētajos saskaņotajos standartos vai kopīgajās specifikācijās, Komisija piemēro Regulas (ES) Nr. 1025/2012 11. pantā paredzēto procedūru.

82. pants

Atbilstīgas MI sistēmas, kas rada risku

1. Ja dalībvalsts tirgus uzraudzības iestāde pēc 79. pantā paredzētās izvērtēšanas, apspriedusies ar attiecīgo valsts publisko iestādi, kas minēta 77. panta 1. punktā, secina, ka augsta riska MI sistēma gan atbilst šai regulai, bet rada risku personu veselībai vai drošībai, pamattiesībām vai citiem sabiedrības interešu aizsardzības aspektiem, tā pieprasa attiecīgajam operatoram bez liekas kavēšanās termiņā, kuru tā var noteikt, veikt visus pienācīgos pasākumus, lai nodrošinātu, ka attiecīgā MI sistēma, kad tā tiek laista tirgū vai nodota ekspluatācijā, vairs nerada minēto risku.

2. Nodrošinātājs vai cits attiecīgs operators 1. punktā minētās dalībvalsts tirgus uzraudzības iestādes noteiktajā termiņā nodrošina, ka tiek veikta korektīva darbība attiecībā uz visām attiecīgajām MI sistēmām, kuras tas ir darījis pieejamas Savienības tirgū.
3. Dalībvalstis nekavējoties informē Komisiju un pārējās dalībvalstis par 1. punktā paredzēto secinājumu. Informācijā ietver visas pieejamās ziņas, jo īpaši datus, kas nepieciešami attiecīgās MI sistēmas identificēšanai, datus par MI sistēmas izcelsmi un piegādes ķēdi, saistītā riska raksturu un veikto valsts pasākumu raksturu un ilgumu.
4. Komisija bez liekas kavēšanās sāk apspriešanos ar attiecīgajām dalībvalstīm un attiecīgajiem operatoriem un izvērtē veiktos valsts pasākumus. Pamatojoties uz minētā izvērtējuma rezultātiem, Komisija pieņem lēmumu par to, vai pasākums ir pamatots, un vajadzības gadījumā ierosina citus pienācīgus pasākumus.
5. Komisija nekavējoties savu lēmumu dara zināmu attiecīgajām dalībvalstīm un attiecīgajiem operatoriem. Tā informē arī pārējās dalībvalstis.

83. pants

Formāla neatbilstība

1. Ja dalībvalsts tirgus uzraudzības iestāde nonāk pie kāda no turpmāk minētajiem konstatējumiem, tā pieprasa, lai attiecīgais nodrošinātājs novērst attiecīgo neatbilstību termiņā, kādu tā var noteikt:
 - a) CE zīme ir uzlikta, pārkāpjot 48. pantu;
 - b) CE zīme nav uzlikta;
 - c) nav sagatavota 47. pantā minētā ES atbilstības deklarācija;
 - d) 47. pantā minētā ES atbilstības deklarācija nav sagatavota pareizi;
 - e) nav veikta reģistrācija 71. pantā minētajā ES datubāzē;
 - f) attiecīgā gadījumā – nav iecelts pilnvarotais pārstāvis;
 - g) nav pieejama tehniskā dokumentācija.
2. Ja 1. punktā minētā neatbilstība netiek novērsta, attiecīgās dalībvalsts tirgus uzraudzības iestāde veic pienācīgus un samērīgus pasākumus, lai ierobežotu vai aizliegtu augsta riska MI sistēmu darīt pieejamu tirgū vai panāktu tās tūlītēju atsaukšanu vai izņemšanu no tirgus.

84. pants

Savienības MI testēšanas atbalsta struktūras

1. Komisija izraugās vienu vai vairākas Savienības MI testēšanas atbalsta struktūras Regulas (ES) 2019/1020 21. panta 6. punktā uzskaitīto uzdevumu veikšanai MI jomā.
2. Neskarot 1. punktā minētos uzdevumus, Savienības MI testēšanas atbalsta struktūras arī sniedz neatkarīgas tehniskas vai zinātniskas konsultācijas pēc MI padomes, Komisijas vai tirgus uzraudzības iestāžu lūguma.

4. IEDAĻA

Tiesību aizsardzība

85. pants

Tiesības iesniegt sūdzību tirgus uzraudzības iestādē

Neskarot citus tiesību aizsardzības līdzekļus administratīvā kārtā vai tiesā, jebkura fiziska vai juridiska persona, kurai ir pamats uzskatīt, ka ir pārkāpti šīs regulas noteikumi, var iesniegt sūdzības attiecīgajai tirgus uzraudzības iestādei.

Saskaņā ar Regulu (ES) 2019/1020 šādas sūdzības ņem vērā, lai veiktu tirgus uzraudzības darbības, un tās izskata, ievērojot īpašas procedūras, ko šajā nolūkā izstrādājušas tirgus uzraudzības iestādes.

86. pants

Tiesības saņemt skaidrojumu par individuālu lēmumu pieņemšanu

1. Jebkurai skartajai personai, uz kuru attiecas lēmums, ko uzturētājs pieņēmis, pamatojoties uz III pielikumā uzskaitītas augsta riska MI sistēmas iznākumu, izņemot tā 2. punktā uzskaitītās sistēmas, un kas rada juridiskas sekas vai līdzīgā veidā būtiski ietekmē minēto personu tādā veidā, ka tā uzskata, ka tas nelabvēlīgi ietekmē tās veselību, drošību vai pamattiesības, ir tiesības saņemt no uzturētāja skaidrus un jēgpilnus paskaidrojumus par MI sistēmas lomu lēmumu pieņemšanas procedūrā un pieņemtā lēmuma galvenajiem elementiem.

2. Šā panta 1. punktu nepiemēro tādu MI sistēmu lietošanai, attiecībā uz kurām izņēmumi no minētā punktā minētā pienākuma vai tā ierobežojumi izriet no Savienības vai valsts tiesību aktiem saskaņā ar Savienības tiesību aktiem.

3. Šo pantu piemēro tikai tiktāl, ciktāl 1. punktā minētās tiesības nav citādi paredzētas Savienības tiesību aktos.

87. pants

Ziņošana par pārkāpumiem un ziņojošo personu aizsardzība

Ziņošanai par šīs regulas pārkāpumiem un to personu aizsardzībai, kuras ziņo par šādiem pārkāpumiem, piemēro Direktīvu (ES) 2019/1937.

5. IEDAĻA

Uzraudzība, izmeklēšana, izpildes panākšana un pārraudzība attiecībā uz vispārīga lietojuma mi modeļu nodrošinātājiem

88. pants

Vispārīga lietojuma MI modeļu nodrošinātāju pienākumu izpildes panākšana

1. Komisijai ir ekskluzīvas pilnvaras uzraudzīt un panākt V nodaļas izpildi, ņemot vērā procesuālās garantijas, kas paredzētas 94. pantā. Komisija šo uzdevumu īstenošanu uztic MI birojam, neskarot Komisijas organizatoriskās pilnvaras un kompetenču sadalījumu starp dalībvalstīm un Savienību, pamatojoties uz Līgumiem.

2. Neskarot 75. panta 3. punktu, tirgus uzraudzības iestādes var lūgt Komisijai īstenot šajā nodaļā paredzētās pilnvaras, ja tas ir nepieciešams un samērīgi, lai palīdzētu tām pildīt šajā regulā noteiktos uzdevumus.

89. pants

Pārraudzības darbības

1. Lai MI birojs varētu veikt tam šajā iedaļā noteiktos uzdevumus, tas var veikt darbības, kas nepieciešamas, lai pārraudzītu, vai attiecīgie vispārīga lietojuma MI modeļu nodrošinātāji faktiski īsteno un ievēro šo regulu, tostarp, vai tie ievēro apstiprinātos prakses kodeksus.
2. Lejasposma nodrošinātājiem ir tiesības iesniegt sūdzību, apgalvojot, ka ir pārkāpta šī regula. Sūdzību pienācīgi pamato un tajā norāda vismaz:
 - a) attiecīgā vispārīga lietojuma MI modeļa nodrošinātāja kontaktpunktu;
 - b) attiecīgo faktu aprakstu, attiecīgos šīs regulas noteikumus un iemeslu, kādēļ lejasposma nodrošinātājs uzskata, ka attiecīgā vispārīga lietojuma MI modeļa nodrošinātājs ir pārkāpis šo regulu;
 - c) jebkādu citu informāciju, kuru lejasposma nodrošinātājs, kas nosūtījis pieprasījumu, uzskata par būtisku, attiecīgā gadījumā arī informāciju, kas savākta pēc paša iniciatīvas.

90. pants

Zinātniskās grupas brīdinājumi par sistēmiskiem riskiem

1. Zinātniskā grupa var iesniegt kvalificētu brīdinājumu MI birojam, ja tai ir pamats aizdomām, ka
 - a) vispārīga lietojuma MI modelis rada konkrētu identificējamu risku Savienības līmenī; vai
 - b) vispārīga lietojuma MI modelis atbilst 51. pantā minētajiem nosacījumiem.
2. Ja saņemts šāds kvalificēts brīdinājums, Komisija ar MI biroja starpniecību un pēc MI padomes informēšanas var īstenot šajā sadaļā noteiktās pilnvaras, lai novērtētu jautājumu. MI birojs informē MI padomi par visiem pasākumiem saskaņā ar 91.–94. pantu.
3. Kvalificētu brīdinājumu pienācīgi pamato un tajā norāda vismaz:
 - a) attiecīgā vispārīga lietojuma MI modeļa ar sistēmisku risku nodrošinātāja kontaktpunktu;
 - b) attiecīgo faktu aprakstu un zinātniskās grupas kvalificētā brīdinājuma pamatojumu;
 - c) jebkādu citu informāciju, kuru zinātniskā grupa uzskata par būtisku, attiecīgā gadījumā arī informāciju, kas savākta pēc pašu iniciatīvas.

91. pants

Pilnvaras pieprasīt dokumentāciju un informāciju

1. Komisija var pieprasīt attiecīgā vispārīga lietojuma MI modeļa nodrošinātājam iesniegt dokumentāciju, ko nodrošinātājs sagatavojis saskaņā ar 53. un 55. pantu, vai jebkādu papildu informāciju, kas vajadzīga, lai novērtētu nodrošinātāja atbilstību šai regulai.
2. Pirms informācijas pieprasījuma nosūtīšanas MI birojs var sākt strukturētu dialogu ar vispārīga lietojuma MI modeļa nodrošinātāju.
3. Pēc pienācīgi pamatota zinātniskās grupas pieprasījuma Komisija var izdot informācijas pieprasījumu vispārīga lietojuma MI modeļa nodrošinātājam, ja piekļuve informācijai ir nepieciešama un samērīga zinātniskās grupas uzdevumu izpildei saskaņā ar 68. panta 2. punktu.

4. Informācijas pieprasījumā norāda pieprasījuma juridisko pamatu un nolūku, konkrēti norādot, kāda informācija ir vajadzīga, nosaka termiņu, kurā informācija jāsniedz, un norāda 101. pantā paredzētos naudas sodus par nepareizas, nepilnīgas vai maldinošas informācijas sniegšanu.

5. Attiecīgā vispārīga lietojuma MI modeļa nodrošinātājs vai tā pārstāvis sniedz pieprasīto informāciju. Juridisku personu, uzņēmumu vai uzņēmēj sabiedrību gadījumā, vai, ja nodrošinātājs nav juridiska persona, pieprasīto informāciju attiecīgā vispārīga lietojuma MI modeļa nodrošinātāja vārdā sniedz personas, kas ir pilnvarotas tos pārstāvēt pēc likuma vai pēc to statūtiem. Juristi, kas ir pienācīgi pilnvaroti rīkoties, var sniegt informāciju savu klientu vārdā. Tomēr klienti ir pilnībā atbildīgi, ja sniegtā informācija ir nepilnīga, nepareiza vai maldinoša.

92. pants

Pilnvaras veikt izvērtēšanas

1. MI birojs pēc apspriešanās ar MI padomi var veikt attiecīgā vispārīga lietojuma MI modeļa izvērtēšanu, lai
 - a) novērtētu, kā nodrošinātājs ievēro šajā regulā noteiktos pienākumus, ja informācija, kas savākta, ievērojot 91. pantu, nav pietiekama; vai
 - b) izmeklētu vispārīga lietojuma MI modeļu ar sistēmiskiem riskiem radītos sistēmiskos riskus Savienības līmenī, jo īpaši pēc tam, kad zinātniskā grupa ir sniegusi kvalificētu brīdinājumu saskaņā ar 90. panta 1. punkta c) apakšpunktu.
2. Komisija var nolemt iecelt neatkarīgus ekspertus, lai tie veiktu izvērtēšanas tās vārdā, tostarp no zinātniskās grupas, kas izveidota, ievērojot 68. pantu. Šim uzdevumam ieceltie neatkarīgie eksperti atbilst 68. panta 2. punktā izklāstītajiem kritērijiem.
3. Šā panta 1. punkta nolūkos Komisija var pieprasīt piekļuvi attiecīgajam vispārīga lietojuma MI modelim, izmantojot API vai vēl citus piemērotus tehniskos līdzekļus un rīkus, tostarp pirmkodu.
4. Piekļuves pieprasījumā norāda pieprasījuma juridisko pamatu, nolūku un pamatojumu un nosaka termiņu, kurā piekļuve jāsniedz, kā arī 101. pantā paredzētos naudas sodus par piekļuves nesniegšanu.
5. Attiecīgā vispārīga lietojuma MI modeļa nodrošinātāji vai tā pārstāvis sniedz pieprasīto informāciju. Juridisku personu gadījumā, uzņēmēj sabiedrības vai uzņēmumi, vai – ja nodrošinātājs nav juridiska persona – personas, kas ir pilnvarotas tos pārstāvēt pēc likuma vai pēc to statūtiem, sniedz pieprasīto piekļuvi attiecīgā vispārīga lietojuma MI modeļa nodrošinātāja vārdā.
6. Komisija pieņem īstenošanas aktus, kuros nosaka izvērtēšanu detalizētu kārtību un nosacījumus, tostarp neatkarīgu ekspertu iesaistes detalizētu kārtību un to atlases procedūru. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.
7. Pirms pieprasīt piekļuvi attiecīgajam vispārīga lietojuma MI modelim, MI birojs var sākt strukturētu dialogu ar vispārīga lietojuma MI modeļa nodrošinātāju, lai savāktu vairāk informācijas par modeļa iekšējo testēšanu, iekšējiem aizsardzības pasākumiem sistēmisku risku novēršanai un citām iekšējām procedūrām un pasākumiem, ko nodrošinātājs ir veicis, lai mazinātu šādus riskus.

93. pants

Pilnvaras pieprasīt pasākumus

1. Vajadzības gadījumā un ja tas ir lietderīgi, Komisija var pieprasīt nodrošinātājiem
 - a) veikt pienācīgus pasākumus, lai izpildītu 53. un 54. pantā noteiktos pienākumus;

- b) īstenot riska mazināšanas pasākumus, ja izvērtējums, kas veikts saskaņā ar 92. pantu, ir raisījis nopietnas un pamatotas bažas par sistēmisku risku Savienības līmenī;
 - c) ierobežot to, ka modelis tiek darīts pieejams tirgū, izņemot to no tirgus vai atsaukt.
2. Pirms pasākuma pieprasīšanas MI birojs var sākt strukturētu dialogu ar vispārīga lietojuma MI modeļa nodrošinātāju.
3. Ja 2. punktā minētā strukturētā dialoga laikā vispārīga lietojuma MI modeļa ar sistēmisku risku nodrošinātājs piedāvā saistības nolūkā īstenot riska mazināšanas pasākumus, lai novērstu sistēmisku risku Savienības līmenī, Komisija ar lēmumu var tādas saistības padarīt saistošas un paziņot, ka vairs nav pamata rīcībai.

94. pants

Vispārīga lietojuma MI modeļa uzņēmēju procesuālās tiesības

Vispārīga lietojuma MI modeļa nodrošinātājiem *mutatis mutandis* piemēro Regulas (ES) 2019/1020 18. pantu, neskarot konkrētākas procesuālās tiesības, kas paredzētas šajā regulā.

X NODAĻA

RĪCĪBAS KODEKSI UN PAMATNOSTĀDNES

95. pants

Rīcības kodeksi attiecībā uz konkrētu prasību brīvprātīgu piemērošanu

1. MI birojs un dalībvalstis rosina un sekmē tādu rīcības kodeksu, tostarp saistītu pārvaldības mehānismu, izstrādi, kuru mērķis ir veicināt dažu vai visu šīs regulas III nodaļas 2. iedaļā noteikto prasību brīvprātīgu piemērošanu MI sistēmām, kas nav augsta riska MI sistēmas, ņemot vērā pieejamos tehniskos risinājumus un nozares paraugpraksi, kas nodrošina iespēju piemērot šādas prasības.
2. MI birojs un dalībvalstis sekmē rīcības kodeksu izstrādi attiecībā uz konkrētu prasību brīvprātīgu piemērošanu visām MI sistēmām, tostarp no uzturētāju puses, pamatojoties uz skaidriem mērķiem un galvenajiem snieguma rādītājiem, lai izmērītu minēto mērķu sasniegšanu, tostarp šādus elementus, bet ne tikai:
- a) piemērojamie elementi, kas paredzēti Savienības ētikas vadlīnijās uzticamam MI;
 - b) MI sistēmu ietekmes uz vides ilgtspēju novērtēšana un mazināšana, tostarp attiecībā uz energoefektīvu plānošanu un MI efektīvas projektēšanas, apmācības un lietošanas metodēm;
 - c) MI pratības veicināšana, jo īpaši to personu, kas nodarbojas ar MI izstrādi, darbināšanu un lietošanu;
 - d) iekļaujošas un daudzveidīgas MI sistēmu projektēšanas sekmēšana, tostarp ar iekļaujošu un daudzveidīgu izstrādes komandu izveidi un ieinteresēto personu dalības veicināšanu minētajā procesā;
 - e) MI sistēmu nelabvēlīgās ietekmes uz neaizsargātām personām vai neaizsargātu personu grupām novērtēšana un novēršana, tostarp attiecībā uz personu ar invaliditāti piekļuves iespējām, kā arī uz dzimumu līdztiesību.
3. Rīcības kodeksus var izstrādāt atsevišķi MI sistēmu nodrošinātāji vai uzturētāji vai organizācijas, kas tos pārstāv, vai abēji, arī – iesaistot ieinteresētās personas un viņus pārstāvošās organizācijas, tostarp pilsoniskās sabiedrības organizācijas un akadēmiskās aprindas. Rīcības kodeksi var aptvert vienu vai vairākas MI sistēmas, ņemot vērā attiecīgajām sistēmām paredzētā nolūka līdzību.
4. Rosinot un sekmējot rīcības kodeksu izstrādi, MI birojs un dalībvalstis ņem vērā MVU, tostarp jaunuzņēmumu, konkrētās intereses un vajadzības.

96. pants

Komisijas pamatnostādnes par šīs regulas īstenošanu

1. Komisija izstrādā pamatnostādnes par šīs regulas praktisko īstenošanu un jo īpaši par:
 - a) 8. līdz 15. pantā un 25. pantā minēto prasību un pienākumu piemērošanu;
 - b) 5. pantā minēto aizliegto praksi;
 - c) to noteikumu praktisko īstenošanu, kas saistīti ar būtisku modifikāciju;
 - d) 50. pantā noteikto pārredzamības pienākumu praktisko īstenošanu;
 - e) sīku informāciju par šīs regulas saistību ar I pielikumā uzskaitītajiem Savienības saskaņošanas tiesību aktiem, kā arī citiem attiecīgiem Savienības tiesību aktiem, tostarp par to izpildes panākšanas saskaņību;
 - f) 3. panta 1. punktā sniegtās MI sistēmas definīcijas piemērošanu.

Izdodot šādas pamatnostādnes, Komisija īpašu uzmanību pievērš MVU, tostarp jaunuzņēmumu, vietējo publisko iestāžu un to nozaru vajadzībām, kuras, visticamāk, skars šī regula.

Šā punkta pirmajā daļā minētajās pamatnostādnēs pienācīgi ņem vērā vispāratzītos jaunākos sasniegumus MI jomā, kā arī 40. un 41. pantā minētos saskaņotos standartus un kopīgās specifikācijas vai tos saskaņotos standartus vai tehniskās specifikācijas, kas noteikti, ievērojot Savienības saskaņošanas tiesību aktus.

2. Pēc dalībvalstu vai MI biroja pieprasījuma vai pēc savas iniciatīvas Komisija vajadzības gadījumā atjaunina iepriekš pieņemtas pamatnostādnes.

XI NODAĻA

PILNVARU DELEĢĒŠANA UN KOMITEJU PROCEDŪRA

97. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā paredzētos nosacījumus.
2. Pilnvaras pieņemt 6. panta 6. un 7. punktā, 7. panta 1. un 3. punktā, 11. panta 3. punktā, 43. panta 5. un 6. punktā, 47. panta 5. punktā, 51. panta 3. punktā, 52. panta 4. punktā un 53. panta 5. un 6. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no 2024. gada 1. augusta. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.
3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 6. panta 6. un 7. punktā, 7. panta 1. un 3. punktā, 11. panta 3. punktā, 43. panta 5. un 6. punktā, 47. panta 5. punktā, 51. panta 3. punktā, 52. panta 4. punktā un 53. panta 5. un 6. punktā minēto pilnvaru deleģēšanu. 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. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar katras dalībvalsts ieceltajiem ekspertiem saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz Komisija pieņem deleģētu aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.
6. Saskaņā ar 6. panta 6. un 7. punktu, 7. panta 1. un 3. punktu, 11. panta 3. punktu, 43. panta 5. vai 6. punktu, 47. panta 5. punktu, 51. panta 3. punktu, 52. panta 4. punktu vai 53. panta 5. vai 6. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja trīs mēnešos no dienas, kad minētais akts paziņots 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.

98. 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 NODAĻA

SODI

99. pants

Sodi

1. Saskaņā ar šīs regulas noteikumiem dalībvalstis nosaka noteikumus par sodiem un citiem izpildes panākšanas pasākumiem – kuri var ietvert arī brīdinājumus un nemonētārus pasākumus –, kas piemērojami par operatoru izdarītiem šīs regulas pārkāpumiem, un veic visus nepieciešamos pasākumus, lai nodrošinātu, ka tie tiek īstenoti pareizi un efektīvi un ņemot vērā norādījumus, ko Komisija izdevusi, ievērojot 96. pantu. Paredzētie sodi ir iedarbīgi, samērīgi un atturoši. Tajos ņem vērā MVU, tostarp jaunuzņēmumu, intereses un to ekonomisko dzīvotspēju.
2. Dalībvalstis nekavējoties un vēlākais līdz piemērošanas sākuma dienai paziņo Komisijai par 1. punktā minētajiem noteikumiem par sodiem un citiem izpildes panākšanas pasākumiem un nekavējoties paziņo tai par visiem to turpmākiem grozījumiem.
3. Par 5. pantā minētās MI prakses aizlieguma neievērošanu piemēro administratīvos naudas sodus līdz 35 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 7 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kurš no tiem ir lielāks.
4. Par neatbilstību kādam no turpmāk uzskaitītajiem noteikumiem, kas attiecas uz operatoriem vai paziņotajām struktūrām, atskaitot tos, kas noteikti 5. pantā, piemēro administratīvos naudas sodus līdz 15 000 000 EUR apmērā vai, ja pārkāpējs ir uzņēmums, līdz 3 % apmērā no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kurš no tiem ir lielāks:
- a) nodrošinātāju pienākumi, ievērojot 16. pantu;
 - b) pilnvaroto pārstāvju pienākumi, ievērojot 22. pantu;
 - c) importētāju pienākumi, ievērojot 23. pantu;
 - d) izplatītāju pienākumi, ievērojot 24. pantu;
 - e) uzturētāju pienākumi, ievērojot 26. pantu;
 - f) prasības attiecībā uz paziņotajām struktūrām un to pienākumi saskaņā ar 31. pantu, 33. panta 1., 3. un 4. punktu vai 34. pantu;
 - g) pārredzamības pienākumi attiecībā uz nodrošinātājiem un uzturētājiem, ievērojot 50. pantu.

5. Par nepareizas, nepilnīgas vai maldinošas informācijas sniegšanu paziņotajām struktūrām un valsts kompetentajām iestādēm atbildē uz pieprasījumu piemēro administratīvos naudas sodus līdz 7 500 000 EUR apmērā vai, ja pārkāpējs ir uzņēmums, līdz 1 % apmērā no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kurš no tiem ir lielāks.
6. MVU, tostarp jaunuzņēmumu, gadījumā katrs šajā pantā minētais naudas sods ir līdz procentuālajam apmēram vai apmēram, kas minēts 3., 4. un 5. punktā, atkarībā no tā, kurš no tiem ir mazāks.
7. Lemjot par to, vai piemērot administratīvo naudas sodu, un lemjot par administratīvā naudas soda apmēru, katrā atsevišķā gadījumā ņem vērā visus attiecīgos konkrētās situācijas apstākļus un, attiecīgā gadījumā, izvērtē šādus elementus:
- a) pārkāpuma un tā seku raksturs, smagums un ilgums, ņemot vērā MI sistēmas nolūku, kā arī, attiecīgā gadījumā, skarto personu skaits un tām nodarītā kaitējuma apmērs;
 - b) vai citas tirgus uzraudzības iestādes jau ir piemērojušas administratīvos naudas sodus tam pašam operatoram par to pašu pārkāpumu;
 - c) vai citas iestādes tam pašam operatoram jau ir piemērojušas administratīvos naudas sodus par citu Savienības vai valsts tiesību aktu pārkāpumiem, ja šādu pārkāpumu pamatā ir tā pati darbība vai bezdarbība, kas ir attiecīgs šīs regulas pārkāpums;
 - d) operatora, kurš izdarījis pārkāpumu, lielums, gada apgrozījums un tirgus daļa;
 - e) jebkāds cits pastiprinošs vai mīkstinošs apstāklis, kas piemērojams lietas apstākļiem, piemēram, no pārkāpuma tieši vai netieši gūti finansiālie labumi vai novērsti zaudējumi;
 - f) pakāpe, kādā notiek sadarbība ar valstu kompetentajām iestādēm, lai novērstu pārkāpumu un mazinātu tā iespējamās nelabvēlīgās sekas;
 - g) operatora atbildības pakāpe, ņemot vērā tā īstenotos tehniskos un organizatoriskos pasākumus;
 - h) veids, kādā par pārkāpumu ir uzzinājušas valsts kompetentās iestādes, jo īpaši to, vai operators ir ziņojis par pārkāpumu, un, ja ir, – kādā mērā;
 - i) vai pārkāpums izdarīts tīši vai nolaidības dēļ;
 - j) visas darbības, ko operators veicis, lai mazinātu skartajām personām nodarīto kaitējumu.
8. Katra dalībvalsts paredz noteikumus par to, kādā mērā administratīvos naudas sodus var uzlikt publiskām iestādēm un struktūrām, kas izveidotas minētajā dalībvalstī.
9. Atkarībā no dalībvalstu tiesību sistēmas noteikumus par administratīvajiem naudas sodiem var piemērot tādā veidā, ka naudas sodus uzliek, attiecīgi, kompetentās valsts tiesas vai citas struktūras minētajās dalībvalstīs. Šādu noteikumu piemērošanai minētajās dalībvalstīs ir līdzvērtīga ietekme.
10. Šajā pantā paredzēto pilnvaru izmantošanai piemēro atbilstošas procesuālas garantijas saskaņā ar Savienības un valsts tiesību aktiem, tostarp efektīvu tiesību aizsardzību tiesā un pienācīgu procesu.
11. Dalībvalstis katru gadu ziņo Komisijai par administratīvajiem naudas sodiem, ko tās attiecīgajā gadā ir noteikušas, saskaņā ar šo pantu, un par visām saistītajām tiesvedībām vai tiesas procesiem.

100. pants

Administratīvie naudas sodi Savienības iestādēm, struktūrām, birojiem un aģentūrām

1. Eiropas Datu aizsardzības uzraudzītājs var uzlikt administratīvus naudas sodus Savienības iestādēm, struktūrām, birojiem un aģentūrām, uz ko attiecas šī regula. Lemjot par to, vai piemērot administratīvo naudas sodu, un lemjot par administratīvā naudas soda apmēru, katrā atsevišķā gadījumā ņem vērā visus attiecīgos konkrētās situācijas apstākļus un rūpīgi izvērtē šādus elementus:

- a) pārkāpuma un tā seku raksturs, smagums un ilgums, pārkāpuma un tā seku raksturs, smagums un ilgums, ņemot vērā attiecīgajai MI sistēmai paredzēto nolūku, kā arī attiecīgā gadījumā skarto personu skaits un tām nodarītā kaitējuma apmērs;
- b) Savienības iestādes, struktūras, biroja vai aģentūras atbildības pakāpe, ņemot vērā to īstenotos tehniskos un organizatoriskos pasākumus;
- c) visas darbības, ko Savienības iestāde, struktūra, birojs vai aģentūra veikusi, lai mazinātu skartajām personām nodarīto kaitējumu;
- d) sadarbības pakāpe 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, struktūrai, birojam vai aģentūrai tajā pašā jautājumā;
- e) līdzīgi agrāki Savienības iestādes, struktūras, biroja vai aģentūras pārkāpumi;
- f) veids, kādā par pārkāpumu uzzināja Eiropas datu aizsardzības uzraudzītājs, jo īpaši, vai Savienības iestāde, struktūra, birojs vai aģentūra ir ziņojusi par pārkāpumu, un šādā gadījumā – kādā apjomā;
- g) Savienības iestādes, struktūras, biroja vai aģentūras gada budžets.

2. Par 5. pantā minētās MI prakses aizlieguma neievērošanu piemēro administratīvos naudas sodus līdz 1 500 000 EUR apmērā.

3. Par MI sistēmas neatbilstību šajā regulā noteiktajām prasībām vai pienākumiem, atskaitot tos, kas noteikti 5. pantā, piemēro administratīvos naudas sodus līdz 750 000 EUR apmērā.

4. Pirms lēmumu pieņemšanas saskaņā ar šo pantu Eiropas Datu aizsardzības uzraudzītājs dod Savienības iestādei, struktūrai, birojam vai aģentūrai, kas 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 individu vai uzņēmumu likumīgās intereses to personas datu vai uzņēmējdarbības noslēpumu aizsardzībā.

6. Līdzekļus, kas iegūti, uzliekot naudas sodus saskaņā ar šo pantu, iemaksā Savienības vispārējā budžetā. Naudas sodi neietekmē sodītās Savienības iestādes, struktūras, biroja vai aģentūras efektīvu darbību.

7. Eiropas Datu aizsardzības uzraudzītājs katru gadu paziņo Komisijai par administratīvajiem naudas sodiem, ko tas uzlicis, ievērojot šo pantu, un tiesvedībām un tiesas procesiem, ko tas ierosinājis.

101. pants

Vispārīga lietojuma MI modeļu nodrošinātājiem piemērojami naudas sodi

1. Komisija var uzlikt vispārīga lietojuma MI modeļu nodrošinātājiem naudas sodus, kas nepārsniedz 3 % no to kopējā gada globālā apgrozījuma iepriekšējā finanšu gadā vai 15 000 000 EUR, atkarībā no tā, kura summa ir lielāka, ja Komisija konstatē, ka nodrošinātājs tiši vai nolaidības dēļ:

- a) ir pārkāpis attiecīgos šīs regulas noteikumus;
- b) nav pildījis dokumenta vai informācijas pieprasījumu, kas paredzēts 91. pantā, vai ir sniedzis nepareizu, nepilnīgu vai maldinošu informāciju;
- c) nav pildījis pasākumu, kas pieprasīts saskaņā ar 93. pantu;

- d) nav darījis Komisijai pieejamu piekļuvi vispārīga lietojuma MI modelim vai vispārīga lietojuma MI modelim ar sistēmisku risku nolūkā veikt izvērtēšanu, ievērojot 92. pantu.

Nosakot naudas soda vai periodiskā soda maksājuma apmēru, ņem vērā pārkāpuma raksturu, smagumu un ilgumu, pienācīgi ievērojot samērīguma un piemērotības principus. Komisija ņem vērā arī saistības saskaņā ar 93. panta 3. punktu vai saistības attiecīgajos prakses kodeksos saskaņā ar 56. pantu.

2. Pirms pieņemt lēmumu, ievērojot 1. punktu, Komisija savus sākotnējos konstatējumus paziņo vispārīga lietojuma MI modeļa nodrošinātājam un dod tam iespēju tikt uzklaustītam.
3. Saskaņā ar šo pantu uzliktie naudas sodi ir iedarbīgi, samērīgi un atturoši.
4. Informāciju par naudas sodiem, kas uzlikti saskaņā ar šo pantu, attiecīgā gadījumā dara zināmu arī MI padomei.
5. Eiropas Savienības Tiesai ir neierobežota jurisdikcija pārskatīt Komisijas lēmumus, ar kuriem nosaka šajā pantā paredzēto naudas sodu. Tā var atcelt, samazināt vai palielināt uzlikto naudas sodu.
6. Komisija pieņem īstenošanas aktus, kuros ietver sīki izstrādātu procesuālo kārtību un procesuālajām garantijām attiecībā uz iespējamu lēmumu pieņemšanu, ievērojot šā panta 1. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 98. panta 2. punktā.

XIII NODAĻA

NOBEIGUMA NOTEIKUMI

102. pants

Grozījums Regulā (EK) Nr. 300/2008

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

“Pieņemot sīki izstrādātus pasākumus, kas attiecas uz drošības iekārtu tehnisko raksturojumu un to apstiprināšanas un lietošanas procedūrām, kuras attiecas uz mākslīgā intelekta sistēmām Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

103. pants

Grozījums Regulā (ES) Nr. 167/2013

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

“Kad tiek pieņemti deleģētie akti, ievērojot pirmo daļu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

104. pants

Grozījums Regulā (ES) Nr. 168/2013

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

“Kad tiek pieņemti deleģētie akti, ievērojot pirmo daļu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

105. pants

Grozījums Direktīvā 2014/90/ES

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

“5. Attiecībā uz mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, kad tiek veiktas darbības, ievērojot 1. punktu, un tiek pieņemtas tehniskās specifikācijas un testēšanas standarti saskaņā ar 2. un 3. punktu, Komisija ņem vērā prasības, kas noteiktas minētās regulas III nodaļas 2. iedaļā.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

106. pants

Grozījums Direktīvā (ES) 2016/797

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

“12. Kad tiek pieņemti deleģētie akti, ievērojot 1. punktu, un īstenošanas akti, ievērojot 11. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

107. pants

Grozījumi Regulā (ES) 2018/858

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

“4. Kad tiek pieņemti deleģētie akti, ievērojot 3. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

108. pants

Grozījumi Regulā (ES) 2018/1139

Regulu (ES) 2018/1139 groza šādi:

1) regulas 17. pantam pievieno šādu punktu:

“3. Neskarot 2. punktu, kad tiek pieņemti īstenošanas akti, ievērojot 1. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”;

2) regulas 19. pantam pievieno šādu punktu:

“4. Kad tiek pieņemti deleģētie akti, ievērojot 1. un 2. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) 2024/1689 nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.”;

3) regulas 43. pantam pievieno šādu punktu:

“4. Kad tiek pieņemti īstenošanas akti, ievērojot 1. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) 2024/1689 nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.”;

4) regulas 47. pantam pievieno šādu punktu:

“3. Kad tiek pieņemti deleģētie akti, ievērojot 1. un 2. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) 2024/1689 nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.”;

5) regulas 57. pantam pievieno šādu punktu:

“Pieņemot minētos īstenošanas aktus par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) 2024/1689 nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.”;

6) regulas 58. pantam pievieno šādu punktu:

“3. Kad tiek pieņemti deleģētie akti, ievērojot 1. un 2. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Regulas (ES) 2024/1689 nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.”

109. pants

Grozījumi Regulā (ES) 2019/2144

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

“3. Kad tiek pieņemti īstenošanas akti, ievērojot 2. punktu, par mākslīgā intelekta sistēmām, kas ir drošības sastāvdaļas Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689 (*) nozīmē, ņem vērā minētās regulas III nodaļas 2. iedaļā noteiktās prasības.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

110. pants

Grozījums Direktīvā (ES) 2020/1828

Eiropas Parlamenta un Padomes Direktīvas (ES) 2020/1828 ⁽⁵⁸⁾ I pielikumā pievieno šādu punktu:

“68) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”

111. pants

MI sistēmas, kas jau ir laistas tirgū vai nodotas ekspluatācijā un vispārēja lietojuma AI modeļi, kas jau laisti tirgū

1. Neskarot 5. panta piemērošanu, kā minēts 113. panta 3. punkta a) apakšpunktā, to MI sistēmu, kas ir tādu lielapjoma IT sistēmu sastāvdaļas, kuras izveidotas ar X pielikumā uzskaitītajiem tiesību aktiem, un kas ir laistas tirgū vai nodotas ekspluatācijā pirms 2027. gada 2. augusta, atbilstību šai regulai panāk līdz 2030. gada 31. decembrim.

Šajā regulā noteiktās prasības ņem vērā katras ar X pielikumā uzskaitītajiem tiesību aktiem izveidotās lielapjoma IT sistēmas izvērtēšanā, kas jāveic, kā paredzēts minētajos tiesību aktos un ja minētie tiesību akti tiek aizstāti vai grozīti.

2. Neskarot 5. panta piemērošanu, kā minēts 113. panta 3. punkta a) apakšpunktā, uz to augsta riska MI sistēmu operatoriem, kuras ir laistas tirgū vai nodotas ekspluatācijā pirms 2026. gada 2. augusta, atskaitot šā panta 1. punktā minētās, šī regula attiecas tikai tad, ja no minētā datuma šajās sistēmās notikušas būtiskas izmaiņas to uzbūvē. Jebkurā gadījumā augsta riska MI sistēmu, kas paredzētas publisko iestāžu lietošanai, nodrošinātāji un uzturētāji veic nepieciešamos pasākumus, lai izpildītu šīs regulas prasības un pienākumus līdz 2030. gada 2. augustam.

3. To vispārīga lietojuma MI modeļu nodrošinātāji, kuri laisti tirgū pirms 2025. gada 2. augusta, veic nepieciešamos pasākumus, lai izpildītu šajā regulā noteiktos pienākumus līdz 2027. gada 2. augustam.

(⁵⁸) Eiropas Parlamenta un Padomes Direktīva (ES) 2020/1828 (2020. gada 25. novembris) par pārstāvības prasībām patērētāju kolektīvo interešu aizsardzībai un ar ko atceļ Direktīvu 2009/22/EK (OV L 409, 4.12.2020., 1. lpp.).

112. pants

Izvērtēšana un pārskatīšana

1. Reizi gadā pēc šīs regulas stāšanās spēkā un līdz 97. pantā noteiktā pilnvaru deleģēšanas laikposma beigām Komisija novērtē nepieciešamību grozīt III pielikuma sarakstu un 5. pantā paredzēto aizliegtās MI prakses sarakstu. Minētās novērtēšanas konstatējumus Komisija iesniedz Eiropas Parlamentam un Padomei.
2. Līdz 2028. gada 2. augustam un pēc tam reizi četros gados Komisija izvērtē un ziņo Eiropas Parlamentam un Padomei par:
 - a) nepieciešamību pēc grozījumiem nolūkā paplašināt esošās jomu kategorijas vai pievienot jaunas jomu kategorijas III pielikumā;
 - b) grozījumiem MI sistēmu sarakstā, attiecībā uz kurām vajadzīgi papildu pārredzamības pasākumi 50. pantā;
 - c) grozījumiem nolūkā stiprināt uzraudzības un pārvaldības sistēmas efektivitāti.
3. Līdz 2029. gada 2. augustam un pēc tam reizi četros gados Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu. Ziņojumā ietver novērtējumu attiecībā uz izpildes panākšanas struktūru un iespējamu vajadzību pēc Savienības aģentūras visu apzināto trūkumu novēršanai. Pamatojoties uz konstatējumiem, minētajam ziņojumam attiecīgā gadījumā pievieno priekšlikumu šīs regulas grozījumiem. Šos ziņojumus publicē.
4. Ziņojumos, kas minēti 2. punktā, īpašu uzmanību pievērš šādiem jautājumiem:
 - a) to valstu kompetento iestāžu finanšu, tehnisko un cilvēkresursu statuss, kas vajadzīgi, lai efektīvi veiktu uzdevumus, kuri tam uzticēti saskaņā ar šo regulu;
 - b) situācija saistībā ar sodiem, jo īpaši administratīvajiem naudas sodiem, kā minēts 99. panta 1. punktā, kurus dalībvalstis piemēro par šīs regulas noteikumu pārkāpumiem;
 - c) pieņemtie saskaņotie standarti un kopīgās specifikācijas, kas izstrādātas šīs regulas atbalstam;
 - d) to uzņēmumu skaits, kas ienāk tirgū pēc šīs regulas piemērošanas sākuma, un cik daudz no tiem ir MVU.
5. Līdz 2028. gada 2. augustam Komisija izvērtē MI biroja darbību, to, vai MI birojam ir piešķirtas pietiekamas pilnvaras un kompetences, lai tas varētu pildīt savus uzdevumus, un vai šīs regulas pienācīgai īstenošanai un izpildes panākšanai būtu svarīgi un nepieciešami uzlabot MI biroju un tā izpildes panākšanas kompetences un palielināt tā resursus. Komisija iesniedz izvērtējuma ziņojumu Eiropas Parlamentam un Padomei.
6. Līdz 2028. gada 2. augustam un pēc tam reizi četros gados Komisija iesniedz ziņojumu par vispārīga lietojuma MI modeļu energoefektīvas izstrādes standartizācijas nodevumu izstrādē gūtā progresa pārskatīšanu un novērtē vajadzību pēc turpmākiem pasākumiem vai darbībām, tostarp saistošiem pasākumiem vai darbībām. Šo ziņojumu iesniedz Eiropas Parlamentam un Padomei un publicē.
7. Līdz 2028. gada 2. augustam un pēc tam reizi trīs gados Komisija izvērtē brīvprātīgo rīcības kodeksu ietekmi un efektivitāti, lai veicinātu III nodaļas 2. iedaļā noteikto prasību piemērošanu attiecībā uz MI sistēmām, kas nav augsta riska MI sistēmas, un, iespējams, citu papildu prasību piemērošanu attiecībā uz MI sistēmām, kas nav augsta riska MI sistēmas, tostarp saistībā ar vides ilgtspēju.
8. Šā panta 1. līdz 7. punkta nolūkos MI padome, dalībvalstis un valstu kompetentās iestādes Komisijai pēc tās pieprasījuma un bez liekas kavēšanās sniedz informāciju.
9. Veicot 1. līdz 7. punktā minēto izvērtēšanu un pārskatīšanu, Komisija ņem vērā MI padomes, Eiropas Parlamenta, Padomes un citu attiecīgo struktūru vai avotu nostāju un konstatējumus.

10. Vajadzības gadījumā Komisija iesniedz attiecīgus priekšlikumus par šīs regulas grozīšanu, jo īpaši, ņemot vērā norises tehnoloģiju jomā, MI sistēmu ietekmi uz veselību un drošību un pamattiesībām un ņemot vērā attīstības stāvokli informācijas sabiedrībā.

11. Lai ievirzītu šā panta 1. līdz 7. punktā minēto izvērtēšanu un pārskatīšanu, MI birojs appēmas izstrādāt objektīvu un līdzdalīgu metodiku riska līmeņa izvērtēšanai, balstoties uz attiecīgajos pantos izklāstītajiem kritērijiem un jaunu sistēmu iekļaušanu:

a) III pielikumā ietvertajā sarakstā, tostarp attiecībā uz spēkā esošo jomu kategoriju paplašināšanu vai jaunu jomu kategoriju pievienošanu minētajā pielikumā;

b) 5. pantā ietvertajā aizliegtās MI prakses sarakstā; un

c) MI sistēmu sarakstā, attiecībā uz kurām, ievērojot 50. pantu, vajadzīgi papildu pārredzamības pasākumi.

12. Visos grozījumos, ko veic šajā regulā, ievērojot 10. punktu, vai attiecīgajos turpmākajos deleģētajos vai īstenošanas aktos, kas attiecas uz I pielikuma B iedaļā uzskaitītajiem Savienības saskaņošanas tiesību aktiem, ņem vērā katras nozares regulējuma specifiku un spēkā esošos pārvaldības, atbilstības novērtēšanas un izpildes panākšanas mehānismus un ar tiem izveidoto iestāžu darbību.

13. Līdz 2031. gada 2. augustam Komisija novērtē šīs regulas izpildes panākšanu un sniedz ziņojumu par to Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai, ņemot vērā pirmos šīs regulas piemērošanas gadus. Pamatojoties uz minētā ziņojuma secinājumiem, Komisija attiecīgā gadījumā tam pievieno priekšlikumu par šīs regulas grozīšanu attiecībā uz izpildes panākšanas struktūru un vajadzību veidot Savienības aģentūru visu apzināto trūkumu novēršanai.

113. pants

Stāšanās spēkā un piemērošana

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas Eiropas Savienības Oficiālajā Vēstnesī.

To piemēro no 2026. gada 2. augusta.

Tomēr:

a) I un II nodaļu piemēro no 2025. gada 2. februāra;

b) III nodaļas 4. iedaļu, V nodaļu, VII nodaļu un XII nodaļu, un 78. pantu piemēro no 2025. gada 2. augusta, izņemot 101. pantu;

c) 6. panta 1. punktu un attiecīgos šajā regulā paredzētos pienākumus piemēro no 2027. gada 2. augusta.

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

Briselē, 2024. gada 13. jūnijā

Eiropas Parlamenta vārdā –

priekšsēdētāja

R. METSOLA

Padomes vārdā –

priekšsēdētājs

M. MICHEL

I PIELIKUMS

Savienības saskaņošanas tiesību aktu saraksts

A iedaļa. Jaunajā tiesiskajā regulējumā balstīto Savienības saskaņošanas tiesību aktu saraksts

1. Eiropas Parlamenta un Padomes Direktīva 2006/42/EK (2006. gada 17. maijs) par mašīnām, un ar kuru groza Direktīvu 95/16/EK (OV L 157, 9.6.2006., 24. lpp.).
2. Eiropas Parlamenta un Padomes Direktīva 2009/48/EK (2009. gada 18. jūnijs) par rotaļlietu drošumu (OV L 170, 30.6.2009., 1. lpp.).
3. Eiropas Parlamenta un Padomes Direktīva 2013/53/ES (2013. gada 20. novembris) par atpūtas kuģiem un ūdens motocikliem un ar ko atceļ Direktīvu 94/25/EK (OV L 354, 28.12.2013., 90. lpp.).
4. Eiropas Parlamenta un Padomes Direktīva 2014/33/ES (2014. gada 26. februāris) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz liftiem un liftu drošības sastāvdaļām (OV L 96, 29.3.2014., 251. lpp.).
5. Eiropas Parlamenta un Padomes Direktīva 2014/34/ES (2014. gada 26. februāris) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz iekārtām un aizsardzības sistēmām, kas paredzētas lietošanai sprādzienbīstamā vidē (OV L 96, 29.3.2014., 309. lpp.).
6. Eiropas Parlamenta un Padomes Direktīva 2014/53/ES (2014. gada 16. aprīlis) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz radioiekārtu pieejamību tirgū un ar ko atceļ Direktīvu 1999/5/EK (OV L 153, 22.5.2014., 62. lpp.).
7. Eiropas Parlamenta un Padomes Direktīva 2014/68/ES (2014. gada 15. maijs) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz spiedieniekārtu pieejamību tirgū (OV L 189, 27.6.2014., 164. lpp.).
8. Eiropas Parlamenta un Padomes Regula (ES) 2016/424 (2016. gada 9. marts) par trošu ceļu iekārtām un ar ko atceļ Direktīvu 2000/9/EK (OV L 81, 31.3.2016., 1. lpp.).
9. Eiropas Parlamenta un Padomes Regula (ES) 2016/425 (2016. gada 9. marts) par individuālajiem aizsardzības līdzekļiem un ar ko atceļ Padomes Direktīvu 89/686/EEK (OV L 81, 31.3.2016., 51. lpp.).
10. Eiropas Parlamenta un Padomes Regula (ES) 2016/426 (2016. gada 9. marts) par gāzveida kurināmā iekārtām un ar ko atceļ Direktīvu 2009/142/EK (OV L 81, 31.3.2016., 99. lpp.).
11. 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.).
12. 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.).

B iedaļa. Citu Savienības saskaņošanas tiesību aktu saraksts

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

16. 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.).
17. 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.).
18. 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.).
19. 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, (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.).
20. 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.), ciktāl tā attiecas uz tās 2. panta 1. punkta a) un b) apakšpunktā minēto gaisa kuģu konstruēšanu, ražošanu un laišanu tirgū, kur tas attiecas uz bezpilota gaisa kuģiem un to dzinējiem, propelleriem, daļām un to tālvaldības ierīcēm.

II PIELIKUMS

5. panta 1. punkta pirmās daļas e) apakšpunkta iii) punktā minēto noziedzīgo nodarījumu saraksts

5. panta 1. punkta pirmās daļas e) apakšpunkta iii) punktā minētie noziedzīgie nodarījumi:

- terorisms,
- cilvēku tirdzniecība,
- bērnu seksuāla izmantošana un bērnu pornogrāfija,
- narkotisko vielu un psihotropo vielu nelikumīga tirdzniecība,
- ieroču, munīcijas un sprāgstvielu nelikumīga tirdzniecība,
- slepkavība, smagi miesas bojājumi,
- cilvēku orgānu un audu nelikumīga tirdzniecība,
- kodolmateriālu vai radioaktīvu materiālu nelikumīga tirdzniecība,
- personu nolaupīšana, nelikumīga brīvības atņemšana vai ķīlnieku sagrābšana,
- noziegumi, kas ir Starptautiskās Krimināltiesas jurisdikcijā,
- gaisa kuģu vai kuģu nelikumīga sagrābšana,
- izvarošana,
- noziegumi pret vidi,
- organizēta vai bruņota laupīšana,
- sabotāža,
- dalība noziedzīgā organizācijā, kas iesaistīta vienā vai vairākos iepriekš uzskaitītajos nodarījumos.

III PIELIKUMS

6. panta 2. punktā minētās augsta riska MI sistēmas

6. panta 2. punktā minētās augsta riska MI sistēmas ir norādītās MI sistēmas, ko izmanto kādā no tālāk uzskaitītajām jomām.

1. Biometrija, ciktāl to izmantošanu atļauj attiecīgie Savienības vai valsts tiesību akti:
 - a) biometriskās tālidentifikācijas sistēmas.

Tas neietver MI sistēmas, ko paredzēts izmantot biometriskai verifikācijai, kuras vienīgais nolūks ir apstiprināt, ka konkrēta fiziska persona ir persona, par kuru tā uzdodas;
 - b) MI sistēmas, ko paredzēts izmantot biometriskai kategorizēšanai pēc sensitīviem vai aizsargātiem atribūtiem vai raksturlielumiem, pamatojoties uz minēto atribūtu vai raksturlielumu inferenci;
 - c) MI sistēmas, ko paredzēts izmantot emociju atpazīšanai.
2. Kritiskā infrastruktūra: MI sistēmas, ko paredzēts izmantot kā drošības sastāvdaļas kritiskās digitālās infrastruktūras pārvaldībā un darbībā, ceļu satiksmē vai ūdens, gāzes vai elektroapgādē vai apkures nodrošināšanā.
3. Izglītība un arodmācības:
 - a) MI sistēmas, ko paredzēts izmantot, lai noteiktu fizisku personu piekļuvi izglītības un arodmācību iestādēm visos līmeņos vai viņu iestāšanos tajās vai viņu uzņemšanu tajās;
 - b) MI sistēmas, ko paredzēts izmantot, lai izvērtētu mācību rezultātus, tostarp, ja šos rezultātus izmanto, lai vadītu fizisku personu mācību procesu izglītības un arodmācību iestādēs visos līmeņos;
 - c) MI sistēmas, ko paredzēts izmantot, lai novērtētu pienācīgu izglītības līmeni, kuru persona saņems vai kuram tā varēs piekļūt izglītības un arodmācības iestādēs vai saistībā ar tām visos līmeņos;
 - d) MI sistēmas, ko paredzēts izmantot, lai pārbaudījumu laikā izglītības un arodmācības iestādēs vai saistībā ar tām uzraudzītu un konstatētu audzēkņu neatļautu uzvedību visos līmeņos.
4. Nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai:
 - a) MI sistēmas, ko paredzēts izmantot fizisku personu pieņemšanai darbā vai darbinieku atlasei, jo īpaši, lai izvietotu mērķtiecīgus darba sludinājumus, analizētu un atsijātu darba pieteikumus un izvērtētu kandidātus;
 - b) MI sistēmas, ko paredzēts izmantot, lai pieņemtu lēmumus, kas skar darba attiecību, paaugstināšanas amatā vai darba līgumattiecību izbeigšanas kārtību, sadalītu uzdevumus, pamatojoties uz individuālo uzvedību vai personības iezīmēm vai īpašībām, vai lai pārraudzītu un izvērtētu darba līgumattiecībās esošo personu sniegumu un uzvedību.
5. Piekļuve privātiem pamatpakalpojumiem un sabiedriskajiem pamatpakalpojumiem un pabalstiem un to izmantošana:
 - a) MI sistēmas, ko paredzēts izmantot publiskajās iestādēs vai to vārdā, lai izvērtētu fizisku personu tiesības saņemt pamata sociālās palīdzības pabalstus un pakalpojumus, tostarp veselības aprūpes pakalpojumus, kā arī lai piešķirtu, samazinātu, atsauktu vai atgūtu šādus pabalstus un pakalpojumus;
 - b) MI sistēmas, ko paredzēts izmantot fizisku personu kredīspējas izvērtēšanai vai to kredītnovērtējuma noteikšanai, izņemot tādas MI sistēmas, kuras izmanto krāpšanas atklāšanai finanšu jomā;
 - c) MI sistēmas, ko paredzēts izmantot riska novērtēšanai un cenu noteikšanai attiecībā uz fiziskām personām dzīvības un veselības apdrošināšanas gadījumā;

- d) MI sistēmas, ko paredzēts izmantot, lai izvērtētu un klasificētu fizisku personu ārkārtas palīdzības izsaukumus vai ārkārtas pirmās reaģēšanas dienestu, tostarp policijas, ugunsdzēsēju un medicīniskās palīdzības sniedzēju, nosūtīšanai vai nosūtīšanas prioritāšu noteikšanai, kā arī neatliekamās medicīniskās aprūpes pacientu triāžas sistēmām.
6. Tiesībaizsardzība, ciktāl to izmantošanu atļauj attiecīgie Savienības vai valsts tiesību akti:
- a) MI sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, vai to vārdā, lai novērtētu risku, ka fiziska persona varētu kļūt par cietušo personu noziedzīgos nodarījumos;
- b) MI sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, piemēram, melu detektoru un līdzīgi rīki;
- c) MI sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, pierādījumu uzticamības izvērtēšanai noziedzīgu nodarījumu izmeklēšanas vai kriminālvajāšanas gaitā;
- d) MI sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, lai novērtētu risku, ka fiziska persona varētu izdarīt vai atkārtoti izdarīt nodarījumu, pamatojoties ne tikai uz fizisku personu profilēšanu, kas minēta Direktīvas (ES) 2016/680 3. panta 4. punktā, vai lai novērtētu fizisku personu vai grupu personības iezīmes un rakstura īpašības vai agrāku noziedzīgu rīcību;
- e) MI sistēmas, ko paredzēts izmantot tiesībaizsardzības iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, kas atbalsta tiesībaizsardzības iestādes, Direktīvas (ES) 2016/680 3. panta 4. punktā minētajai fizisku personu profilēšanai noziedzīgu nodarījumu atklāšanas, izmeklēšanas vai kriminālvajāšanas gaitā.
7. Migrācijas, patvēruma un robežkontroles pārvaldība, ciktāl to izmantošanu atļauj attiecīgie Savienības vai valsts tiesību akti:
- a) MI sistēmas, ko paredzēts izmantot kompetentās publiskajās iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās kā melu detektorus vai līdzīgus rīkus;
- b) MI sistēmas, ko paredzēts izmantot kompetentās publiskajās iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, lai novērtētu risku, tostarp drošības risku, neatbilstīgas migrācijas risku vai veselības risku, ko rada fiziska persona, kas vēlas ieceļot vai ir ieceļojusi dalībvalsts teritorijā;
- c) MI sistēmas, ko paredzēts izmantot kompetentās publiskajās iestādēs vai to vārdā, vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, lai palīdzētu kompetentām publiskajām iestādēm izskatīt patvēruma, vīzu vai uzturēšanās atļauju pieteikumus, kā arī saistītās sūdzības, nosakot, vai fiziskās personas, kuras iesniegušas pieteikumu uz kādu no minētajiem statusiem, atbilst kritērijiem, tostarp veicot saistītu pierādījumu patiesuma novērtēšanu;
- d) MI sistēmas, ko paredzēts izmantot kompetentās publiskajās iestādēs vai Savienības iestādēs, struktūrās, birojos vai aģentūrās, vai to vārdā saistībā ar migrācijas, patvēruma vai robežkontroles pārvaldību nolūkā atklāt, atpazīt vai identificēt fiziskas personas, izņemot ceļošanas dokumentu verifikāciju.
8. Tiesvedība un demokrātijas procesi:
- a) MI sistēmas, ko paredzēts izmantot tiesu iestādē vai tās vārdā, lai palīdzētu tiesu iestādei izpētīt un interpretēt faktus vai tiesību normas un piemērot tiesību normas konkrētam faktu kopumam, vai izmantot līdzīgā veidā strīdu alternatīvā izšķiršanā;

- b) MI sistēmas, ko paredzēts izmantot, lai ietekmētu vēlēšanu vai referenduma rezultātus vai fizisku personu uzvedību balsošanā, kad tās balso vēlēšanās vai referendumos. Tas neattiecas uz MI sistēmām, kuru rezultātam fiziskas personas nav tieši pakļautas, piemēram, rīkiem, ko izmanto, lai organizētu, optimizētu vai strukturētu politiskas kampaņas no administratīvā vai loģistikas viedokļa.
-

IV PIELIKUMS

Tehniskā dokumentācija, kas minēta 11. panta 1. punktā

Tehniskajā dokumentācijā, kas minēta 11. panta 1. punktā, norāda vismaz turpmāk uzskaitīto informāciju, ja tā ir attiecināma uz konkrēto MI sistēmu.

1. Vispārējs MI sistēmas apraksts, kas ietver šādu informāciju:
 - a) tās paredzētais nolūks, nodrošinātāja nosaukums/vārds un sistēmas versija, atspoguļojot tās saikni ar iepriekšējām versijām;
 - b) attiecīgā gadījumā – kā MI sistēma mijiedarbojas, vai var tikt izmantota mijiedarbībai, ar aparāturu vai programmatūru, tostarp ar citām MI sistēmām, kas nav pašas MI sistēmas daļa;
 - c) attiecīgās programmatūras vai aparātprogrammatūras versijas un prasības par versiju atjaunināšanu;
 - d) apraksts par visām formām, kādās MI sistēma laista tirgū vai nodota ekspluatācijā, piemēram, programmatūras pakotnes, kas iegultas aparatūrā, lejupielādes vai API;
 - e) tās aparatūras apraksts, kurā MI sistēmai paredzēts darboties;
 - f) ja MI sistēma ir produktu sastāvdaļa – fotoattēli vai ilustrācijas, kas parāda šo produktu ārējās iezīmes, marķējumu un iekšējo izkārtojumu;
 - g) uzturētājam nodrošinātās lietotāja saskarnes pamatapraksts;
 - h) lietošanas instrukcija uzturētājam un, attiecīgā gadījumā, uzturētājam nodrošinātās lietotāja saskarnes pamatapraksts;
2. Detalizēts MI sistēmas elementu un tās izstrādes procesa apraksts, kas ietver šādu informāciju:
 - a) MI sistēmas izstrādes metodes un soļi, attiecīgā gadījumā ietverot norādes par iepriekš apmācītu sistēmu vai trešo personu nodrošinātu instrumentu izmantošanu un to, kā nodrošinātājs ir tos izmantojis, integrējis vai modificējis;
 - b) sistēmas projekta specifikācijas, proti, MI sistēmas un algoritmu vispārīgā loģika; galvenās projektēšanas izvēles, arī pamatojums un izdarītie pieņēmumi, tostarp saistībā ar personām vai personu grupām, attiecībā uz kurām sistēmu paredzēts izmantot; galvenās klasifikācijas izvēles; ko ar sistēmu paredzēts optimizēt un kāda ir dažādo parametru nozīme; sistēmas paredzamā iznākuma un iznākuma kvalitātes apraksts; lēmumi par iespējamajiem kompromisiem saistībā ar izmantotajiem tehniskajiem risinājumiem, lai nodrošinātu atbilstību III nodaļas 2. iedaļā noteiktajām prasībām;
 - c) sistēmas arhitektūras apraksts, kurā paskaidrots, kā programmatūras komponenti ir balstīti cits citā vai papildina cits citu un kā tie integrēti kopējā programmas darbībā; skaitļošanas resursi, kas izmantoti MI sistēmas izstrādē, apmācīšanā, testēšanā un validēšanā;
 - d) attiecīgā gadījumā – datu prasības, t. i., datu lapas, kurās aprakstīti izmantotie apmācības paņēmieni un metodes, kā arī apmācības datu kopas, tostarp šo datu kopu vispārējs apraksts, sniegta informācija par to izcelsmi, to tvērumu un galvenajiem raksturlielumiem; kā dati iegūti un atlasīti; marķēšanas procedūras (piemēram, uzraudzītās mācīšanās gadījumā), datu tīrīšanas metodes (piemēram, izlecošo vērtību noteikšana);
 - e) 14. pantā prasīto cilvēka virsvadības pasākumu novērtējums, tostarp novērtējums par tehniskajiem pasākumiem, kas saskaņā ar 13. panta 3. punkta d) apakšpunktu jāievieš, lai palīdzētu uzturētājiem interpretēt MI sistēmu iznākumus;
 - f) attiecīgā gadījumā – detalizēts apraksts par iepriekš noteiktām izmaiņām MI sistēmā un tās veikspējā un visa attiecīgā informācija par tehniskajiem risinājumiem, kas izmantoti, lai nodrošinātu MI sistēmas pastāvīgu atbilstību attiecīgajām III nodaļas 2. iedaļas prasībām;
 - g) izmantotās validēšanas un testēšanas procedūras, arī informācija par izmantotajiem validēšanas un testēšanas datiem un to galvenajām iezīmēm; rādītāji, kas izsaka precizitāti, robustumu un atbilstību citām attiecīgām III nodaļas 2. iedaļā noteiktajām prasībām, kā arī potenciāli diskriminējošo ietekmi; testēšanas žurnāli un visi testēšanas ziņojumi, ko datējušas un parakstījušas atbildīgās personas, tai skaitā tādi, kuri attiecas uz iepriekš noteiktām izmaiņām, kas minētas f) apakšpunktā;

- h) ieviestie kibernetikas pasākumi.
3. Detalizēta informācija par MI sistēmas pārbaudību, darbību un kontroli, it īpaši par: tās spējam un veikspējas ierobežojumiem, tostarp precizitātes līmeni attiecībā uz konkrētām personām vai personu grupām, attiecībā uz kurām sistēmu paredzēts lietot, un kopējo paredzamo precizitātes līmeni paredzētā nolūka izpildē; prognozējamiem neparedzētiem iznākumiem un tādu risku avotiem, kas apdraud veselību, drošību un pamattiesības un var radīt diskrimināciju, ņemot vērā MI sistēmas paredzēto nolūku; 14. pantā prasītajiem cilvēka virsvadības pasākumiem, tostarp tehniskajiem pasākumiem, kas ieviesti, lai palīdzētu uzturētājiem interpretēt MI sistēmu iznākumus; attiecīgā gadījumā – ievaddatu specifiskajām.
 4. Konkrētās MI sistēmas veikspējas rādītāju piemērotības apraksts.
 5. Detalizēts apraksts par riska pārvaldības sistēmu, kas izveidota saskaņā ar 9. pantu.
 6. Attiecīgo izmaiņu apraksts, ko sistēmai tās darbībā veicis nodrošinātājs.
 7. To saskaņoto standartu saraksts, kas piemēroti pilnībā vai daļēji un uz ko atsaucas publicētas Eiropas Savienības Oficiālajā Vēstnesī; ja šādi saskaņotie standarti nav tikuši piemēroti – detalizēts apraksts par risinājumiem, kas izmantoti, lai izpildītu III nodaļas 2. iedaļā noteiktās prasības, tai skaitā citu izmantoto attiecīgo standartu un tehnisko specifiskumu saraksts.
 8. Šīs regulas 47. pantā minētās ES atbilstības deklarācijas kopija.
 9. Detalizēts apraksts par sistēmu, kas ieviesta MI sistēmas veikspējas izvērtēšanai pēctirgus posmā saskaņā ar 72. pantu, kā arī pēctirgus uzraudzības plāns, kas minēts 72. panta 3. punktā.
-

V PIELIKUMS

ES atbilstības deklarācija

ES atbilstības deklarācijā, kas minēta 47. pantā, iekļauj visu turpmāk uzskaitīto informāciju.

1. MI sistēmas nosaukums un tips un citas nepārprotamas atsauces, kas nodrošina MI sistēmas identifikāciju un izsekojamību.
2. Nodrošinātāja vai, attiecīgā gadījumā, tā pilnvarotā pārstāvja nosaukums/vārds un adrese.
3. Paziņojums, ka 47. pantā minētā ES atbilstības deklarācija ir izdota vienīgi uz nodrošinātāja atbildību.
4. Paziņojums, ka MI sistēma atbilst šīs regulas noteikumiem un attiecīgā gadījumā citu tādu attiecīgo Savienības tiesību aktu noteikumiem, kuri paredz 47. pantā minētās ES atbilstības deklarācijas izdošanu.
5. Ja MI sistēma ietver personas datu apstrādi, paziņojums, ka šī MI sistēma atbilst Regulai (ES) 2016/679, Regulai (ES) 2018/1725 un Direktīvai (ES) 2016/680.
6. Norādes uz attiecīgiem saskaņotajiem standartiem, kas izmantoti, vai norādes uz citām kopīgām specifikācijām, par kurām deklarē atbilstību.
7. Attiecīgā gadījumā – paziņotās struktūras nosaukums un identifikācijas numurs, veiktās atbilstības novērtēšanas procedūras apraksts un izdotā sertifikāta identifikācija.
8. Deklarācijas izdošanas vieta un datums, to parakstījušās personas vārds un amats, kā arī norāde par to, kam vai kā vārdā minētā persona to parakstījusi, paraksts.

VI PIELIKUMS

Atbilstības novērtēšanas procedūra uz iekšējās kontroles pamata

1. Atbilstības novērtēšanas procedūra uz iekšējās kontroles pamata ir atbilstības novērtēšanas procedūra, kuras pamatā ir 2., 3. un 4. punkts.
 2. Nodrošinātājs pārlicinās, ka ieviestā kvalitātes vadības sistēma atbilst 17. panta prasībām.
 3. Nodrošinātājs pārbauda tehniskajā dokumentācijā ietverto informāciju, lai novērtētu MI sistēmas atbilstību attiecīgajām būtiskajām prasībām, kas noteiktas III nodaļas 2. iedaļā.
 4. Tāpat nodrošinātājs pārlicinās, ka MI sistēmas projektēšanas un izstrādes process un 72. pantā minētā tās pēctirgus pārraudzība atbilst tehniskajai dokumentācijai.
-

VII PIELIKUMS

Atbilstība, kuras pamatā ir kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtējums

1. Ievads

Atbilstības novērtēšana, kuras pamatā ir kvalitātes vadības sistēmas un tehniskās dokumentācijas novērtējums, ir atbilstības novērtēšanas procedūra, kuras pamatā ir 2. līdz 5. punkts.
2. Pārskats

Apstiprināto 17. pantam atbilstošo kvalitātes vadības sistēmu MI sistēmu projektēšanai, izstrādei un testēšanai pārbauda saskaņā ar 3. punktu un uz to attiecas uzraudzība, kā aprakstīts 5. punktā. MI sistēmas tehnisko dokumentāciju pārbauda saskaņā ar 4. punktu.
3. Kvalitātes vadības sistēma
 - 3.1. Nodrošinātāja pieteikumā iekļauj:
 - a) nodrošinātāja nosaukumu/vārdu un adresi un, ja pieteikumu iesniedz pilnvarotais pārstāvis, arī šā pārstāvja nosaukumu/vārdu un adresi;
 - b) to MI sistēmu uzskaitījumu, uz kurām attiecas tā pati kvalitātes vadības sistēma;
 - c) tehnisko dokumentāciju par katru MI sistēmu, uz ko attiecas tā pati kvalitātes vadības sistēma;
 - d) kvalitātes vadības sistēmas dokumentāciju, kurā aptverti visi 17. pantā uzskaitītie aspekti;
 - e) to procedūru aprakstu, kas ieviestas, lai nodrošinātu, ka kvalitātes vadības sistēma nezaudē piemērotību un efektivitāti;
 - f) rakstisku paziņojumu, ka tāds pats pieteikums nav iesniegts nevienai citai paziņotajai struktūrai.
 - 3.2. Paziņotā struktūra novērtē kvalitātes vadības sistēmu un konstatē, vai tā atbilst 17. pantā minētajām prasībām.

Lēmumu paziņo nodrošinātājam vai tā pilnvarotajam pārstāvim.

Paziņojumā iekļauj kvalitātes vadības sistēmas novērtējuma secinājumus un argumentētu novērtējuma lēmumu.
 - 3.3. Nodrošinātājs turpina īstenot un uzturēt apstiprināto kvalitātes vadības sistēmu tā, lai tā nezaudētu piemērotību un efektivitāti.
 - 3.4. Nodrošinātājs informē paziņoto struktūru par plānotām izmaiņām apstiprinātajā kvalitātes vadības sistēmā vai to MI sistēmu sarakstā, uz kurām tā attiecas.

Paziņotā struktūra izskata ierosinātās izmaiņas un pieņem lēmumu par to, vai mainītā kvalitātes vadības sistēma joprojām atbilst 3.2. punkta prasībām vai arī ir nepieciešams atkārtots novērtējums.

Paziņotā struktūra savu lēmumu paziņo nodrošinātājam. Paziņojumā iekļauj izmaiņu pārbaudes secinājumus un argumentētu novērtējuma lēmumu.
4. Tehniskās dokumentācijas kontrole
 - 4.1. Papildus 3. punktā minētajam pieteikumam nodrošinātājs iesniedz paša izvēlētai paziņotajai struktūrai pieteikumu par tās MI sistēmas tehniskās dokumentācijas novērtēšanu, kuru nodrošinātājs vēlas laist tirgū vai nodot ekspluatācijā un uz kuru attiecas 3. punktā minētā kvalitātes vadības sistēma.
 - 4.2. Pieteikumā iekļauj:
 - a) nodrošinātāja nosaukumu/vārdu un adresi;
 - b) rakstisku deklarāciju, ka tāds pats pieteikums nav iesniegts nevienai citai paziņotajai struktūrai;
 - c) IV pielikumā norādīto tehnisko dokumentāciju.

- 4.3. Paziņotā struktūra pārbauda tehnisko dokumentāciju. Attiecīgā gadījumā un tiktāl, ciktāl tas ir nepieciešams paziņotās struktūras uzdevumu izpildei, tai nodrošina pilnu piekļuvi izmantotajām apmācības, validēšanas un testēšanas datu kopām, tostarp – attiecīgā gadījumā un ievērojot drošības aizsardzības pasākumus – izmantojot API vai citus attiecīgus tehniskos līdzekļus un rīkus, kas nodrošina attālu piekļuvi.
- 4.4. Pārbaudot tehnisko dokumentāciju, paziņotā struktūra var prasīt, lai nodrošinātājs iesniedz papildu pierādījumus vai veic papildu testus, lai būtu iespējams pilnvērtīgi pārbaudīt MI sistēmas atbilstību III nodaļas 2. iedaļā noteiktajām prasībām. Ja paziņoto struktūru neapmierina nodrošinātāja veiktie testi, paziņotā struktūra pēc vajadzības pati veic attiecīgus testus.
- 4.5. Ja tas nepieciešams, lai novērtētu augsta riska MI sistēmas atbilstību III nodaļas 2. iedaļā izklāstītajām prasībām, pēc tam, kad izsmelti visi citi saprātīgi līdzekļi atbilstības verificēšanai un ir pierādījies, ka tie ir bijuši nepietiekami, un pēc pamatota pieprasījuma nodrošina arī paziņotās struktūras piekļuvi MI sistēmas apmācībai un apmācītajiem modeļiem, tostarp tās attiecīgajiem parametriem. Uz šādu piekļuvi attiecas spēkā esošie Savienības tiesību akti par intelektuālā īpašuma un komercnoslēpumu aizsardzību.
- 4.6. Paziņotās struktūras lēmumu paziņo nodrošinātājam vai tā pilnvarotajam pārstāvim. Paziņojumā iekļauj tehniskās dokumentācijas novērtējuma secinājumus un argumentētu novērtējuma lēmumu.

Ja MI sistēma atbilst III nodaļas 2. iedaļā noteiktajām prasībām, paziņotā struktūra izdod Savienības tehniskās dokumentācijas novērtējuma sertifikātu. Sertifikātā norāda nodrošinātāja nosaukumu/vārdu un adresi, pārbaudes secinājumus, sertifikāta derīguma nosacījumus (ja tādi ir) un MI sistēmas identifikācijai nepieciešamos datus.

Sertifikātā un tā pielikumos iekļauj visu attiecīgo informāciju, kas ļauj izvērtēt MI sistēmas atbilstību un attiecīgā gadījumā pārbaudīt MI sistēmu tās lietošanas laikā.

Ja MI sistēma neatbilst III nodaļas 2. iedaļā noteiktajām prasībām, paziņotā struktūra neizdod Savienības tehniskās dokumentācijas novērtējuma sertifikātu un par to informē pieteikuma iesniedzēju, detalizēti norādot atteikuma iemeslus.

Ja MI sistēma neatbilst prasībām par datiem, kas izmantoti tās apmācīšanai, pirms pieteikšanās jaunai atbilstības novērtēšanai ir jāveic MI sistēmas atkārtota apmācīšana. Šādā gadījumā paziņotās struktūras argumentētajā novērtējuma lēmumā, ar ko tā atsaka izdot Savienības tehniskās dokumentācijas novērtējuma sertifikātu, norāda konkrētus apsvērumus par MI sistēmas apmācībai izmantoto datu kvalitāti, jo īpaši par neatbilstības iemesliem.
- 4.7. Jebkādas MI sistēmā veiktas izmaiņas, kas varētu ietekmēt MI sistēmas atbilstību prasībām vai tās paredzētajam nolūkam, novērtē paziņotā struktūra, kura izdevusi Savienības tehniskās dokumentācijas novērtējuma sertifikātu. Nodrošinātājs informē šādu paziņoto struktūru par savu ieceri ieviest kādas minētās izmaiņas vai ja tam kā citādi kļūst zināms, ka tādas izmaiņas ir notikušas. Paziņotā struktūra novērtē iecerētās izmaiņas un pieņem lēmumu par to, vai saistībā ar šīm izmaiņām ir nepieciešams jauns atbilstības novērtējums saskaņā ar 43. panta 4. punktu jeb vai tās varētu iekļaut Savienības tehniskās dokumentācijas novērtējuma sertifikāta papildinājumā. Otrajā minētajā gadījumā paziņotā struktūra novērtē izmaiņas, paziņo nodrošinātājam savu lēmumu un, ja izmaiņas tiek apstiprinātas, izdod nodrošinātājam Savienības tehniskās dokumentācijas novērtējuma sertifikāta papildinājumu.
5. Apstiprinātās kvalitātes vadības sistēmas uzraudzība
 - 5.1. Kvalitātes vadības sistēmas uzraudzību 3. punktā minētā paziņotā struktūra veic, lai pārliecinātos, ka nodrošinātājs pienācīgi ievēro apstiprinātās kvalitātes vadības sistēmas noteikumus.
 - 5.2. Novērtēšanas vajadzībām nodrošinātājs ļauj paziņotajai struktūrai iekļūt telpās, kurās notiek MI sistēmu projektēšana, izstrāde vai testēšana. Nodrošinātājs arī sniedz paziņotajai struktūrai visu nepieciešamo informāciju.
 - 5.3. Paziņotā struktūra periodiski veic revīziju, lai pārliecinātos, ka nodrošinātājs uztur un piemēro kvalitātes vadības sistēmu, un iesniedz nodrošinātājam revīzijas ziņojumu. Minētās revīzijas ietvaros paziņotā struktūra var veikt to MI sistēmu papildu testus, kurām ticis izdots Savienības tehniskās dokumentācijas novērtējuma sertifikāts.

VIII PIELIKUMS

Informācija, kas jāiesniedz, reģistrējot augsta riska MI sistēmas saskaņā ar 49. pantu

A iedaļa – Informācija, kas nodrošinātājiem jāiesniedz, reģistrējot augsta riska MI sistēmas saskaņā ar 49. panta 1. punktu
Par augsta riska MI sistēmām, kas jāreģistrē saskaņā ar 49. panta 1. punktu, sniedz un pēc tam regulāri atjaunina šādu informāciju:

1. Nodrošinātāja nosaukums/vārds, adrese un kontaktinformācija.
2. Ja informāciju nodrošinātāja vārdā iesniedz cita persona – šīs personas nosaukums/vārds, adrese un kontaktinformācija.
3. Attiecīgā gadījumā – pilnvarotā pārstāvja nosaukums/vārds, adrese un kontaktinformācija.
4. MI sistēmas tirdzniecības nosaukums un citas nepārprotamas atsauces, kas nodrošina MI sistēmas identifikāciju un izsekojamību.
5. MI sistēmai paredzētā nolūka un ar šo MI sistēmu atbalstīto sastāvdaļu un funkciju apraksts.
6. Sistēmas izmantotās informācijas (datu, ievaddatu) un tās darbības loģikas kodolīgs pamatapraksts.
7. MI sistēmas statuss (tirgū vai ekspluatācijā; vairs netiek laista tirgū / vairs nav ekspluatācijā, atsaukta).
8. Paziņotās struktūras izdotā sertifikāta tips, numurs un derīguma termiņš un – attiecīgā gadījumā – minētās paziņotās struktūras nosaukums vai identifikācijas numurs.
9. Attiecīgā gadījumā – 8. punktā minētā sertifikāta skenēta kopija.
10. Dalībvalstis, kurās MI sistēma tikusi laista tirgū, nodota ekspluatācijā vai darīta pieejama Savienībā.
11. 47. pantā minētās ES atbilstības deklarācijas kopija.
12. Elektroniska lietošanas instrukcija; šo informāciju nesniedz par III pielikuma 1., 6. un 7. punktā minētajām augsta riska AI sistēmām, ko izmanto tiesībsargsardzības, kā arī migrācijas, patvēruma vai robežkontroles pārvaldības jomā.
13. URL papildu informācijai (neobligāti).

B iedaļa – Informācija, kas nodrošinātājiem jāiesniedz, reģistrējot augsta riska MI sistēmas saskaņā ar 49. panta 2. punktu
Par MI sistēmām, kas jāreģistrē saskaņā ar 49. panta 2. punktu, sniedz un pēc tam regulāri atjaunina šādu informāciju.

1. Nodrošinātāja nosaukums/vārds, adrese un kontaktinformācija.
2. Ja informāciju nodrošinātāja vārdā iesniedz cita persona – šīs personas nosaukums/vārds, adrese un kontaktinformācija.
3. Attiecīgā gadījumā – pilnvarotā pārstāvja nosaukums/vārds, adrese un kontaktinformācija.
4. MI sistēmas tirdzniecības nosaukums un citas nepārprotamas atsauces, kas nodrošina MI sistēmas identifikāciju un izsekojamību.
5. Paredzētā MI sistēmas nolūka apraksts.
6. 6. panta 3. punktā paredzēts nosacījums vai nosacījumi, uz ko pamatojoties MI sistēma tiek uzskatīta par tādu, kas nav augsta riska MI sistēma;
7. Īss pamatojuma kopsavilkums, kāpēc MI sistēmu uzskata par tādu, kas nav augsta riska MI sistēma, piemērojot 6. panta 3. punktā paredzēto procedūru.
8. MI sistēmas statuss (tirgū vai ekspluatācijā; vairs netiek laista tirgū / vairs nav ekspluatācijā, atsaukta).
9. Visas dalībvalstis, kurās MI sistēma bija laista tirgū, nodota ekspluatācijā vai darīta pieejama Savienībā.

C iedaļa – Informācija, kas uzturētājiem jāiesniedz, reģistrējot augsta riska MI sistēmas saskaņā ar 49. panta 3. punktu

Par augsta riska MI sistēmām, kas jāreģistrē saskaņā ar 49. panta 3. punktu, sniedz un pēc tam regulāri atjaunina šādu informāciju:

1. Uzturētāja nosaukums/vārds, adrese un kontaktinformācija.
 2. Tās personas nosaukums/vārds, adrese un kontaktinformācija, kura sniedz informāciju uzturētāja vārdā.
 3. URL nodrošinātāja veiktai MI sistēmas reģistrācijai ES datubāzē.
 4. Saskaņā ar 27. pantu veiktā novērtējuma par ietekmi uz pamattiesībām konstatējumu kopsavilkums.
 5. Attiecīgā gadījumā – kopsavilkums novērtējumam par ietekmi uz datu aizsardzību, kas veikts saskaņā ar Regulas (ES) 2016/679 35. pantu vai Direktīvas (ES) 2016/680 27. pantu, kā noteikts šīs regulas 26. panta 8. punktā.
-

IX PIELIKUMS

Informācija, kas jāiesniedz, reģistrējot III pielikumā uzskaitītās augsta riska MI sistēmas saistībā ar testēšanu reālos apstākļos saskaņā ar 60. pantu

Saistībā ar veicamo reģistrāciju sniedz un pēc tam regulāri atjaunina šādu informāciju attiecībā uz testēšanu reālos apstākļos saskaņā ar 60. pantu.

1. Unikāls Savienības mēroga vienots identifikācijas numurs testēšanai reālos apstākļos.
2. Nodrošinātāja vai potenciālā nodrošinātāja un uzturētāju, kas iesaistīti testēšanā reālos apstākļos, nosaukums/vārds un kontaktinformācija.
3. Īss MI sistēmas apraksts, tai paredzētais nolūks un cita informācija, kas vajadzīga sistēmas identificēšanai.
4. Testēšanas reālos apstākļos plāna galveno raksturlielumu kopsavilkums.
5. Informācija par testēšanas reālos apstākļos apturēšanu vai izbeigšanu.

X PIELIKUMS

Savienības tiesību akti par lielapjoma IT sistēmām brīvības, drošības un tiesiskuma telpā

1. Šengenas Informācijas sistēma

- a) Eiropas Parlamenta un Padomes Regula (ES) 2018/1860 (2018. gada 28. novembris) par Šengenas informācijas sistēmas izmantošanu to trešo valstu valstspiederīgo atgriešanai, kuri dalībvalstīs uzturas nelikumīgi (OV L 312, 7.12.2018., 1. lpp.).
- b) Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu robežpārbaudīšanā un ar kuru groza Konvenciju, ar ko īsteno Šengenas nolīgumu, un groza un atceļ Regulu (EK) Nr. 1987/2006 (OV L 312, 7.12.2018., 14. lpp.).
- c) Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (2018. gada 28. novembris) par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās un ar ko groza un atceļ Padomes Lēmumu 2007/533/TI un atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1986/2006 un Komisijas Lēmumu 2010/261/ES (OV L 312, 7.12.2018., 56. lpp.).

2. Vīzu informācijas sistēma

- a) Eiropas Parlamenta un Padomes Regula (ES) 2021/1133 (2021. gada 7. jūlijs), ar ko attiecībā uz nosacījumu izveidi piekļuvei citām ES informācijas sistēmām vīzu informācijas sistēmas VIS vajadzībām groza Regulas (ES) Nr. 603/2013, (ES) 2016/794, (ES) 2018/1862, (ES) 2019/816 un (ES) 2019/818 (OV L 248, 13.7.2021., 1. lpp.).
- b) Eiropas Parlamenta un Padomes Regula (ES) 2021/1134 (2021. gada 7. jūlijs), ar ko Vīzu informācijas sistēmas reformas nolūkā groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (EK) Nr. 810/2009, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1860, (ES) 2018/1861, (ES) 2019/817 un (ES) 2019/1896 un atceļ Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 248, 13.7.2021., 11. lpp.).

3. Eurodac

Eiropas Parlamenta un Padomes Regula (ES) 2024/1358 (2024. gada 14. maijs) par *Eurodac* izveidi biometrisku datu salīdzināšanai, lai efektīvi piemērotu Eiropas Parlamenta un Padomes Regulas (ES) 2024/1315 un (ES) 2024/1350 un Padomes Direktīvu 2001/55/EK un lai identificētu trešās valsts valstspiederīgo vai bezvalstnieku, kas dalībvalstī uzturas nelikumīgi, un par dalībvalstu tiesībsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībsardzības nolūkos, un ar ko groza Eiropas parlamenta un Padomes Regulas (ES) 2018/1240 un (ES) 2019/818 un atceļ Eiropas Parlamenta un Padomes Regulu (ES) Nr. 603/2013 (OV L, 2024/1358, 22.5.2024., ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>).

4. Ieceļošanas/izceļošanas sistēma

Eiropas Parlamenta un Padomes Regula (ES) 2017/2226 (2017. gada 30. novembris), ar ko izveido ieceļošanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo ieceļošanas un izceļošanas datus un ieceļošanas atteikumu datus, kuri šķērso dalībvalstu ārējās robežas, un ar ko paredz nosacījumus piekļuvei IIS tiesībsardzības nolūkos, un ar ko groza Konvenciju, ar ko īsteno Šengenas nolīgumu, un Regulas (EK) Nr. 767/2008 un (ES) Nr. 1077/2011 (OV L 327, 9.12.2017., 20. lpp.).

5. Eiropas ceļošanas informācijas un atļauju sistēma

- a) Eiropas Parlamenta un Padomes Regula (ES) 2018/1240 (2018. gada 12. septembris), ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (ETIAS) un groza Regulas (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 un (ES) 2017/2226 (OV L 236, 19.9.2018., 1. lpp.).
- b) Eiropas Parlamenta un Padomes Regula (ES) 2018/1241 (2018. gada 12. septembris), ar ko Eiropas ceļošanas informācijas un atļauju sistēmas (ETIAS) izveides nolūkā groza Regulu (ES) 2016/794 (OV L 236, 19.9.2018., 72. lpp.).

6. Eiropas Sodū reģistru informācijas sistēma par trešo valstu valstspiederīgajiem un bezvalstniekiem
Eiropas Parlamenta un Padomes Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodamības reģistru informācijas sistēmas papildināšanai izveido centralizētu sistēmu (ECRIS-TCN) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (OV L 135, 22.5.2019., 1. lpp.).
 7. Sadarbība
 - a) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbībai robežu un vīzu jomā un ar ko groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).
 - b) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbībai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un ar ko groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (OV L 135, 22.5.2019., 85. lpp.).
-

XI PIELIKUMS

Tehniskā dokumentācija, kas minēta 53. panta 1. punkta a) apakšpunktā – tehniskā dokumentācija vispārīga lietojuma MI modeļu nodrošinātājiem

1. iedaļa

Informācija, kas jāsniedz visiem vispārīga lietojuma MI modeļu nodrošinātājiem

Tehniskajā dokumentācijā, kas minēta 53. panta 1. punkta a) apakšpunktā, norāda vismaz turpmāk uzskaitīto informāciju atbilstīgi modeļa lielumam un riska profilam.

1. Vispārīga lietojuma MI modeļa vispārīgs apraksts, kas ietver šādu informāciju:
 - a) uzdevumi, kādus modelim paredzēts veikt, un to MI sistēmu veids un raksturs, kādās to var integrēt;
 - b) piemērojamās pieļaujamās lietošanas politikas;
 - c) izlaides datums un izplatīšanas metodes;
 - d) arhitektūra un parametru skaits;
 - e) ievaddatu un iznākumu modalitāte (piemēram, teksts, attēls) un formāts;
 - f) licence.
2. Detalizēts 1. punktā minētā modeļa elementu apraksts un relevanta informācija par izstrādes procesu, kas ietver šādus elementus:
 - a) tehniskie līdzekļi (piemēram, lietošanas instrukcija, infrastruktūra, rīki), kas vajadzīgi, lai vispārīga lietojuma MI modeli integrētu MI sistēmās;
 - b) modeļa un apmācības procesa projekta specifikācijas, tostarp apmācības metodikas un metodes, galvenās projektēšanas izvēles, tostarp pamatojums un izdarītie pieņēmumi; ko ar modeli paredzēts optimizēt un, attiecīgi, kāda ir dažādo parametru nozīme;
 - c) attiecīgā gadījumā – informācija par apmācībai, validēšanai un testēšanai izmantotajiem datiem, tostarp datu veidu un izcelsmi un kūrēšanas metodiku (piemēram, tīrīšana, filtrēšana), datu punktu skaitu, to tvērumu un galvenajiem raksturlielumiem; to, kā dati iegūti un atlasīti, kā arī, attiecīgā gadījumā, citiem pasākumiem nolūkā atklāt datu avotu nepiemērotību un metodēm nolūkā atklāt identificējamu neobjektivitāti;
 - d) skaitļošanas resursi, ko izmanto modeļa apmācīšanai (piemēram, peldošā punkta operāciju skaits), apmācības laiks un cita būtiska informācija, kas saistīta ar apmācību;
 - e) modeļa zināmais vai aplēstais enerģijas patēriņš.

Attiecībā uz e) apakšpunktu, ja modeļa enerģijas patēriņš nav zināms, enerģijas patēriņu var balstīt uz informāciju par izmantotajiem skaitļošanas resursiem.

2. iedaļa

Papildu informācija, kas jāsniedz vispārīga lietojuma MI modeļu ar sistēmisku risku nodrošinātājiem

1. Izvērtēšanas stratēģiju detalizēts apraksts, ietverot izvērtēšanu rezultātus, pamatojoties uz pieejamiem publiskiem izvērtēšanas protokoliem un rīkiem vai citādi uz citām izvērtēšanas metodikām. Izvērtēšanas stratēģijas ietver izvērtēšanas kritērijus, rādītājus un metodiku saistībā ar ierobežojumu identifikāciju.
2. Attiecīgā gadījumā – detalizēts apraksts par pasākumiem, kas ieviesti, lai veiktu iekšēju un/vai ārēju pretinieckisko testēšanu (piemēram, sarkanās komandas pieeju (*red teaming*)), modeļa pielāgojumus, tostarp līdzināšanu un precīzu iestatīšanu.

3. Attiecīgā gadījumā – detalizēts sistēmas arhitektūras apraksts, kurā paskaidrots, kā programmatūras komponenti ir balstīti cits citā vai papildina cits citu un kā tie integrēti kopējā programmas darbībā.
-

XII PIELIKUMS

53. panta 1. punkta b) apakšpunktā minētā informācija par pārredzamību – tehniskā dokumentācija nodrošinātājiem, kas nodrošina vispārīga lietojuma MI modeļus lejasposma nodrošinātājiem, kuri integrē modeli savā MI sistēmā

53. panta 1. punkta b) apakšpunktā minētajā informācijā ietver vismaz:

1. Vispārīga lietojuma MI modeļa vispārēju aprakstu, kas ietver šādu informāciju:
 - a) uzdevumi, kādus modelim paredzēts veikt, un to MI sistēmu veids un raksturs, kādās to var integrēt;
 - b) piemērojamās pieļaujamās lietošanas politikas;
 - c) izlaides datums un izplatīšanas metodes;
 - d) attiecīgā gadījumā – kā modelis mijiedarbojas vai var tikt izmantots mijiedarbībai ar aparatūru vai programmatūru, kas nav paša modeļa daļa;
 - e) attiecīgā gadījumā – attiecīgās ar vispārīga lietojuma MI modeļa lietošanu saistītās programmatūras versijas;
 - f) arhitektūra un parametru skaits;
 - g) ievaddatu un iznākumu modalitāte (piemēram, teksts, attēls) un formāts;
 - h) modeļa licence.
2. Modeļa elementu un tās izstrādes procesa apraksts, kas ietver šādu informāciju:
 - a) tehniskie līdzekļi (piemēram, lietošanas instrukcija, infrastruktūra, rīki), kas vajadzīgi, lai vispārīga lietojuma MI modeli integrētu MI sistēmās;
 - b) ievaddatu un iznākumu modalitāte (piemēram, teksts, attēls) un formāts un to maksimālais izmērs (piemēram, konteksta loga garums, utt.);
 - c) attiecīgā gadījumā – informācija par apmācībai, validēšanai un testēšanai izmantotajiem datiem, tostarp datu veidu un izcelsmi un kūrēšanas metodiku.

XIII PIELIKUMS

Kritēriji atzīšanai par vispārīga lietojuma MI modeli ar sistēmisku risku, kas minēts 51. pantā

Lai noteiktu, vai vispārīga lietojuma MI modelim ir spējas vai ietekme, kas ir līdzvērtīga 51. panta 1. punkta a) apakšpunktā minētajām spējām vai ietekmei, Komisija ņem vērā šādus kritērijus:

- a) modeļa parametru skaits;
- b) datu kopu kvalitāte vai lielums, piemēram, mērot ar datsegmentiem;
- c) modeļa apmācībai izmantotais skaitļošanas resursu apjoms, mērīts peldošā punkta operācijās vai izteikts ar citu mainīgo lielumu kombināciju, piemēram, apmācības lēstās izmaksas, lēstais apmācībai nepieciešamais laiks vai lēstais enerģijas patēriņš apmācībai;
- d) modeļa ievades un izvades modalitātes, piemēram, no teksta uz tekstu (lielie valodu modeļi), no teksta uz attēlu, multimodalitāte un jaunākās robežvērtības augstas ietekmes spēju noteikšanai katrai modalitātei, un konkrētais ievaddatu un iznākumu veids (piemēram, bioloģiskās sekvences);
- e) modeļa spēju kritēriji un izvērtēšanas, tostarp ņemot vērā uzdevumu skaitu bez papildu apmācības, spēju pielāgoties jaunu, atšķirīgu uzdevumu apguvei, tā autonomijas pakāpi un mērogojamību, rīkus, kuriem tam ir piekļuve;
- f) vai tam ir liela ietekme uz iekšējo tirgu tā tvēruma dēļ – to tā pieņem, kad modelis ir darīts pieejams vismaz 10 000 reģistrētu komerciālo lietotāju, kas iedibināti Savienībā;
- g) reģistrēto galalietotāju skaits.