EUROPOS
KOMISIJA

Briuselis, 2021 04 21
COM(2021) 206 final

2021/0106 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

KURIUO NUSTATOMOS SUDERINTOS DIRBTINIO INTELEKTO TAISYKLĖS (DIRBTINIO INTELEKTO AKTAS) IR IŠ DALIES KEIČIAMI TAM TIKRI SĄJUNGOS TEISĖKŪROS PROCEDŪRA PRIIMTI AKTAI

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

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

1.1. Pasiūlymo pagrindimas ir tikslai

Šis aiškinamasis memorandumas pridedamas prie pasiūlymo dėl reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas). Dirbtinis intelektas (DI) – tai greitai vystoma technologijų grupė. Šios technologijos gali duoti visokeriopą ekonominę ir visuomeninę naudą pačiose įvairiausiose pramonės šakose ir socialinės veiklos srityse. Dirbtinis intelektas prisideda prie geresnės predikcijos, operacijų optimizavimo, išteklių paskirstymo ir paslaugų pritaikymo prie individualių poreikių, todėl jis gali padėti siekti socialiniu ir aplinkos požiūriu naudingų rezultatų ir suteikti įmonėms bei Europos ekonomikai svarbių konkurencinių pranašumų. Tokie veiksmai ypač reikalingi didelį poveikį darančiuose sektoriuose, kaip antai klimato kaitos, aplinkos ir sveikatos, viešojo sektoriaus, finansų, judumo, vidaus reikalų ir žemės ūkio. Tačiau tie patys aspektai ir metodai, kurie sudaro sąlygas siekti socialinės ir ekonominės naudos panaudojant DI, taip pat gali sukelti naują riziką arba neigiamas pasekmes asmenims arba visuomenei. Atsižvelgdama į sparčius technologinius pokyčius ir galimas problemas, ES yra įsipareigojusi siekti subalansuoto požiūrio. Sąjunga suinteresuota užtikrinti tolesnį ES technologinį pirmavimą bei užtikrinti, kad europiečiai galėtų naudotis naujomis technologijomis, kurios yra sukurtos ir veikia laikantis Sąjungos vertybių, pagrindinių teisių ir principų.

Šis pasiūlymas grindžiamas Komisijos pirmininkės U. von der Leyen politiniu įsipareigojimu, apie kurį ji pranešė savo 2019–2024 m. Komisijos politinėse gairėse „Daugiau siekianti Sąjunga“[1]. Vykdydama šį politinį įsipareigojimą, Komisija turi pateikti teisės aktą dėl suderinto Europos požiūrio į DI poveikį žmogui ir etikai. Po šio pranešimo 2020 m. vasario 19 d. Komisija paskelbė baltąją knygą „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“[2]. Baltojoje knygoje nustatytos politikos galimybės, kaip pasiekti dvejopą tikslą, t. y. skatinti plačiau diegti DI ir mažinti su tam tikrais tokios technologijos naudojimo būdais susijusią riziką. Šiuo pasiūlymu siekiama antrojo tikslo, susijusio su pasitikėjimo ekosistemos sukūrimu pasiūlant teisinę sistemą, kuria reglamentuojamas patikimas DI. Pasiūlymas grindžiamas ES vertybėmis ir pagrindinėmis teisėmis ir juo siekiama suteikti asmenims ir kitiems naudotojams pasitikėjimo priimti DI pagrįstus sprendimus, kartu skatinant įmones juos plėtoti. DI turėtų būti žmonėms skirta ir visuomenės poreikius tenkinanti priemonė, kurios galutinis tikslas – didinti žmonių gerovę. Todėl Sąjungos rinkoje prieinamą ar kitaip Sąjungoje esantiems asmenims poveikį darantį DI reglamentuojančios taisyklės turėtų būti orientuotos į žmogų, kad žmonės galėtų būti tikri, jog technologija naudojama saugiai ir laikantis teisės aktų bei gerbiant pagrindines teises. Paskelbusi baltąją knygą, Komisija pradėjo didelį suinteresuotųjų subjektų susidomėjimą sukėlusias plataus masto konsultacijas su suinteresuotaisiais subjektais, kurie iš esmės pritarė reglamentavimo intervencijai, siekiant spręsti su vis dažnesniu DI naudojimu susijusias problemas ir klausimus.

Pasiūlyme taip pat atsižvelgiama į aiškius Europos Parlamento (EP) ir Europos Vadovų Tarybos prašymus, kuriuose ne kartą buvo raginama imtis teisėkūros veiksmų, siekiant užtikrinti gerai veikiančią dirbtinio intelekto sistemų (DI sistemos) vidaus rinką, kurioje Sąjungos lygmeniu būtų tinkamai sprendžiami tiek DI naudos, tiek keliamos rizikos

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

[2] Europos Komisijos Baltoji knyga „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“, COM (2020) 65 *final*, 2020 m.

klausimai. Jame pritariama siekiui, kad Sąjunga pirmautų pasaulyje plėtojant saugų, patikimą ir etišką dirbtinį intelektą, kaip nurodė Europos Vadovų Taryba[3], ir užtikrintų etinių principų apsaugą, kaip to konkrečiai prašė Europos Parlamentas[4].

2017 m. Europos Vadovų Taryba paragino „suvok[ti], kad reikia skubiai reaguoti į besiformuojančias tendencijas“, įskaitant „klausimus, susijusius su dirbtiniu intelektu, <...> kartu užtikrinant aukšto lygio duomenų apsaugą, skaitmenines teises ir etikos standartus“[5]. Savo 2019 m. išvadose dėl suderinto Europoje kuriamo dirbtinio intelekto plėtros ir naudojimo plano[6] Taryba dar kartą pabrėžė, kad svarbu užtikrinti visapusišką pagarbą Europos piliečių teisėms, ir paragino peržiūrėti dabartinius atitinkamus teisės aktus, kad jie būtų tikslingi atsižvelgiant į naujas DI suteikiamas galimybes ir keliamas problemas. Europos Vadovų Taryba taip pat paragino aiškiai nuspręsti, kurios DI prietaikos turėtų būti laikomos keliančiomis didelę riziką[7].

Naujausiose 2020 m. spalio 21 d. išvadose dar kartą paraginta spręsti tam tikrų DI sistemų neskaidrumo, sudėtingumo, šališkumo, tam tikro laipsnio nenuspėjamumo ir iš dalies autonomiško veikimo klausimus, siekiant užtikrinti jų suderinamumą su pagrindinėmis teisėmis ir palengvinti teisinių taisyklių vykdymo užtikrinimą[8].

Europos Parlamentas taip pat nemažai nuveikė DI srityje. 2020 m. spalio mėn. jis priėmė įvairias rezoliucijas, susijusias su DI, įskaitant rezoliucijas dėl etikos[9], atsakomybės[10] ir autorių teisių[11]. 2021 m. po minėtų rezoliucijų buvo priimtos rezoliucijos dėl DI baudžiamosiose bylose[12] ir DI švietimo, kultūros ir audiovizualiniame sektoriuje[13]. EP rezoliucijoje dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos Komisijai konkrečiai rekomenduojama pasiūlyti teisėkūros veiksmus siekiant išnaudoti DI teikiamas galimybes ir privalumus, kartu užtikrinant etikos principų apsaugą. Rezoliucijoje pateiktas pasiūlymo dėl teisėkūros procedūra priimamo reglamento dėl etikos principų, kurių reikia laikytis plėtojant, diegiant ir naudojant DI, robotiką ir susijusias technologijas, tekstas. Remiantis politiniu įsipareigojimu, kurį, atsižvelgdama į Europos Parlamento pagal SESV 225 straipsnį priimtas rezoliucijas, savo politinėse gairėse davė Pirmininkė U. von der Leyen,

---

3 Europos Vadovų Taryba, Specialusis Europos Vadovų Tarybos susitikimas (2020 m. spalio 1 ir 2 d.). Išvados, EUCO 13/20, 2020 m., p. 6.

4 2020 m. spalio 20 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos, 2020/2012(INL).

5 Europos Vadovų Taryba, *Europos Vadovų Tarybos susitikimas (2017 m. spalio 19 d.). Išvados*, EUCO 14/17, 2017 m., p. 8.

6 Europos Sąjungos Taryba, *Dirbtinis intelektas b) Išvados dėl suderinto dirbtinio intelekto plano. Priėmimas*, 6177/19, 2019 m.

7 Europos Vadovų Taryba, *Specialusis Europos Vadovų Tarybos susitikimas (2020 m. spalio 1 ir 2 d.). Išvados*, EUCO 13/20, 2020 m.

8 Europos Sąjungos Taryba, *Pirmininkavimo išvados. Pagrindinių teisių chartija dirbtinio intelekto ir skaitmeninių pokyčių kontekste*, 11481/20, 2020 m.

9 2020 m. spalio 20 d. Europos Parlamento rezoliucija dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos, 2020/2012(INL).

10 2020 m. spalio 20 d. Europos Parlamento rezoliucija dėl naudojant dirbtinį intelektą taikomos civilinės atsakomybės tvarkos, 2020/2014(INL).

11 2020 m. spalio 20 d. Europos Parlamento rezoliucija dėl intelektinės nuosavybės teisių plėtojant dirbtinio intelekto technologijas, 2020/2015(INI).

12 Europos Parlamento pranešimo projektas „Dirbtinis intelektas baudžiamojoje teisėje ir jo naudojimas policijoje ir teisminėse institucijose nagrinėjant baudžiamąsias bylas“, 2020/2016(INI).

13 Europos Parlamento pranešimo projektas „Dirbtinis intelektas švietimo, kultūros ir audiovizualiniame sektoriuje“, 2020/2017(INI). Šiuo atžvilgiu Komisija priėmė 2021–2027 m. skaitmeninio švietimo veiksmų planą „Švietimo ir mokymo pritaikymas prie skaitmeninio amžiaus“, kuriame nustatytos etikos gairės dėl DI ir duomenų naudojimo švietimo srityje, Komisijos komunikatas, COM(2020) 624 *final*.

šiame pasiūlyme į minėtą Europos Parlamento rezoliuciją atsižvelgiama visapusiškai paisant proporcingumo, subsidiarumo ir geresnio reglamentavimo principų.

Atsižvelgdama į šį politinį kontekstą, Komisija teikia siūlomą dirbtinio intelekto reglamentavimo sistemą, kuria siekia šių **konkrečių tikslų**:

- užtikrinti, kad Sąjungos rinkai pateikiamos ir naudojamos DI sistemos būtų saugios ir derėtų su dabartiniais pagrindines teises ir Sąjungos vertybes reglamentuojančiais teisės aktais;
- užtikrinti teisinį tikrumą, siekiant sudaryti palankesnes sąlygas investicijoms ir inovacijoms DI srityje;
- gerinti valdymą ir veiksmingą dabartinių teisės aktų, kuriais reglamentuojamos pagrindinės teisės ir DI sistemoms taikytini saugos reikalavimai, vykdymo užtikrinimą;
- palengvinti bendrosios teisėtų, saugių ir patikimų DI prietaikų rinkos plėtrą ir užkirsti kelią rinkos susiskaidymui.

Siekiant šių tikslų, šiame pasiūlyme pateikiamas subalansuotas ir proporcingas horizontalusis požiūris į DI reglamentavimą, apimantis minimalius būtinus reikalavimus, kad būtų pašalinta su DI susijusi rizika ir problemos, nepagrįstai neapribojant ir netrukdant technologinės plėtros arba kitaip neproporcingai nepadidinant DI sprendimų pateikimo rinkai išlaidų. Pasiūlymu nustatoma patikima ir lanksti teisinė sistema. Viena vertus, ji, atsižvelgiant į pagrindinius sprendimus reglamentavimo srityje, įskaitant principais grindžiamus reikalavimus, kuriuos turėtų atitikti DI sistemos, yra išsami ir orientuota į ateitį. Kita vertus, ja nustatoma proporcinga reglamentavimo sistema, grindžiama tinkamai apibrėžtu, rizika pagrįstu reglamentavimo metodu, kuriuo nesukuriami nereikalingi apribojimai prekybai, pagal kurį teisinė intervencija pritaikoma prie tų konkrečių situacijų, kuriose yra pagrįsta priežastis susirūpinti arba kai tokį susirūpinimą galima pagrįstai numatyti artimiausioje ateityje. Kartu teisinėje sistemoje numatyti lankstūs mechanizmai, kurie sudaro sąlygas ją dinamiškai pritaikyti prie technologinių pokyčių ir naujų susirūpinimą keliančių situacijų.

Pasiūlyme, vadovaujantis proporcingu rizika pagrįstu metodu, nustatytos suderintos DI sistemų plėtojimo, pateikimo rinkai ir naudojimo Sąjungoje taisyklės. Jame pasiūlyta bendra į ateitį orientuota DI apibrėžtis. Tam tikra ypač žalinga DI praktika draudžiama, kaip prieštaraujanti Sąjungos vertybėms, o tam tikram nuotolinio biometrinio tapatybės nustatymo sistemų naudojimui teisėsaugos tikslais siūlomi konkretūs apribojimai ir apsaugos priemonės. Pasiūlyme nustatyta patikima rizikos metodika, kuria remiantis apibrėžiamos didelės rizikos DI sistemos, keliančios didelę riziką asmenų sveikatai ir saugai arba pagrindinėms teisėms. Šios DI sistemos turės atitikti patikimam DI taikomą rinkinį horizontalių privalomų reikalavimų ir prieš šias sistemas pateikiant Sąjungos rinkai turės būti atliktos atitikties vertinimo procedūros. Šių sistemų tiekėjams ir naudotojams taip pat nustatomos nuspėjamos, proporcingos ir aiškios pareigos, siekiant per visą DI sistemų gyvavimo ciklą užtikrinti saugumą ir atitiktį galiojantiems teisės aktams, kuriais saugomos pagrindinės teisės. Dėl kai kurių konkrečių DI sistemų siūlomos tik minimalios skaidrumo pareigos, visų pirma tais atvejais, kai naudojami pokalbių robotai arba sintetinė sankaita (angl. *deep fakes*).

Pasiūlytų taisyklių vykdymas bus užtikrinamas naudojant valstybės narės lygmens valdymo sistemą, pagrįstą jau esamomis struktūromis, ir Sąjungos lygmens bendradarbiavimo mechanizmu, kartu įsteigiant Europos dirbtinio intelekto valdybą. Siekiant paremti inovacijas, taip pat siūlomos papildomos priemonės, visų pirma per DI apribotą bandomąją reglamentavimo aplinką, ir kitos priemonės, kuriomis siekiama sumažinti reglamentavimo naštą ir paremti mažąsias ir vidutines įmones (MVĮ) bei startuolius.

1.2. Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis

Atsižvelgiant į pasiūlymo horizontalųjį pobūdį, būtina užtikrinti visišką nuoseklumą su dabartiniais Sąjungos teisės aktais, taikomais sektoriuose, kuriuose jau naudojamos arba artimiausioje ateityje gali būti naudojamos didelės rizikos DI sistemos.

Taip pat užtikrinamas nuoseklumas su ES pagrindinių teisių chartija ir esamais antriniais Sąjungos teisės aktais, reglamentuojančiais duomenų apsaugą, vartotojų apsaugą, nediskriminavimą ir lyčių lygybę. Pasiūlymas nedaro poveikio Bendrajam duomenų apsaugos reglamentui (Reglamentas (ES) 2016/679) ir Teisėsaugos direktyvai (Direktyva (ES) 2016/680) ir juos papildo suderintų taisyklių, taikomų tam tikrų didelės rizikos DI sistemų projektavimui, plėtojimui ir naudojimui, rinkiniu ir tam tikrų nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo būdų apribojimais. Be to, pasiūlymas papildo esamus Sąjungos teisės aktus dėl nediskriminavimo, taikant konkrečius reikalavimus, kuriais siekiama kuo labiau sumažinti algoritminės diskriminacijos riziką, visų pirma atsižvelgiant į duomenų rinkinių, naudojamų kuriant DI sistemas, struktūrą ir kokybę, kartu šias sistemas papildant bandymo, rizikos valdymo, dokumentacijos ir žmogiškosios priežiūros per visą DI sistemų gyvavimo ciklą pareigomis. Pasiūlymas nedaro poveikio Sąjungos konkurencijos teisės taikymui.

Kalbant apie didelės rizikos DI sistemas, kurios yra gaminių saugos komponentai, pažymėtina, kad šis pasiūlymas bus integruotas į esamus sektorių saugumo teisės aktus, siekiant užtikrinti nuoseklumą, išvengti dubliavimo ir kuo labiau sumažinti papildomą naštą. Visų pirma dėl didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi naujosios teisės aktų sistemos teisės aktai (pvz., mašinos, medicinos prietaisai, žaislai), pažymėtina, kad šiame pasiūlyme išdėstyti DI sistemoms taikomi reikalavimai bus patikrinti pagal naująją teisės aktų sistemą atliekant dabartines atitikties vertinimo procedūras. Dėl reikalavimų sąveikos pažymėtina, kad nors būtent su DI sistemomis susijusi saugumo rizika turi būti šalinama laikantis šio pasiūlymo reikalavimų, naujosios teisės aktų sistemos teisės aktais siekiama užtikrinti bendrą galutinio gaminio saugumą, todėl jame gali būti nustatyti konkretūs reikalavimai, susiję su saugiu DI sistemos integravimu į galutinį gaminį. Pasiūlymas dėl mašinų reglamento, kuris priimamas tą pačią dieną kaip ir šis pasiūlymas, visiškai dera su šiuo metodu. Dėl didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi atitinkami senojo požiūrio teisės aktai (pvz., aviacija, automobiliai), pažymėtina, kad šis pasiūlymas nebus tiesiogiai taikomas tokiems gaminiams. Tačiau į šiame pasiūlyme išdėstytus *ex ante* esminius reikalavimus didelės rizikos DI sistemoms reikės atsižvelgti pagal tuos aktus priimant įgyvendinimo arba deleguotuosius teisės aktus.

Dėl DI sistemų, kurias teikia arba naudoja reguliuojamos kredito įstaigos, pažymėtina, kad už Sąjungos finansines paslaugas reglamentuojančių teisės aktų priežiūrą atsakingos institucijos turėtų būti paskirtos kompetentingomis šio pasiūlymų reikalavimų priežiūros institucijomis, siekiant užtikrinti nuoseklų šiame pasiūlyme ir Sąjungos finansines paslaugas reglamentuojančiuose teisės aktuose nustatytų pareigų vykdymą tais atvejais, kai DI sistemos turi būti tam tikru mastu numanomai reguliuojamos atsižvelgiant į kredito įstaigų vidaus valdymo sistemą. Siekiant toliau didinti nuoseklumą, šiame pasiūlyme nustatyta atitikties vertinimo procedūra ir kai kurios tiekėjų procedūrinės pareigos integruojamos į Direktyvoje 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios priežiūros numatytas procedūras[14].

[14] 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš

Šis pasiūlymas taip pat dera su taikytinais Sąjungos teisės aktais dėl paslaugų, įskaitant tarpininkavimo paslaugas, kurios reglamentuojamos E. prekybos direktyva 2000/31/EB[15], ir su naujausiu Komisijos pasiūlymu dėl Skaitmeninių paslaugų akto (SPA)[16].

Dėl DI sistemų, kurios yra Europos Sąjungos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūros (eu-LISA) valdomų didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje sudedamosios dalys, pažymėtina, kad pasiūlymas nebus taikomas toms DI sistemoms, kurios rinkai buvo pateiktos arba pradėtos naudoti anksčiau nei praėjus vieniems metams nuo šio reglamento įsigaliojimo, išskyrus atvejus, kai dėl tų teisės aktų panaikinimo arba pakeitimo atsiranda esminių DI sistemos arba atitinkamų DI sistemų struktūros arba numatytosios paskirties pokyčių.

1.3. Suderinamumas su kitomis Sąjungos politikos sritimis

Pasiūlymas yra išsamesnio priemonių, kuriomis sprendžiamos DI kūrimo ir naudojimo keliamos problemos, rinkinio sudedamoji dalis, kaip aprašyta Baltojoje knygoje dėl DI. Todėl nuoseklumas ir papildomumas užtikrinami kitomis įgyvendinamomis ar planuojamomis Komisijos iniciatyvomis, kuriomis taip pat siekiama spręsti šias problemas, įskaitant sektorinių gaminių teisės aktų (pvz., Mašinų direktyvos, Bendrosios gaminių saugos direktyvos) peržiūrą ir iniciatyvas, kuriomis sprendžiami atsakomybės klausimai, susiję su naujosiomis technologijomis, įskaitant DI sistemas. Šios iniciatyvos bus grindžiamos šiuo pasiūlymu ir jį papildys, siekiant suteikti teisinį tikrumą ir skatinti pasitikėjimo DI ekosistemos plėtrą Europoje.

Pasiūlymas taip pat dera su Komisijos bendra skaitmenine strategija, nes juo padedama skatinti žmonėms tarnaujančią technologiją, kuri yra vienas iš trijų pagrindinių politikos gairių ir tikslų, paskelbtų komunikate „Europos skaitmeninės ateities formavimas“, ramsčių[17]. Jame nustatyta nuosekli, veiksminga ir proporcinga sistema, kuria siekiama užtikrinti, kad DI būtų kuriamas gerbiant žmogaus teises ir užsitarnaujant žmonių pasitikėjimą, taip padedant Europai prisitaikyti prie skaitmeninio amžiaus ir artimiausius dešimt metų paversti **skaitmeniniu dešimtmečiu**[18].

Be to, DI grindžiamų inovacijų skatinimas yra glaudžiai susijęs su **Duomenų valdymo aktu**[19]**, Atvirųjų duomenų direktyva**[20] ir kitomis **ES duomenų strategijos**[21] iniciatyvomis, kurios padės sukurti patikimus mechanizmus ir paslaugas, skirtas pakartotiniam duomenų, turinčių esminę reikšmę duomenimis grindžiamų kokybiškų DI modelių kūrimui, naudojimui, dalijimuisi jais ir jų kaupimui.

---

dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (Tekstas svarbus EEE), OL L 176, 2013 6 27, p. 338–436.

15 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva), OL L 178, 2000 7 17, p. 1–16.

16 Žr. pasiūlymą dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO dėl bendrosios skaitmeninių paslaugų rinkos (Skaitmeninių paslaugų aktas), kuriuo iš dalies keičiama Direktyva 2000/31/EB, COM(2020) 825 *final*.

17 Komisijos komunikatas „Europos skaitmeninės ateities formavimas“, COM(2020) 67 *final*.

18 Europos skaitmeninis dešimtmetis.2030 m. skaitmeniniai tikslai.

19 Pasiūlymas dėl reglamento dėl Europos duomenų valdymo (Duomenų valdymo aktas) COM/2020/767.

20 2019 m. birželio 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/1024 dėl atvirųjų duomenų ir viešojo sektoriaus informacijos pakartotinio naudojimo, PE/28/2019/REV/1, OL L 172, 2019 6 26, p. 56–83.

21 Komisijos komunikatas „Europos duomenų strategija“, COM/2020/66 *final*.

Pasiūlymu taip pat sustiprinamas Sąjungos vaidmuo padedant formuoti pasaulines normas ir standartus, taip pat skatinti patikimą DI, kuris dera su Sąjungos vertybėmis ir interesais. Juo Sąjungai suteikiamas tvirtas pagrindas toliau bendradarbiauti su savo išorės partneriais, įskaitant trečiąsias valstybes, ir tarptautiniu mastu sprendžiant su DI susijusius klausimus.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

2.1. Teisinis pagrindas

Pasiūlymo teisinis pagrindas visų pirma yra Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 114 straipsnis, kuriame numatyta galimybė priimti priemones, siekiant užtikrinti vidaus rinkos sukūrimą ir veikimą.

Pasiūlymas yra pagrindinė ES bendrosios skaitmeninės rinkos strategijos dalis. Pagrindinis šio pasiūlymo tikslas – užtikrinti tinkamą vidaus rinkos veikimą nustatant suderintas taisykles, visų pirma susijusias su gaminių ir paslaugų, kuriuose naudojamos DI technologijos arba kurie tiekiami kaip atskiros DI sistemos, kūrimu, pateikimu Sąjungos rinkai ir naudojimu. Kai kurios valstybės narės jau svarsto galimybę priimti nacionalines taisykles, siekiant užtikrinti, kad AI būtų saugus ir kuriamas bei naudojamas laikantis pagrindinių teisių ir pareigų. Tikėtina, kad dėl to kils dvi pagrindinės problemos: i) vidaus rinkos susiskaidymas dėl esminių elementų, susijusių visų pirma su DI gaminiams ir paslaugoms keliamais reikalavimais, prekyba šiais gaminiais ir paslaugomis, valdžios institucijų atsakomybe ir priežiūra, ir ii) gerokai sumažėjęs DI sistemų tiekėjų ir naudotojų teisinis tikrumas, susijęs su tuo, kaip esamos ir naujos taisyklės Sąjungoje bus taikomos šioms sistemoms. Turint omeny, kad ir paslaugos gaminiai plačiai tiekiami tarpvalstybiniu mastu, šias dvi problemas geriausiai galima išspręsti priimant suderintą ES teisės aktą.

Iš tiesų pasiūlyme apibrėžiami bendri privalomi reikalavimai, taikomi tam tikrų DI sistemų projektavimui ir kūrimui prieš jas pateikiant rinkai; jie bus toliau rengiami nustatant suderintus techninius standartus. Pasiūlyme taip pat aptariama padėtis po DI sistemų pateikimo rinkai, šiuo tikslu suderinant *ex post* kontrolės priemonių įgyvendinimo būdą.

Be to, atsižvelgiant į tai, kad šiame pasiūlyme yra tam tikrų konkrečių taisyklių dėl asmenų apsaugos tvarkant asmens duomenis, visų pirma kiek tai susiję su apribojimais naudoti DI sistemas tikralaikiam nuotoliniam biometriniam tapatybės nustatymui viešosiose erdvėse teisėsaugos tikslais, šį reglamentą, kiek tai susiję su konkrečiomis taisyklėmis, būtų tinkama grįsti SESV 16 straipsniu.

2.2. Subsidiarumo principas (neišimtinės kompetencijos atveju)

DI, kuris dažnai grindžiamas dideliais ir įvairiais duomenų rinkiniais ir gali būti integruotas į bet kurį laisvai vidaus rinkoje platinamą gaminį arba paslaugą, pobūdis lemia tai, kad valstybės narės negali veiksmingai pasiekti šio pasiūlymo tikslų veikdamos atskirai. Be to, gali būti, kad bus kuriamos skirtingos nacionalinės taisyklės, kurios trukdys sklandžiam su DI sistemomis susijusių gaminių ir paslaugų judėjimui ES ir veiksmingai neužtikrins pagrindinių teisių ir Sąjungos vertybių įvairiose valstybėse narėse saugumą ir apsaugą. Dėl nacionalinių problemų sprendimo metodų paprasčiausiai atsiras daugiau teisinio netikrumo ir kliūčių, o DI įsisavinimas rinkoje bus lėtesnis.

Šio pasiūlymo tikslą galima geriau pasiekti Sąjungos lygmeniu, siekiant išvengti tolesnio bendrosios rinkos susiskaidymo į potencialiai prieštaraujančias nacionalines sistemas, kurios užkirstų kelią laisvam DI grindžiamų prekių ir paslaugų judėjimui. Tvirta patikimo DI Europos reglamentavimo sistema taip pat padės užtikrinti vienodas sąlygas ir visų žmonių apsaugą, kartu stiprinant Europos konkurencingumą ir DI pramoninį pagrindą. Tik imantis

bendrų veiksmų Sąjungos lygmeniu taip pat galima apsaugoti Sąjungos skaitmeninį suverenitetą ir suderinti priemones ir reglamentavimo įgaliojimus, siekiant formuoti pasaulines taisykles ir standartus.

2.3. Proporcingumo principas

Pasiūlymas grindžiamas esamomis teisinėmis sistemomis ir yra proporcingas bei būtinas siekiant nustatytų tikslų, nes jame vadovaujamasi rizika pagrįstu metodu ir reglamentavimo našta nustatoma tik kai DI sistema gali kelti didelę riziką pagrindinėms teisėms ir saugumui. Dėl kitų didelės rizikos nekeliančių DI sistemų nustatomos tik labai ribotos skaidrumo pareigos, pavyzdžiui, susijusios su informacijos teikimu, siekiant paženklinti su žmonėmis sąveikaujančios DI sistemos naudojimą. Didelės rizikos DI sistemų atveju griežtai būtina parengti kokybiškų duomenų, dokumentacijos, atsekamumo, skaidrumo, žmogiškosios priežiūros, tikslumo ir patikimumo reikalavimus, siekiant sumažinti riziką pagrindinėms teisėms ir saugumui, kurią kelia DI ir kuri neaptariama kitose esamose teisinėse sistemose. Darnieji standartai ir pagalbinės gairės bei atitikties priemonės padės tiekėjams ir naudotojams laikytis pasiūlyme nustatytų reikalavimų ir kuo labiau sumažinti patiriamas išlaidas. Veiklos vykdytojų patiriamos išlaidos yra proporcingos pasiektiems tikslams ir ekonominei bei reputacinei naudai, kurios veiklos vykdytojai gali tikėtis iš šio pasiūlymo.

2.4. Priemonės pasirinkimas

Reglamento, kaip teisinės priemonės, pasirinkimas grindžiamas poreikiu vienodai taikyti naujas taisykles, pavyzdžiui, dėl DI apibrėžties, draudimo taikyti tam tikrą žalingą DI grindžiamą praktiką ir tam tikrų DI sistemų klasifikavimo. Tiesioginis reglamento taikymas pagal SESV 288 straipsnį padės sumažinti teisinį susiskaidymą ir teisėtų, saugių ir patikimų DI sistemų bendrosios rinkos plėtrą. Tai visų pirma bus daroma nustatant suderintų pagrindinių reikalavimų, susijusių su DI sistemomis, kurios klasifikuojamos kaip didelės rizikos, ir šių sistemų tiekėjams ir naudotojams taikomų pareigų rinkinį, taip pagerinant pagrindinių teisių apsaugą ir suteikiant vienodą teisinį tikrumą tiek veiklos vykdytojams, tiek vartotojams.

Kartu reglamento nuostatos nėra pernelyg griežtos ir jomis valstybėms narėms paliekama erdvės įvairiais lygmenimis imtis veiksmų dėl aspektų, kuriais nepažeidžiamas iniciatyvos tikslas, visų pirma tai pasakytina apie rinkos priežiūros sistemos vidaus organizavimą ir inovacijų skatinimo priemonių panaudojimą.

3. EX POST VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

3.1. Konsultacijos su suinteresuotosiomis šalimis

Šis pasiūlymas – tai plataus masto konsultacijų su visomis pagrindinėmis suinteresuotosiomis šalimis rezultatas. Jų metu buvo taikomi Komisijos konsultacijų su suinteresuotosiomis šalimis bendrieji principai ir būtinieji standartai.

Internetinės viešos konsultacijos buvo pradėtos 2020 m. vasario 19 d. tuo pat metu, kai buvo paskelbta Baltoji knyga dėl dirbtinio intelekto, ir tęsėsi iki 2020 m. birželio 14 d. Šių konsultacijų tikslas buvo išsiaiškinti požiūrį ir nuomonę apie baltąją knygą. Jos buvo skirtos visoms viešojo ir privačiojo sektoriaus suinteresuotosioms šalims, įskaitant vyriausybes, vietos valdžios institucijas, komercines ir nekomercines organizacijas, socialinius partnerius,

ekspertus, akademinės bendruomenės narius ir piliečius. Išanalizavusi visus gautus atsakymus, Komisija savo svetainėje paskelbė rezultatų santrauką ir pavienius atsakymus[22].

Iš viso gauta 1 215 atsakymų, iš kurių 352 atsakymus pateikė įmonės arba verslo organizacijos ir (arba) asociacijos, 406 atsakymus – pavieniai asmenys (92 proc. asmenų iš ES), 152 atsakymai pateikti mokslo / mokslinių tyrimų įstaigų vardu ir 73 atsakymus pateikė valdžios institucijos. Pilietinės visuomenės nuomonę pareiškė 160 respondentų (tarp kurių 9 vartotojų organizacijos, 129 nevyriausybinės organizacijos ir 22 profesinės sąjungos), 72 respondentai savo nuomonę pareiškė kaip „kiti“ respondentai. Iš 352 verslo ir pramonės atstovų, 222 buvo įmonių ir verslo atstovai, 41,5 proc. iš jų – labai mažos, mažosios ir vidutinės įmonės. Likę respondentai – verslo asociacijos. Iš viso 84 proc. įmonių ir pramonės sektoriaus atsakymų gauta iš ES 27. Priklausomai nuo klausimo, 81–598 respondentų pasinaudojo galimybe pastabas pateikti laisvo teksto laukelyje. Iš viso ES apklausos svetainėje buvo pateikta 450 pozicijos dokumentų, kurie pridėti prie klausimyno atsakymų (daugiau nei 400) arba pateikti kaip atskiri dokumentai (daugiau nei 50).

Apskritai suinteresuotieji subjektai iš esmės sutaria, kad reikia imtis veiksmų. Dauguma suinteresuotųjų subjektų sutaria, kad esama teisės aktų spragų arba kad reikia naujų teisės aktų. Tačiau keletas suinteresuotųjų subjektų perspėjo Komisiją vengti dubliavimo, prieštaraujančių pareigų ir perteklinio reglamentavimo. Buvo pateikta nemažai pastabų, kuriose pažymima technologiškai neutralios ir proporcingos reglamentavimo sistemos svarba.

Suinteresuotieji subjektai dažniausiai reikalavo siaurai, aiškiai ir tiksliai apibrėžti DI. Suinteresuotieji subjektai taip pat pabrėžė, kad be DI sąvokos paaiškinimo, svarbu apibrėžti sąvokas „rizika“, „didelė rizika“, „nedidelė rizika“, „nuotolinis biometrinis tapatybės nustatymas“ ir „žala“.

Akivaizdu, kad dauguma respondentų palankiai vertina rizika pagrįstą metodą. Rizika pagrįstos sistemos naudojimas buvo laikomas geresne galimybe nei visų DI sistemų išsamus reglamentavimas. Rizikos ir grėsmių rūšys turėtų būti grindžiamos požiūriu į kiekvieną konkretų sektorių ir atvejį. Rizika taip pat turėtų būti įvertinama atsižvelgiant į poveikį teisėms ir saugumui.

Apribota reglamentavimo bandomoji aplinka galėtų būti labai naudinga skatinant DI ir ją palankiai vertina tam tikri suinteresuotieji subjektai, visų pirma verslo asociacijos.

Tarp respondentų, kurie pareiškė savo nuomonę dėl vykdymo užtikrinimo modelių, t. y. daugiau nei 50 proc., ypač tai pasakytina apie verslo asociacijas, palankiai vertino savarankiško *ex ante* rizikos vertinimo ir didelės rizikos DI sistemoms taikomų reikalavimų *ex post* vykdymo užtikrinimą.

3.2. Tiriamųjų duomenų rinkimas ir naudojimas

Pasiūlymas grindžiamas dvejų metų trukmės analize ir glaudžiu bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant akademinės bendruomenės narius, įmones, socialinius partnerius, nevyriausybines organizacijas, valstybes nares ir piliečius. Parengiamieji darbai pradėti 2018 m. sudarius **Aukšto lygio ekspertų grupę dirbtinio intelekto klausimais (HLEG)**, kurią, užtikrinant įtraukią ir plačią sudėtį, sudarė 52 gerai žinomi ekspertai, kuriems pavesta užduotis konsultuoti Komisiją jos dirbtinio intelekto strategijos įgyvendinimo klausimais. 2019 m. balandžio mėn. Komisija parėmė[23] pagrindinius reikalavimus, išdėstytus Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais parengtose patikimo DI gairėse[24],

[22] Visus konsultacijų rezultatus galima rasti čia.

[23] Europos Komisija, *Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas*, COM(2019) 168.

[24] Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais, *Patikimo DI etikos gairės*, 2019 m.

kurios buvo peržiūrėtos siekiant atsižvelgti į daugiau nei 500 pastabų, kurias pateikė suinteresuotieji subjektai. Pagrindiniuose reikalavimuose atsispindi plataus masto bendras požiūris, pagal kurį DI kūrimas ir naudojimas turi būti grindžiamas tam tikrais esminiais į vertybes orientuotais principais, kaip buvo pastebėta daugybėje įvairių Europos ir užsienio privačių ir viešųjų organizacijų parengtų etikos kodeksų ir principų. Dirbtinio intelekto patikimumo vertinimo kriterijų sąraše (angl. ALTAI)[25] šie reikalavimai buvo taikomi bandomajame procese, kuriame dalyvavo daugiau nei 350 organizacijų.

Be to, buvo suformuotas **DI aljansas**[26], kuris tapo apytiksliai 4 000 suinteresuotųjų subjektų vienijanti platforma, skirta technologinėms ir visuomeninėms DI pasekmėms aptarti, kurios svarbiausias renginys metinė asamblėja DI klausimais.

Baltojoje knygoje dėl DI toliau plėtojamas šis įtraukus požiūris, dėl kurio pastabas pateikė daugiau nei 1 250 suinteresuotųjų šalių, taip pat pateikta daugiau nei 450 papildomų pozicijos dokumentų. Todėl Komisija paskelbė įžanginį poveikio vertinimą, dėl kurio paskui sulaukta daugiau nei 130 pastabų[27]. Taip pat buvo surengti **papildomi suinteresuotųjų subjektų praktiniai seminarai ir renginiai**, kurių rezultatai padeda atlikti su poveikio vertinimu susijusią analizę ir įvertinti šiame pasiūlyme pateiktas politikos galimybes[28]. Taip pat buvo surengti viešieji pirkimai dėl **išorės tyrimo**, kuriuo buvo siekiama gauti informacijos poveikio vertinimui.

3.3. Poveikio vertinimas

Laikydamasi savo geresnio reglamentavimo politikos, Komisija atliko šio pasiūlymo poveikio vertinimą, kurį išnagrinėjo Komisijos reglamentavimo patikros valdyba. Susitikimas su Reglamentavimo patikros valdyba buvo surengtas 2020 m. gruodžio 16 d. ir jame buvo priimta neigiama nuomonė. Reglamentavimo patikros valdyba, iš esmės peržiūrėjusi poveikio vertinimą, siekdama atsižvelgti į pastabas, ir pakartotinai pateikus poveikio vertinimą, 2021 m. kovo 21 d. priėmė teigiamą nuomonę. Reglamentavimo patikros valdybos nuomonės, rekomendacijos ir paaiškinimai, kaip į jas buvo atsižvelgta, pateikti poveikio vertinimo 1 priede.

Komisija išnagrinėjo įvairias politikos galimybes siekiant bendro pasiūlymo tikslo – **užtikrinti tinkamą bendrosios rinkos veikimą** sukuriant sąlygas patikimo AI kūrimo ir naudojimo Sąjungoje sąlygas.

Buvo įvertintos keturios skirtingo reglamentavimo intervencijos laipsnio politikos galimybės:

- **1 galimybė –** ES teisėkūros priemonė, kuria nustatoma savanoriška ženklinimo sistema;
- **2 galimybė –** sektorinis *ad hoc* metodas;
- **3 galimybė –** horizontali ES teisėkūros priemonė, parengta vadovaujantis proporcingu rizika pagrįstu metodu;

---

[25] Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais, *Dirbtinio intelekto patikimumo vertinimo kriterijų sąrašas (angl. ALTAI), skirtas savarankiškam vertinimui atlikti*, 2020 m.

[26] DI aljansas yra 2018 m. birželio mėn. pradėjęs veikti įvairių suinteresuotųjų subjektų forumas, DI aljansas https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

[27] Europos Komisija, *Europos Parlamento ir Tarybos teisės akto, kuriuo nustatomi dirbtiniam intelektui taikomi reikalavimai, įžanginis poveikio vertinimas*.

[28] Daugiau informacijos apie visas surengtas konsultacijas žr. poveikio vertinimo 2 priedą.

- **3+ galimybė –** horizontali ES teisėkūros priemonė, parengta vadovaujantis proporcingu rizika pagrįstu metodu, įskaitant elgesio kodeksus didelės rizikos nekeliančioms DI sistemoms;
- **4 galimybė –** horizontali ES teisėkūros priemonė, nustatanti visoms DI sistemoms privalomus reikalavimus, nepaisant jų keliamos rizikos.

Remiantis Komisijos nustatyta metodika, kiekviena politikos galimybė buvo įvertinta atsižvelgiant į ekonominį ir visuomeninį poveikį, ypatingą dėmesį skiriant poveikiui pagrindinėms teisėms. Tinkamiausia galimybė yra 3+ galimybė, t. y. tik didelės rizikos DI sistemoms taikomai reglamentavimo sistemai, įskaitant galimybę visiems didelės rizikos nekeliančių DI sistemų tiekėjams vadovautis elgesio kodeksu. Reikalavimai bus susiję su duomenimis, dokumentavimu ir atsekamumu, informacijos teikimu ir skaidrumu, žmogaus atliekama priežiūra, patvarumu ir tikslumu, ir jie būtų privalomi didelės rizikos DI sistemoms. Įmonės, nustačiusios kitų DI sistemų elgesio kodeksus, tai darytų savanoriškai.

Tinkamiausia galimybė įvertinta, kaip tinkama, siekiant veiksmingiausiai įgyvendinti šios iniciatyvos tikslus. Pagal tinkamiausią galimybę reikalaujama, kad DI kūrėjai ir naudotojai imtųsi ribotų, tačiau veiksmingų veiksmų – taip ribojama žmogaus pagrindinių teisių ir saugumo pažeidimo rizika bei skatinama veiksminga priežiūra ir vykdymo užtikrinimas; šiuo tikslu reikalavimai taikomi tik toms sistemoms, kuriose kyla didelė tokių pažeidimų rizika. Todėl pagal tą galimybę reikalavimų laikymosi išlaidos išlaikomos kuo mažesnės, kartu išvengiant bereikalingų didesnių kainų ir reikalavimų laikymosi išlaidų sukeltų kliūčių greitam įsisavinimui. Siekiant pašalinti galimus neigiamus aspektus MVĮ, šią galimybę sudaro keletas nuostatų, kuriomis remiamas MVĮ reikalavimų laikymasis ir sumažinamos jų išlaidos, įskaitant apribotos bandomosios reglamentavimo aplinkos sukūrimą ir pareigą atsižvelgti į MVĮ interesus nustatant su atitikties vertinimu susijusius mokesčius.

Tinkamiausia galimybė padės padidinti žmonių pasitikėjimą DI, įmonėms bus naudingas teisinis tikrumas, o valstybės narės neturės pagrindo imtis vienašališkų veiksmų, dėl kurių gali atsirasti susiskaidymas bendrojoje rinkoje. Tikėtina, kad DI bendroji rinka suklestės dėl didesnės paklausos, kurią lems didesnis pasitikėjimas, platesnio prieinamų pasiūlymų asortimento, kurį lems teisinis tikrumas, ir kliūčių tarpvalstybiniam DI sistemų judėjimui nebuvimo. Europos Sąjunga toliau plėtos sparčiai augančią novatoriškų paslaugų ir gaminių, kuriuose naudojama DI technologija, arba atskirų DI sistemų DI ekosistemą, kuri prisidės prie didesnės skaitmeninės autonomijos.

Įmonės arba valdžios institucijos, kurios kuria ar naudoja DI prietaikas, keliančias ypač didelę riziką piliečių saugumui ar pagrindinėms teisėms, turėtų atitikti konkrečius reikalavimus ir dėl jų turėtų būti taikomi konkretūs įpareigojimai. Šių reikalavimų laikymasis reikštų maždaug 6 000–7 000 EUR išlaidas iki 2025 m. tiekiant vidutinę didelės rizikos DI sistemą, kurios apytikslė vertė – 170 000 EUR. DI naudotojai taip pat patirtų metines išlaidas, susijusias su žmogaus užtikrinama priežiūra, kai tai yra tinkama ir priklausomai nuo naudojimo būdo. Apskaičiuota, kad šios išlaidos siektų maždaug 5 000–8 000 EUR per metus. Didelės rizikos DI paslaugų teikėjų tikrinimo išlaidos galėtų siekti dar 3 000–7 500 EUR. Įmonėms arba valdžios institucijoms, kurios kuria arba naudoja bet kokias DI prietaikas, kurios neklasifikuojamos kaip didelės rizikos, bus nustatytos tik minimalios pareigos teikti informaciją. Vis dėlto jos gali nuspręsti drauge su kitais priimti elgesio kodeksą, siekdamos vadovautis tinkamais reikalavimais ir užtikrinti, kad jų DI sistemos būtų patikimos. Tokiu atveju išlaidos galėtų būti tokio pat dydžio, kaip ir didelės rizikos DI sistemų atveju, tačiau labiau tikėtina, kad jos būtų mažesnės.

Politikos galimybių poveikis įvairioms suinteresuotųjų subjektų kategorijoms (ekonominės veiklos vykdytojams / įmonėms; atitikties vertinimo įstaigoms, standartizacijos įstaigoms ir

kitoms viešosioms įstaigoms; asmenims / piliečiams; tyrėjams) išsamiai paaiškintas prie šio pasiūlymo pridėto poveikio vertinimo 3 priede.

3.4. Reglamentavimo tinkamumas ir supaprastinimas

Šiuo pasiūlymu nustatomos pareigos, kurios bus taikomos didelės rizikos DI sistemų tiekėjams ir naudotojams. Tokias sistemas kuriantiems ir Sąjungos rinkai pateikiantiems tiekėjams šiuo pasiūlymu bus sukurtas teisinis tikrumas ir užtikrinama, kad neatsirastų jokių kliūčių tarpvalstybiniam su DI susijusių paslaugų ir gaminių tiekimui. DI naudojančioms įmonėms tai padės skatinti pasitikėjimą tarp jų klientų. Nacionalinių viešojo administravimo institucijų atžvilgiu pasiūlymas padės skatinti visuomenės pasitikėjimą DI naudojimu ir stiprinti vykdymo užtikrinimo mechanizmus (nustatant Europos koordinavimo mechanizmą, suteikiant tinkamus pajėgumus ir palengvinant DI sistemų auditus nustatant naujus dokumentacijos, atsekamumo ir skaidrumo reikalavimus). Be to, sistemoje bus numatytos konkrečios inovacijų paramos priemonės, įskaitant apribotą bandomąją reglamentavimo aplinką ir konkrečias paramos priemones, skirtas smulkiesiems didelės rizikos DI sistemų naudotojams ir tiekėjams, kad būtų laikomasi naujų taisyklių.

Pasiūlymu taip pat konkrečiai siekiama stiprinti Europos konkurencingumą ir pramoninį pagrindą DI srityje. Užtikrinamas visiškas nuoseklumas su dabartiniais sektoriaus Sąjungos teisės aktais, taikomais DI sistemoms (pvz., gaminius ir paslaugas reglamentuojantys teisės aktai), ir tai padės suteikti dar daugiau aiškumo ir supaprastins naujų taisyklių vykdymo užtikrinimą.

3.5. Pagrindinės teisės

DI naudojimas, atsižvelgiant į jo konkrečius ypatumus (pvz., neskaidrumas, sudėtingumas, priklausomybė nuo duomenų, autonomiškas veikimas), gali daryti neigiamą poveikį įvairioms ES pagrindinių teisių chartijoje (toliau – Chartija) nustatytoms pagrindinėms teisėms. Šiuo pasiūlymu siekiama užtikrinti aukšto lygio šių pagrindinių teisių apsaugą ir siekiama pašalinti įvairius rizikos šaltinius, aiškiai apibrėžiant rizika pagrįstą metodą. Pasiūlyme nustatant patikimo DI reikalavimus ir proporcingas pareigas visiems vertės grandinės dalyviams bus stiprinama ir skatinama pagal Chartiją saugomų teisių apsauga: teisė į žmogaus orumą (1 straipsnis), teisė į privatų gyvenimą ir asmens duomenų apsaugą (7 ir 8 straipsniai), nediskriminavimas (21 straipsnis) ir moterų ir vyrų lygybė (23 straipsnis). Juo siekiama užkirsti kelią tam, kad nebūtų atgrasoma naudotis saviraiškos teise (11 straipsnis) ir susirinkimų laisve (12 straipsnis), taip pat užtikrinti teisės į veiksmingą teisių gynimo priemonę ir teisės į teisingą bylos nagrinėjimą, teisės į gynybą ir nekaltumo prezumpciją (47 ir 48 straipsniai) apsaugą, taip pat bendrąjį gero administravimo principą. Be to, atsižvelgiant į tai, kad pasiūlymas taikomos tam tikrose srityse, jis darys teigiamą poveikį įvairių socialinių grupių teisėms, pavyzdžiui, darbuotojų teisėms į sąžiningas ir teisingas darbo sąlygas (31 straipsnis), aukšto lygio vartotojų apsaugai (28 straipsnis), vaiko teisėms (24 straipsnis) ir neįgaliųjų integracijai (26 straipsnis). Teisė į aukšto lygio aplinkos apsaugą ir aplinkos kokybės gerinimą (37 straipsnis) taip pat yra svarbi, įskaitant šios teisės ryšį su žmonių sauga ir sveikata. *Ex ante* patikrinimo, rizikos valdymo ir žmogaus atliekamos priežiūros pareigos taip pat sudarys palankesnes sąlygas paisyti kitų pagrindinių teisių, nes padės kuo labiau sumažinti klaidingų arba šališkų sprendimų, priimamų naudojant DI, riziką tokiose svarbiose srityse kaip švietimas ir mokymas, užimtumas, svarbios paslaugos, teisėsauga ir teismai. Jei pagrindinės teisės vis dėlto bus pažeidžiamos, veiksminga nukentėjusių asmenų gynyba bus įmanoma užtikrinant DI sistemų skaidrumą ir atsekamumą, kartu numatant griežtą *ex post* kontrolę.

Šiuo pasiūlymu nustatomi tam tikri laisvės užsiimti verslu (16 straipsnis) ir menų ir mokslo laisvės (13 straipsnis) apribojimai, siekiant užtikrinti atitiktį viršesniems su viešuoju interesu

susijusiems tikslams, pavyzdžiui, sveikatai, saugai, vartotojų apsaugai ir kitoms pagrindinėms teisėms („atsakingos inovacijos“) tais atvejais, kai kuriama arba naudojama didelės rizikos DI technologija. Šie apribojimai yra proporcingi ir apima tik tai, kas yra griežtai būtina siekiant užkirsti kelią ir sumažinti didelę riziką saugai ir tikėtiniems pagrindinių teisių pažeidimams.

Griežtesni įpareigojimai skaidrumo srityje taip pat neturės neproporcingo poveikio teisei į intelektinės nuosavybės apsaugą (17 straipsnio 2 dalis), nes jie bus susiję tik su būtiniausia informacija asmenims, kad jie galėtų pasinaudoti savo teise į veiksmingą teisių gynimą, būtinu priežiūros ir vykdymo užtikrinimo institucijų skaidrumu, atsižvelgiant į jų įgaliojimus. Bet kokia informacija bus atskleidžiama laikantis atitinkamų šioje srityje galiojančių teisės aktų, įskaitant Direktyvą 2016/943 dėl neatskleistos praktinės patirties ir verslo informacijos (komercinių paslapčių) apsaugos nuo neteisėto jų gavimo, naudojimo ir atskleidimo. Kai valdžios institucijoms ir notifikuotosioms įstaigoms reikia suteikti prieigą prie konfidencialios informacijos arba pirminio kodo, kad būtų galima išnagrinėti atitiktį esminėms pareigoms, joms taikomos privalomos konfidencialumo pareigos.

4. POVEIKIS BIUDŽETUI

Valstybės narės turės paskirti priežiūros institucijas, atsakingas už teisės aktų reikalavimų įgyvendinimą. Jų priežiūros funkcija galėtų būti grindžiama dabartinėmis taisyklėmis, pavyzdžiui, susijusiomis su atitikties vertinimo įstaigomis arba rinkos priežiūra, tačiau reikėtų pakankamų technologinių ekspertinių žinių ir žmogiškųjų bei finansinių išteklių. Priklausomai nuo kiekvienoje valstybėje narėje jau esamos struktūros, tai galėtų reikšti 1–25 etato ekvivalentus kiekvienoje valstybėje narėje.

Išsami susijusių išlaidų apžvalga pateikta su šiuo pasiūlymu susijusioje finansinėje pažymoje.

5. KITI ELEMENTAI

5.1. Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka

Patikimo stebėsenos ir įvertinimo mechanizmo numatymas turi esminę reikšmę užtikrinant, kad pasiūlymas būtų veiksmingas siekiant jame nustatytų konkrečių veiksmų. Komisija bus atsakinga už pasiūlymo poveikio stebėseną. Ji nustatys atskirų didelės rizikos DI prietaikų registravimo viešoje ES masto duomenų bazėje sistemą. Ši registracija taip pat sudarys sąlygas kompetentingoms institucijoms, naudotojams ir kitiems suinteresuotiems asmenims patikrinti, ar didelės rizikos DI sistema atitinka pasiūlyme nustatytus reikalavimus, ir vykdyti sustiprintą šių DI sistemų, keliančių didelę riziką pagrindinėms teisėms, priežiūrą. Kad suteiktų duomenų į šią duomenų bazę, DI tiekėjai bus įpareigoti teikti reikšmingą informaciją apie savo sistemas ir atlikti šių sistemų atitikties vertinimą.

Be to, DI tiekėjai bus įpareigoti informuoti nacionalines kompetentingas institucijas apie didelius incidentus arba veikimo sutrikimus, dėl kurių pažeidžiami pagrindinių teisių įsipareigojimai, iš karto, kai apie juos sužinoma, taip pat informuoti apie bet kokius DI sistemų atšaukimus ir pašalinimus iš rinkos. Tuomet nacionalinės kompetentingos institucijos atliks tyrimus dėl incidentų ir (arba) veikimo sutrikimų, surinks visą būtiną informaciją ir nuolat ją perduos Komisijai, įskaitant atitinkamus metaduomenis. Komisija šią informaciją apie incidentus papildys išsamia visos DI rinkos analize.

Komisija paskelbs ataskaitą, kurioje, praėjus penkeriems metams nuo siūlomos DI sistemos taikymo pradžios, ją įvertins ir peržiūrės.

5.2. Išsamus konkrečių pasiūlymo nuostatų paaiškinimas

5.2.1. TAIKYMO SRITIS IR APIBRĖŽTYS (I ANTRAŠTINĖ DALIS)

I antraštinėje dalyje apibrėžiamas naujų taisyklių, taikomų DI sistemų pateikimui rinkai, pradėjimui naudoti ir naudojimui, reglamentavimo dalykas ir taikymo sritis. Joje taip pat pateikiamos visame dokumente vartojamos apibrėžtys. Siekiama, kad DI sistemos apibrėžtis teisinėje sistemoje būtų technologiniu požiūriu kuo neutralesnė ir kuo labiau orientuota į ateitį, atsižvelgiant į sparčius su DI susijusius technologinius ir rinkos pokyčius. Siekiant suteikti reikalingą teisinį tikrumą, I antraštinę dalį papildo I priedas, kuriame pateiktas išsamus DI kūrimo principų ir metodų sąrašas, kurį Komisija turės pritaikyti atsižvelgdama į naujas kuriamas technologijas. Taip pat aiškiai apibrėžiami pagrindiniai DI vertės grandinės dalyviai, pavyzdžiui, DI sistemų tiekėjai ir naudotojai, t. y. viešojo ir privačiojo sektoriaus veiklos vykdytojai, taip užtikrinant vienodas veiklos sąlygas.

5.2.2. DRAUDŽIAMA SU DIRBTINIU INTELEKTU SUSIJUSI PRAKTIKA (II ANTRAŠTINĖ DALIS)

II antraštinėje dalyje nustatytas draudžiamo DI sąrašas. Reglamentavimo srityje laikomasi rizika pagrįsto metodo, darant skirtumą tarp DI, kuris kelia i) nepriimtiną riziką, ii) didelę riziką ir iii) mažą arba minimalią riziką, naudojimo. II antraštinėje dalyje pateiktas draudžiamos praktikos sąrašas apima visas DI sistemas, kurių naudojimas laikomas nepriimtinu dėl prieštaravimo Sąjungos vertybėms, pavyzdžiui, DI sistemomis pažeidžiamos pagrindinės teisės. Draudimai taikomi praktikai, kuri gali turėti reikšmingą potencialą manipuliuoti asmenimis naudojant pasąmonę veikiančius metodus, kurių jie nesuvokia, arba išnaudojant konkrečių pažeidžiamų grupių, pavyzdžiui, vaikų arba neįgaliųjų, pažeidžiamumo aspektus, siekiant iš esmės pakeisti jų elgesį taip, kad jie patys ar kitas asmuo patirtų psichologinę arba fizinę žalą. Kita manipuliavimo arba išnaudojimo praktika, daranti poveikį suaugusiesiems, kurią gali palengvinti DI sistemos, gali būti reglamentuojama pagal galiojančius duomenų apsaugos, vartotojų apsaugos ir skaitmeninių paslaugų teisės aktus, kuriais garantuojamas tinkamas fizinių asmenų informavimas ir suteikiama galimybė nuspręsti, kad jiems nebūtų taikomas profiliavimas arba kita poveikį jų elgesiui galinti daryti praktika. Pasiūlymu taip pat draudžiama valdžios institucijoms bendraisiais tikslais vykdyti DI pagrįstą socialinio reitingavimo. Galiausiai taip pat draudžiamas tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešosiose erdvėse teisėsaugos tikslais, išskyrus atvejus, kai taikomos tam tikros ribotos išimtys.

5.2.3. DIDELĖS RIZIKOS DI SISTEMOS (III ANTRAŠTINĖ DALIS)

III antraštinėje dalyje pateiktos konkrečios taisyklės dėl DI sistemų, kurios kelia didelę riziką fizinių asmenų sveikatai ir saugai arba pagrindinėms teisėms. Laikantis rizika pagrįsto metodo, šiomis didelės rizikos DI sistemomis Europos rinkoje leidžiama prekiauti užtikrinant atitiktį tam tikriems privalomiems reikalavimams ir atlikus *ex ante* atitikties vertinimą. DI sistema priskiriama didelės rizikos sistemoms remiantis numatytąja DI sistemos paskirtimi, laikantis galiojančių gaminių saugos teisės aktų. Todėl sistemos priskyrimas didelės rizikos DI sistemai priklauso ne tik nuo DI sistemos atliekamos funkcijos, bet ir konkrečios tos sistemos paskirties ir jos naudojimo būdų.

III antraštinės dalies 1 skyriuje nustatytos klasifikavimo taisyklės ir įvardijamos dvi pagrindinės didelės rizikos DI sistemų kategorijos:

- DI sistemos, naudojamos kaip gaminio saugos komponentas ir kurių *ex ante* atitikties vertinimą atlieka trečioji šalis;

- kitos atskiros DI sistemos, iš esmės darančios poveikį pagrindinėms teisėms, kurios aiškiai išvardijamos III priede.

Šiame didelės rizikos DI sistemų sąraše, pateiktame III priede, yra kelios DI sistemos, kurių rizika jau pasireiškė arba tikėtina, kad ji pasireikš artimiausioje ateityje. Siekdama užtikrinti, kad reglamentavimą būtų galima pritaikyti prie naujų DI naudojimo būdų ir prietaikų, Komisija gali praplėsti didelės rizikos DI sistemų, naudojamų tam tikrose iš anksto apibrėžtose srityse, sąrašą taikydama kriterijų rinkinį ir rizikos vertinimo metodiką.

2 skyriuje išdėstyti didelės rizikos DI sistemoms taikomi teisiniai reikalavimai, susiję su duomenimis ir duomenų valdymu, dokumentacija ir įrašų saugojimu, skaidrumu ir informacijos teikimu naudotojams, žmogaus atliekama priežiūra, patikimumu, tikslumu ir saugumu. Siūlomi minimalūs reikalavimai jau atitinka rūpestingų veiklos vykdytojų naudojamas pažangiausias technologijas ir yra dvejų metų parengiamojo darbo rezultatas, kurį pasiekė Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais[29] ir išbandė daugiau nei 350 organizacijų[30]. Šie reikalavimai taip pat iš esmės dera su kitomis tarptautinėmis rekomendacijomis ir principais, kuriais užtikrinama, kad siūloma DI sistema derėtų su ES tarptautinės prekybos partnerių priimtomis rekomendacijomis ir principais. Tikslūs techniniai sprendimai, padedantys užtikrinti atitiktį šiems reikalavimams, gali būti numatomi nustatant standartus ar kitas technines specifikacijas arba kitaip parengiami, remiantis bendrosiomis inžinerijos arba mokslinėmis žiniomis, kurias savo nuožiūra panaudoja DI sistemos tiekėjas. Lankstumas yra ypač svarbus, nes sudaro sąlygas DI sistemų tiekėjams nuspręsti, kaip laikytis jiems keliamų reikalavimų, kartu atsižvelgiant į pažangiausias technologijas ir technologijų ir mokslo pažangą šioje srityje.

3 skyriuje nustatomos aiškios horizontaliosios pareigos didelės rizikos DI sistemų tiekėjams. Naudotojams ir kitiems DI vertės grandinės dalyviams (pvz., importuotojams, platintojams, įgaliotiesiems atstovams) taip pat nustatytos proporcingos pareigos.

4 skyriuje nustatoma sistema, taikoma notifikuotosioms įstaigoms, kurios dalyvauja kaip nepriklausomos trečiosios šalys atitikties vertinimo procedūrose, o 5 skyriuje išsamiai paaiškinamos atitikties vertinimo procedūros, kuriomis reikia vadovautis dėl kiekvienos rūšies didelės rizikos DI sistemos. Atitikties vertinimu grindžiamo metodo paskirtis – kuo labiau sumažinti naštą ekonominės veiklos vykdytojams, taip pat notifikuotosioms įstaigoms, kurių pajėgumai ilgainiui turi būti didinami. DI sistemoms, kurias numatoma naudoti kaip gaminių saugos komponentus ir kurioms taikomi naujosios teisės aktų sistemos teisės aktai (pvz., mašinos, žaislai, medicinos prietaisai ir pan.), bus taikomi tie patys gaminių, kurių komponentais yra šios sistemos, *ex ante* ir *ex post* atitikties ir vykdymo užtikrinimo mechanizmai. Pagrindinis skirtumas yra tas, kad *ex ante* ir *ex post* mechanizmai padės užtikrinti atitiktį ne tik sektoriaus teisės aktuose, bet ir šiame reglamente nustatytiems reikalavimams.

Dėl atskirų didelės rizikos DI sistemų, kurios nurodytos III priede, bus sukurta nauja atitikties ir vykdymo užtikrinimo sistema. Šiuo atveju vadovaujamasi naujosios teisės aktų sistemos teisės aktais, kurie įgyvendinami tiekėjams atliekant vidaus kontrolės patikras, išskyrus nuotolinio biometrinio tapatybės nustatymo sistemas, kurioms turėtų būti taikomas trečiosios šalies atitikties vertinimas. Išsamus *ex ante* atitikties vertinimas atliekant vidaus patikras kartu su griežtu *ex post* vykdymo užtikrinimu galėtų būti veiksmingas ir pagrįstas šioms sistemoms taikomas sprendimas, atsižvelgiant į ankstyvąjį reglamentavimo intervencijos etapą ir tai, kad DI sektorius yra labai novatoriškas, o su auditu susijusios specialiosios žinios tik dabar

[29] Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais, *Patikimo DI etinės gairės*, 2019 m.

[30] Joms taip pat pritarė Komisija savo 2019 m. komunikate dėl į žmogų orientuoto DI.

pradedamos kaupti. Vertinimas atliekant atskirų didelės rizikos DI sistemų vidaus patikras turėtų būti neatskiriamas nuo išsamios, veiksmingos ir tinkamai dokumentuotos *ex ante* atitikties, įskaitant visus reglamentavimo ir atitikties reikalavimus kartu su patikimomis kokybės ir rizikos valdymo sistemomis ir priežiūra po pateikimo rinkai. Tiekėjui atlikus atitinkamą atitikties vertinimą, jis turėtų užregistruoti šias atskiras didelės rizikos DI sistemas ES duomenų bazėje, kurią tvarkys Komisija, kad padidintų visuomeninį skaidrumą ir priežiūrą ir sustiprintų kompetentingų institucijų vykdomą *ex post* priežiūrą. Siekiant užtikrinti nuoseklumą su dabartiniais gaminių saugą reglamentuojančiais teisės aktais, DI sistemų, kurios yra gaminių saugos komponentai, atitikties vertinimai bus atliekami naudojant sistemą, kurioje trečioji šalis taiko atitikties vertinimo procedūras, kurios jau nustatytos pagal atitinkamo sektoriaus gaminių saugą reglamentuojančius teisės aktus. Nauji *ex ante* pakartotiniai atitikties vertinimai bus reikalingi atlikus esminius DI sistemų pakeitimus (visų pirma pakeitimus, kurie nėra susiję su tiekėjo parengtuose techniniuose dokumentuose iš anksto nustatytais reikalavimais ir yra patikrinami *ex ante* atitikties vertinimo metu).

5.2.4. TAM TIKROMS DI SISTEMOMS TAIKOMI SKAIDRUMO ĮPAREIGOJIMAI (IV ANTRAŠTINĖ DALIS)

IV antraštinė dalis yra susijusi su tam tikromis DI sistemomis, siekiant atsižvelgti į konkrečią jų keliamą manipuliavimo riziką. Pareigos skaidrumo srityje bus taikomos sistemoms, kurios i) sąveikauja su žmonėmis, ii) naudojamos emocijoms arba asociacijoms su (socialinėmis) kategorijomis nustatyti remiantis biometriniais duomenimis arba iii) kuria turinį arba juo manipuliuoja (sintetinė sankaita). Tais atvejais, kai asmenys sąveikauja su DI sistema arba jų emocijos ar savybės atpažįstamos automatinėmis priemonėmis, žmonės apie šias aplinkybes turi būti informuojami. Jeigu DI sistema naudojama kurti judamo bei nejudamo vaizdo ir garso turinį, kuris yra labai panašus į autentišką turinį, turėtų būti nustatyta pareiga atskleisti, kad turinys kuriamas automatinėmis priemonėmis, išskyrus su teisėtais tikslais susijusias išimtis (teisėsaugos tikslai, saviraiškos laisvė). Taip asmenims sudaromos sąlygos priimti informacija pagrįstus sprendimus arba pasitraukti iš atitinkamos padėties.

5.2.5. PRIEMONĖS INOVACIJOMS REMTI (V ANTRAŠTINĖ DALIS)

V antraštine dalimi prisidedama prie tikslo sukurti inovacijoms palankią, į ateitį orientuotą ir sutrikimams atsparią teisinę sistemą. Šiuo tikslu joje nacionalinės kompetentingos institucijos skatinamos sukurti apribotą bandomąją reglamentavimo aplinką ir nustatoma bazinė valdymo, priežiūros ir atsakomybės sistema. DI apribotoje bandomojoje reglamentavimo aplinkoje sukuriama kontroliuojama aplinka, kurioje ribotą laikotarpį, remiantis bandymų planu, dėl kurio susitarta su kompetentingomis institucijomis, išbandomos naujoviškos technologijos. V antraštinėje dalyje taip pat nustatytos priemonės, kuriomis sumažinama reglamentavimo našta MVĮ ir startuoliams.

5.2.6. VALDYMAS IR ĮGYVENDINIMAS (VI, VII IR VIII ANTRAŠTINĖS DALYS)

VI antraštinėje dalyje nustatytos Sąjungos ir nacionalinio lygmens valdymo sistemos. Sąjungos lygmeniu pasiūlymu sukuriama Europos dirbtinio intelekto valdyba (toliau – Valdyba), kurią sudaro valstybių narių ir Komisijos atstovai. Valdyba palengvins sklandų, veiksmingą ir suderintą šio reglamento įgyvendinimą prisidėdama prie veiksmingo nacionalinių priežiūros institucijų ir Komisijos bendradarbiavimo ir patardama Komisijai bei teikdama jai ekspertinių žinių. Ji taip pat kaups geriausią patirtį ir dalysis ja su valstybėmis narėmis.

Nacionaliniu lygmeniu valstybės narės turės paskirti vieną arba daugiau nacionalinių kompetentingų institucijų, įskaitant nacionalinę priežiūros instituciją, siekiant vykdyti

reglamento taikymo ir įgyvendinimo priežiūrą. Europos duomenų apsaugos priežiūros pareigūnas veiks kaip kompetentinga Sąjungos institucijų, agentūrų ir įstaigų priežiūros institucija tais atvejais, kai joms taikomas šis reglamentas.

VII antraštinės dalies tikslas – palengvinti Komisijos ir nacionalinių institucijų stebėsenos darbą sukuriant ES masto duomenų bazę, skirtą atskiroms didelės rizikos DI sistemoms, kurių poveikis iš esmės yra susijęs su pasekmėmis pagrindinėms teisėms. Duomenų bazę tvarkys Komisija, o duomenis jai teiks DI sistemų tiekėjai, kurie turės užregistruoti savo sistemas prieš pateikdami jas rinkai arba kitaip užtikrindami jų naudojimo pradžią.

VIII antraštinėje dalyje nustatytos DI sistemų tiekėjams taikomos stebėsenos ir pranešimų teikimo pareigos, susijusios su priežiūra po pateikimo rinkai ir pranešimų teikimu bei su DI susijusių incidentų ir veikimo sutrikimų tyrimu. Rinkos priežiūros institucijos taip pat turėtų kontroliuoti rinką ir tirti visoms didelės rizikos DI sistemoms, kurios jau pateiktos rinkai, taikomas pareigas ir reikalavimus. Rinkos priežiūros institucijos turėtų turėti visus įgaliojimus pagal Reglamentą (ES) 2019/1020 dėl rinkos priežiūros. *Ex post* vykdymo užtikrinimo metu turėtų būti užtikrinama, kad rinkai pateikus DI sistemą, valdžios institucijos turėtų įgaliojimus ir išteklius imtis intervencinių veiksmų, jeigu DI sistemos sukelia netikėtą riziką, dėl kurios galima imtis pateisinamų greitų veiksmų. Jos taip pat stebės, kaip veiklos vykdytojai laikosi savo atitinkamų pagal reglamentą nustatytų pareigų. Pagal pasiūlymą nenumatoma automatiškai sukurti kokių nors papildomų įstaigų ar institucijų valstybių narių lygmeniu. Todėl valstybės narės gali paskirti esamas sektoriaus institucijas (ir naudotis jų patirtimi), kurioms taip pat būtų suteikti įgaliojimai stebėti reglamento nuostatų įgyvendinimą ir užtikrinti jų vykdymą.

Visa tai nedaro poveikio esamai sistemai ir įgaliojimų įgyvendinti *ex post* vykdymo užtikrinimo pareigas, susijusias su pagrindinėmis teisėmis, paskirstymui valstybėse narėse. Kai tai yra būtina atsižvelgiant į jų įgaliojimus, esamos priežiūros ir vykdymo užtikrinimo institucijos taip pat turės įgaliojimus prašyti pateikti bet kurį pagal šį reglamentą laikomą dokumentą bei su juo susipažinti ir prireikus prašyti rinkos priežiūros institucijų pasirūpinti didelės rizikos DI sistemos bandymu panaudojant technines priemones.

5.2.7. ELGESIO KODEKSAI (IX ANTRAŠTINĖ DALIS)

IX antraštinėje dalyje sukuriama elgesio kodeksų rengimo sistema, siekiant paskatinti didelės rizikos nekeliančių DI sistemų tiekėjus savanoriškai taikyti didelės rizikos DI sistemoms galiojančius privalomus reikalavimus (kaip nustatyta III antraštinėje dalyje). Didelės rizikos nekeliančių DI sistemų tiekėjai gali patys parengti ir įgyvendinti elgesio kodeksus. Šiuose kodeksuose taip pat gali būti nustatyti savanoriški įsipareigojimai, susiję, pavyzdžiui, su aplinkos tvarumu, neįgaliųjų asmenų prieiga, suinteresuotųjų subjektų dalyvavimu projektuojant ir kuriant DI sistemas, taip pat kūrimo komandų įvairove.

5.2.8. BAIGIAMOSIOS NUOSTATOS (X, XI IR XII ANTRAŠTINĖS DALYS)

X antraštinėje dalyje pabrėžiama visų šalių pareiga gerbti informacijos ir duomenų konfidencialumą ir nustatomos keitimosi informacija, gauta įgyvendinant reglamentą, taisyklės. X antraštinėje dalyje taip pat nustatytos priemonės, kuriomis užtikrinamas veiksmingas reglamento įgyvendinimas taikant veiksmingas, proporcingas ir atgrasomąsias nuobaudas už nuostatų pažeidimus.

XI antraštinėje dalyje nustatytos įgaliojimų delegavimo ir naudojimosi įgyvendinimo įgaliojimais taisyklės. Pasiūlymu Komisija įgaliojama, kai tinkama, priimti įgyvendinimo aktus, kad užtikrintų vienodą reglamento arba deleguotųjų aktų taikymą ir atnaujintų arba papildytų I–VII priedų sąrašus.

XII antraštinėje dalyje nustatyta Komisijos pareiga nuolat įvertinti poreikį atnaujinti III priedą ir parengti reguliarias reglamento vertinimo ir peržiūros ataskaitas. Joje taip pat nustatytos baigiamosios nuostatos, įskaitant skirtingą pradinės reglamento taikymo dienos pereinamąjį laikotarpį, kad visoms suinteresuotosioms šalims jį būtų lengviau įgyvendinti.

2021/0106 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

KURIUO NUSTATOMOS SUDERINTOS DIRBTINIO INTELEKTO TAISYKLĖS (DIRBTINIO INTELEKTO AKTAS) IR IŠ DALIES KEIČIAMI TAM TIKRI SĄJUNGOS TEISĖKŪROS PROCEDŪRA PRIIMTI AKTAI

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 16 ir 114 straipsnius,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[31],

atsižvelgdami į Regionų komiteto nuomonę[32],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) šio reglamento paskirtis – pagerinti vidaus rinkos veikimą nustatant vienodą teisinę sistemą, visų pirma skirtą dirbtinio intelekto kūrimui, pateikimui rinkai ir naudojimui paisant Sąjungos vertybių. Šiuo reglamentu siekiama įvairių svarbių su viešuoju interesu susijusių tikslų, pavyzdžiui, aukšto lygio sveikatos, saugumo ir pagrindinių teisių apsaugos, ir juo užtikrinamas laisvas DI pagrįstų prekių ir paslaugų tarpvalstybinis judėjimas, taip užkertant kelią valstybėms narėms nustatyti apribojimus kuriant, pateikiant rinkai ir naudojant DI sistemas, išskyrus atvejus, kai tai aiškiai leidžiama pagal šį reglamentą;

(2) dirbtinio intelekto sistemos (DI sistemos) gali būti lengvai įdiegtos įvairiuose ekonomikos ir visuomenės sektoriuose, taip pat tarpvalstybiniu mastu, ir jos gali plisti visoje Sąjungoje. Tam tikros valstybės narės jau išnagrinėjo galimybę priimti nacionalines taisykles, siekiant užtikrinti, kad dirbtinis intelektas būtų saugus ir kuriamas bei naudojamas laikantis pagrindinių teisių ir pareigų. Dėl skirtingų nacionalinių taisyklių vidaus rinkoje gali atsirasti susiskaidymas ir sumažėti DI sistemas kuriančių ar naudojančių veiklos vykdytojų teisinis tikrumas. Todėl visoje Sąjungoje reikėtų užtikrinti nuoseklią ir aukšto lygio apsaugą ir reikėtų užkirsti kelią skirtumams, trukdantiems DI sistemoms ir susijusiems gaminiams ir paslaugoms laisvai cirkuliuoti vidaus rinkoje, nustatant vienodas pareigas veiklos vykdytojams ir garantuojant vienodą svarbių viešojo intereso priežasčių ir asmenų teisių apsaugą visoje vidaus rinkoje, remiantis Sutarties dėl Europos Sąjungos (toliau – SESV) veikimo 114 straipsniu. Tiek, kiek šiame reglamente yra konkrečių taisyklių dėl asmenų apsaugos asmens duomenų tvarkymo srityje, susijusių su DI sistemų naudojimo apribojimais, susijusiais su tikruoju laiku viešosiose erdvėse teisėsaugos

[31] OL C […], […], p. […].
[32] OL C […], […], p. […].

tikslais naudojamomis nuotolinio biometrinio tapatybės nustatymo sistemomis, šį reglamentą konkrečių taisyklių atveju būtų tinkama grįsti SESV 16 straipsniu. Atsižvelgiant į tas konkrečias taisykles ir rėmimusi SESV 16 straipsniu, yra tinkama konsultuotis su Europos duomenų apsaugos valdyba;

(3) dirbtinis intelektas – tai greitai vystoma technologijų grupė. Šios technologijos gali duoti visokeriopą ekonominę ir visuomeninę naudą įvairiose pramonės šakose ir socialinės veiklos srityse. Dirbtinio intelekto naudojimas dėl geresnės predikcijos, operacijų optimizavimo ir išteklių paskirstymo, taip pat asmenims ir organizacijoms prieinamo skaitmeninių sprendimų personalizavimo, įmonėms gali suteikti esminius konkurencinius pranašumus ir prisidėti prie socialiniu požiūriu ir aplinkai naudingų pasekmių, pavyzdžiui, sveikatos priežiūros, ūkininkavimo, švietimo ir mokymo, infrastruktūros valdymo, energijos, transporto ir logistikos, viešųjų paslaugų, teisingumo, išteklių ir energijos vartojimo efektyvumo, klimato kaitos ir prisitaikymo prie klimato kaitos srityse;

(4) kartu, priklausomai nuo aplinkybių, susijusių su jo konkrečiu taikymu ir naudojimu, dirbtinis intelektas gali kelti riziką ir padaryti žalos viešiesiems interesams ir teisėms, kurių apsauga užtikrinama Sąjungos teisėje. Tokia žala gali būti reikšminga arba nereikšminga;

(5) todėl Sąjungos teisinė sistema, kuria nustatomos suderintos dirbtinio intelekto taisyklės, yra reikalinga siekiant vidaus rinkoje skatinti kurti, naudoti ir įsisavinti dirbtinį intelektą, kartu užtikrinant aukšto lygio viešųjų interesų, kaip antai saugos ir sveikatos apsaugą, ir pagrindinių teisių apsaugą, kaip pripažįstama ir saugoma Sąjungos teisėje. Kad šis tikslas būtų pasiektas, reikėtų nustatyti taisykles, kuriomis reglamentuojamas tam tikrų DI sistemų pateikimas rinkai ir pradėjimas naudojimo, taip užtikrinant sklandų vidaus rinkos veikimą ir leidžiant išnaudoti tų sistemų privalumus, atsižvelgiant į prekių ir paslaugų laisvo judėjimo principą. Šios taisyklės šiame reglamente nustatomos siekiant remti Sąjungos tikslą pirmauti pasaulyje kuriant saugų, patikimą ir etišką dirbtinį intelektą, kaip nurodė Europos Vadovų Taryba[33], ir juo užtikrinama etikos principų apsauga, atsižvelgiant į konkretų Europos Parlamento prašymą[34];

(6) DI sistemos sąvoka turėtų būti aiškiai apibrėžta, siekiant užtikrinti teisinį tikrumą, kartu suteikiant lankstumo prisitaikyti prie būsimų technologinių pokyčių. Apibrėžtis turėtų būti grindžiama pagrindinėmis funkcinėmis programinės įrangos charakteristikomis, visų pirma gebėjimu, atsižvelgiant į žmogaus apibrėžtų tikslų rinkinį, kurti tokius išvedinius, kaip antai turinį, predikcijas, rekomendacijas arba sprendimus, kurie turi įtakos aplinkai, su kuria sąveikauja sistema, nepaisant to, ar tai yra fizinė, ar skaitmeninė aplinka. DI sistemos gali būti projektuojamos taip, kad veiktų įvairiais autonomijos lygmenimis ir veiktų atskirai arba kaip gaminio komponentas, nepaisant to, ar sistema yra fiziškai integruota (įmontuota) į gaminį arba atlieka gaminio funkciją, tačiau nėra į jį integruota (neįmontuota). DI sistemos apibrėžtį turėtų papildyti konkrečių metodų ir principų, naudojamų ją kuriant, sąrašas, ir jis, Komisijai priimant deleguotuosius aktus, kuriais iš dalies keičiamas tas sąrašas, turėtų būti nuolat atnaujinamas atsižvelgiant į rinkos ir technologinius pokyčius;

---

33 Europos Vadovų Taryba, Specialusis Europos Vadovų Tarybos susitikimas (2020 m. spalio 1 ir 2 d.). Išvados, EUCO 13/20, 2020 m., p. 6.

34 2020 m. spalio 20 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos, 2020/2012(INL).

(7) šiame reglamente vartojama biometrinių domenų sąvoka atitinka ir turi būti nuosekliai aiškinama, atsižvelgiant į biometrinių duomenų sąvoką, apibrėžtą Europos Parlamento ir Tarybos reglamento (ES) 2016/679[35] 4 straipsnio 14 dalyje, Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[36] 3 straipsnio 18 dalyje ir Europos Parlamento ir Tarybos direktyvos (ES) 2016/680[37] 3 straipsnio 13 dalyje;

(8) šiame reglamente vartojama nuotolinio biometrinio tapatybės nustatymo sistemos sąvoka turėtų būti apibrėžta funkciniu požiūriu, kaip DI sistema, skirta fizinių asmenų tapatybei nuotoliniu būdu nustatyti, šiuo tikslu palyginant asmens biometrinius duomenis su informacinėje duomenų bazėje esančiais biometriniais duomenimis iš anksto neturint žinių, ar asmuo, kuriam taikoma tikslinė priemonė bus ir ar galima nustatyti jo tapatybę, nepriklausomai nuo naudojamos konkrečios technologijas, procesų arba biometrinių duomenų rūšies. Atsižvelgiant į skirtingus ypatumus ir naudojimo būdus, taip pat į įvairią susijusią riziką, reikėtų daryti skirtumą tarp tikralaikio ir netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų. Jeigu naudojamos tikralaikės sistemos, biometrinių duomenų rinkimas, lyginimas ir tapatybės nustatymas visuomet vyksta momentiškai, beveik momentiškai arba bet kuriuo atveju be didesnės delsos. Šiuo atžvilgiu neturėtų būti jokių galimybių apeiti šio reglamento taisyklių dėl tikralaikio atitinkamų DI sistemų naudojimo numatant nedidelę delsą. Tikralaikės sistemos yra susijusios su medžiagos naudojimu tiesiogiai arba beveik tiesiogiai, pavyzdžiui, filmuota medžiaga, sukurta naudojant kamerą arba kitą panašią funkciją atliekantį prietaisą. Kita vertus netikralaikių sistemų atveju biometriniai duomenys jau buvo surinkti ir palyginimas bei tapatybės nustatymas atliekami po ilgos delsos. Ji apima medžiagą, pavyzdžiui, nuotraukas arba vaizdo medžiagą, sukurtą naudojant apsaugines vaizdo stebėjimo sistemas arba asmeninius prietaisus prieš pradedant naudoti sistemą atitinkamų fizinių asmenų atžvilgiu;

(9) šiame reglamente sąvoka „viešoji erdvė“ turėtų būti suprantama kaip reiškianti bet kokią visuomenei prieinamą fizinę vietą, nepriklausomai, ar atitinkama vieta valdoma viešai, ar privačiai. Todėl sąvoka netaikoma vietoms, kurios yra privataus pobūdžio ir paprastai nėra viešai prieinamos trečiosioms šalims, įskaitant teisėsaugos institucijas, išskyrus atvejus, kai tos šalys gavo kvietimą arba joms suteikti įgaliojimai, pavyzdžiui, namai, privatūs klubai, biurai, sandėliai ir gamyklos. Ši nuostata netaikoma internetinei erdvei, nes tai nėra fizinė erdvė. Tačiau vien faktas, kad gali būti taikomos tam tikros patekimo į konkrečią vietą sąlygos, pavyzdžiui, leidimai įeiti arba amžiaus apribojimai, nereiškia, kad erdvė nėra viešai prieinama, kaip apibrėžta šiame reglamente. Todėl be viešųjų erdvių, pavyzdžiui, gatvių, atitinkamų valdžios įstaigų pastatų dalių ir daugumos transporto infrastruktūros objektų, tokios vietos kaip kino teatrai, teatrai, parduotuvės ir prekybos centrai, paprastai taip pat yra viešai prieinami.

---

35 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

36 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

37 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (Teisėsaugos direktyva) (OL L 119, 2016 5 4, p. 89).

Tačiau tai, ar atitinkama vieta yra viešai prieinama, turėtų būti nustatyta kiekvienu konkrečiu atveju atsižvelgiant į konkrečios nagrinėjamos situacijos ypatumus;

(10) siekiant užtikrinti vienodas sąlygas ir veiksmingą asmenų teisių ir laisvių apsaugą visoje Sąjungoje, šiame reglamente nustatytos taisyklės turėtų būti taikomos DI sistemų tiekėjams nediskriminuojamai, nepaisant to, ar jie įsisteigę Sąjungoje, ar trečiojoje valstybėje, taip pat Sąjungoje įsisteigusiems DI sistemų naudotojams;

(11) tam tikroms DI sistemoms, atsižvelgiant į jų skaitmeninį pobūdį, šis reglamentas turėtų būti taikomas net jei jos nepateikiamos rinkai, nepradeda veikti ir nepradedamos naudoti Sąjungoje. Taip, pavyzdžiui, yra tuo atveju, kai Sąjungoje įsisteigęs veiklos vykdytojas sudaro sutartis dėl tam tikrų paslaugų su už Sąjungos ribų įsisteigusiu veiklos vykdytoju ir šios paslaugos yra susijusios su veikla, kurią turi atlikti DI sistema, kuri laikoma didelę riziką keliančia sistema ir ji sukeltų pasekmių Sąjungoje esantiems fiziniams asmenims. Šiomis aplinkybėmis už Sąjungos ribų esančio veiklos vykdytojo naudojama DI sistema galėtų tvarkyti duomenis, kurie buvo teisėtai surinkti Sąjungoje ir iš jos perduoti, ir pateikti Sąjungoje esančiam pagal sutartį veikiančiam veiklos vykdytojui, tos DI sistemos, kuri nebuvo pateikta rinkai, nepradėjo veikti ar nebuvo pradėta naudoti Sąjungoje, išvedinį, sukurtą tvarkant tuos duomenis. Siekiant užkirsti kelią šio reglamento reikalavimo apėjimui ir užtikrinti veiksmingą Sąjungoje esančių fizinių asmenų apsaugą, šis reglamentas DI sistemų tiekėjams ir naudotojams, kurie yra įsisteigę trečiojoje valstybėje, taip pat turėtų būti taikomas, jei šių sistemų sugeneruotas išvedinys naudojamas Sąjungoje. Vis dėlto, siekiant atsižvelgti į dabartines taisykles ir specialius bendradarbiavimo su užsienio partneriais, su kuriais keičiamasi informacija ir įrodymais, poreikius, šis reglamentas neturėtų būti taikomas trečiosios valstybės valdžios institucijoms ir tarptautinėms organizacijoms, kai veikiama pagal nacionaliniu arba Europos lygmeniu sudarytus tarptautinius susitarimus teisėsaugos ir teisminio bendradarbiavimo su Sąjunga arba jos valstybėmis narėmis tikslais. Tokius dvišalius susitarimus sudarė valstybės narės ir trečiosios valstybės arba Europos Sąjunga, Europolas ir kitos ES agentūros ir trečiosios šalys bei tarptautinės organizacijos;

(12) šis reglamentas taip pat turėtų būti taikomas Sąjungos institucijoms, tarnyboms, įstaigoms ir agentūroms, kai jos veikia kaip DI sistemos tiekėjai arba naudotojai. DI sistemoms, kurios sukuriamos arba naudojamos tik kariniais tikslais, šis reglamentas neturėtų būti taikomas, jeigu tas naudojimas patenka į išimtinę bendros užsienio ir saugumo politikos taikymo sritį pagal Europos Sąjungos sutarties (ES sutartis) V antraštinę dalį. Šis reglamentas neturėtų daryti poveikio nuostatoms dėl tarpininkavimo tiekėjų atsakomybės, nustatytos Europos Parlamento ir Tarybos direktyvoje 2000/31/EB [iš dalies pakeistoje Skaitmeninių paslaugų aktu];

(13) siekiant užtikrinti nuoseklią ir aukšto lygio viešųjų interesų, susijusių su sveikata, saugumu ir pagrindinėmis teisėmis, apsaugą, reikėtų nustatyti bendrus norminius standartus, taikomus visoms didelės rizikos DI sistemoms. Šie standartai turėtų derėti su Europos Sąjungos pagrindinių teisių chartija (toliau – Chartija), būti nediskriminuojantys ir atitikti Sąjungos tarptautinius prekybos srities įsipareigojimus;

(14) siekiant nustatyti proporcingų ir veiksmingų DI sistemoms taikomų taisyklių rinkinį, reikėtų vadovautis aiškiai apibrėžtu rizika pagrįstu metodu. Laikantis to metodo tokių taisyklių rūšį ir turinį reikėtų pritaikyti prie rizikos, kurią gali sukelti DI sistemos, intensyvumo ir masto. Todėl būtina uždrausti tam tikrą su dirbtiniu intelektu susijusią praktiką, nustatyti didelės rizikos DI sistemoms taikomus reikalavimus, o

atitinkamiems veiklos vykdytojams – pareigas, taip pat nustatyti skaidrumo pareigas tam tikroms DI sistemoms;

(15) be daugybės naudingų dirbtinio intelekto panaudojimo būdų, šia technologija taip pat gali būti piktnaudžiaujama ir ji gali suteikti naujoviškų ir galingų manipuliavimo, išnaudojimo ir socialinės kontrolės praktikos įrankių. Tokia praktika yra ypač žalinga ir turėtų būti draudžiama, nes prieštarauja Sąjungos vertybėms, susijusioms su pagarba žmogaus orumui, laisve, lygybe, demokratija ir teisinės valstybės principu ir Sąjungos pagrindinėmis teisėmis, be kita ko, teisėms į nediskriminavimą, duomenų apsaugą bei privatumą ir vaiko teisėms;

(16) tam tikrų DI sistemų, kuriomis siekiama pakeisti žmogaus elgesį, sukeliant tikėtiną fizinę arba psichologinę žalą, pateikimas rinkai, pradėjimas naudoti arba naudojimas turėtų būti draudžiamas. Tokiose DI sistemose naudojami pasąmonę veikiantys komponentai, kurių asmenys negali suprasti arba kuriais išnaudojamas amžiaus arba fizinių arba psichinių sutrikimų nulemtas vaikų ir žmonių pažeidžiamumas. Šios DI sistemos naudojamos siekiant iš esmės pakeisti asmens elgesį, taip sukeliant faktinę arba potencialią žalą tam ar kitam asmeniui. Prielaidos dėl tokio siekio negalima daryti, jeigu žmogaus elgesys pakeičiamas dėl su DI sistema nesusijusių išorės veiksnių, kurių tiekėjas arba naudotojas negali kontroliuoti. Teisėtų tikslų, susijusių su tokiomis DI sistemomis, tyrimams neturėtų būti trukdoma draudimu tuo atveju, jeigu po tokių tyrimų nepradedamas naudoti DI palaikant žmogaus ir mašinų sąveiką, dėl kurios fiziniams asmenims kyla žalos rizika, ir tyrimai atliekami laikantis pripažintų mokslinių tyrimų etinių standartų;

(17) valdžios institucijoms arba jų vardu bendruoju tikslu naudojant DI sistemas, kurių paskirtis vykdyti fizinių asmenų socialinį reitingavimą, gali būti pasiekti diskriminuojantys rezultatai, o tam tikros grupės gali patirti atskirtį. Taip gali būti pažeista teisė į orumą ir nediskriminavimą ir lygybės bei teisingumo vertybės. Tokiomis DI sistemomis vertinamas arba klasifikuojamas fizinių asmenų patikimumas, remiantis jų socialiniu elgesiu įvairiomis aplinkybėmis arba žinomomis arba nuspėjamomis asmeninėmis ar asmenybės savybėmis. Dėl tokių DI sistemų sukurto socialinio reitingavimo balo gali būti žalingai arba nepalankiai elgiamasi su fiziniais asmenimis arba ištisomis jų grupėmis ir tai gali būti daroma socialinėmis aplinkybėmis, kurios nėra susijusios su aplinkybėmis, kuriomis duomenys buvo iš pradžių sukurti arba surinkti, arba žalingai elgiantis, kai toks elgesys yra neproporcingas arba nepagrįstas atsižvelgiant į jų socialinio elgesio rimtumą. Todėl tokios DI sistemos turėtų būti draudžiamos;

(18) tikralaikio nuotolinio biometrinio fizinių asmenų tapatybės nustatymo DI sistemų naudojimas viešosiose erdvėse teisėsaugos tikslais laikomas ypač ribojančiu atitinkamų asmenų teises ir laisves tiek, kiek jos gali daryti poveikį didelės gyventojų dalies privačiam gyvenimui, sukelti nuolatinį sekimo jausmą ir netiesiogiai atgrasyti nuo naudojimosi susirinkimų teise ir kitomis pagrindinėmis teisėmis. Be to, poveikio betarpiškumas ir ribotos galimybės atlikti tolesnes patikras ar taisymus, susijusius su tokiomis tikruoju laiku veikiančiomis sistemomis, kelia didelę riziką asmenų, kurių atžvilgiu vykdoma teisėsaugos veikla, teisėms ir laisvėms;

(19) todėl šių sistemų naudojimas teisėsaugos tikslais turėtų būti draudžiamas, išskyrus tris išsamiai išvardytas ir siaurai apibrėžtas situacijas, kai sistemas naudoti griežtai būtina siekiant apginti esminį viešąjį interesą, kurio svarba nusveria riziką. Šios situacijos apima potencialių nusikaltimo aukų, įskaitant dingusius vaikus, paieška, tam tikromis grėsmėmis fizinių asmenų gyvybei arba fiziniam saugumui, arba teroristinio išpuolio

grėsmėmis ir Tarybos pamatiniame sprendime 2002/584/TVR[38] nurodytų nusikalstamų veikų vykdytojų arba įtariamųjų radimu, buvimo vietos ir tapatybės nustatymu ar baudžiamuoju persekiojimu, jeigu tos nusikalstamos veikos atitinkamoje valstybėje narėje yra baudžiamos skiriant laisvės atėmimo bausmę arba priimant nutartį dėl sulaikymo ne trumpiau nei trejiems metams ir atsižvelgiant į tai, kaip jos apibrėžtos tos valstybės narės teisėje. Tokia laisvės atėmimo bausmės arba nutarties dėl sulaikymo riba, kuri nustatyta nacionalinėje teisėje, padeda užtikrinti, kad nusikalstama veika būtų pakankamai rimta, siekiant pateisinti galimą tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimą. Be to, iš 32 nusikalstamų veikų, išvardytų Tarybos pamatiniame sprendime 2002/584/TVR, kai kurios praktiniu požiūriu gali būti svarbesnės, palyginti su kitomis, atsižvelgiant į tai, kad tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas gali būti būtinas ir proporcingas labai įvairiu mastu siekiant praktiškai išaiškinti įvairių išvardytų nusikalstamų veikų vykdytoją arba įtariamąjį, nustatyti jo buvimo vietą ir tapatybę ar vykdyti baudžiamąjį persekiojimą, kartu atsižvelgiant į tikėtinus žalos arba galimų neigiamų pasekmių rimtumo, tikėtinumo ir masto skirtumus;

(20) siekiant užtikrinti, kad tos sistemos būtų naudojamos atsakingai ir proporcingai, taip pat svarbu nustatyti, kad kiekvienoje iš šių trijų išsamiai nurodytų ir siaurai apibrėžtų situacijų būtų atsižvelgta į tam tikrus aspektus, visų pirma susijusius su situacijos, kurioje pateikiamas prašymas, pobūdžiu ir tokio naudojimo pasekmėmis visų susijusių asmenų teisėms ir laisvėms, taip pat su tokiu naudojimu susijusiomis apsaugos priemonėmis ir sąlygomis. Be to, tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimui viešosiose erdvėse teisėsaugos tikslais turėtų būti taikomos atitinkamos laiko ir erdvės ribos, atsižvelgiant visų pirma į įrodymus arba požymius, susijusius su grėsmėmis, aukomis arba nusikaltėliu. Su kiekviena iš trijų pirmiau nurodytų situacijų susijusiu atveju yra tinkama informacinė asmenų duomenų bazė;

(21) kiekvieną kartą viešosiose erdvėse teisėsaugos tikslais naudojant tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą, reikėtų gauti aiškų ir konkretų valstybės narės teismo institucijos arba bet kurios nepriklausomos administracinės institucijos leidimą. Toks leidimas iš esmės turėtų būti gautas iki naudojimo pradžios, išskyrus tinkamai pagrįstas neatidėliotinas situacijas, t. y. situacijas, kuriose poreikis naudoti atitinkamas sistemas yra toks, kad faktiškai ir objektyviai neįmanoma gauti leidimo prieš pradedant jas naudoti. Tokiose neatidėliotinose situacijose naudojimas turėtų apimti tik tai, kas absoliučiai minimaliai būtina, įskaitant tinkamų apsaugos priemonių ir sąlygų taikymą, kaip apibrėžta nacionalinėje teisėje ir kaip konkrečiai nurodė pati teisėsaugos institucija, atsižvelgdama į kiekvieną pavienį neatidėliotino naudojimo atvejį. Be to, tokiose situacijose teisėsaugos institucija turėtų stengtis kuo greičiau gauti leidimą, kartu nurodant priežastis, dėl kurių ji negalėjo leidimo prašyti anksčiau;

(22) be to, atsižvelgiant į šiame reglamente nustatytą išsamią sistemą, tinkama numatyti, kad toks naudojimas valstybės narės teritorijoje pagal šį reglamentą turėtų būti įmanomas tik tais atvejais ir tiek, kiek atitinkama valstybė narė nusprendė savo išsamiose nacionalinės teisės taisyklėse aiškiai numatyti galimybę leisti tokį naudojimą. Todėl valstybės narės pagal šį reglamentą gali apskritai nenumatyti tokios galimybės arba numatyti ją tik kai kuriems tikslams, kuriais remiantis būtų galima pateisinti pagal šį reglamentą leistiną naudojimo būdą;

[38] 2002 m. birželio 13 d. Tarybos pagrindų sprendimas 2002/584/TVR dėl Europos arešto orderio ir perdavimo tarp valstybių narių tvarkos (OL L 190, 2002 7 18, p. 1).

(23) viešosiose erdvėse teisėsaugos tikslais naudojant tikralaikes nuotolinio biometrinio fizinių asmenų tapatybės nustatymo DI sistemas neišvengiamai tvarkomi biometriniai duomenys. Šio reglamento taisyklės, kuriomis, išskyrus tam tikras išimtis, draudžiamas toks naudojimas, kuris yra pagrįstas SESV 16 straipsniu, turėtų būti taikomos kaip *lex specialis*, atsižvelgiant į biometrinių duomenų tvarkymo taisykles, nustatytas Direktyvos (ES) 2016/680 10 straipsnyje, taip išsamiai reguliuojant tokį naudojimą ir atitinkamų biometrinių duomenų tvarkymą. Todėl toks naudojimas ir tvarkymas turėtų būti įmanomi tik tiek, kiek tai suderinama su šiuo reglamentu nustatyta sistema, už kurios ribų kompetentingos institucijos, savo veiksmais siekdamos teisėsaugos tikslų, negali naudoti tokių sistemų ir tvarkyti su tuo susijusių tokių duomenų, remdamosi Direktyvos (ES) 2016/680 10 straipsnyje išvardytais pagrindais. Šiomis aplinkybėmis šiuo reglamentu nesiekiama nustatyti asmens duomenų tvarkymo pagal Direktyvos 2016/680 8 straipsnį teisinio pagrindo. Tačiau tikralaikių nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešosiose erdvėse kitais nei teisėsaugos tikslais, įskaitant atvejus, kai tai daro kompetentingos institucijos, neturėtų patekti į konkrečios sistemos, susijusios su tokiu naudojimu teisėsaugos tikslu, kuris nustatytas šiame reglamente, taikymo sritį. Todėl tokiam naudojimui kitais nei teisėsaugos tikslais neturėtų būti taikomas leidimo pagal šį reglamentą ir galiojančias nacionalinės teisės išsamias taisykles, kuriomis gali būti įgyvendinamas reglamentas, reikalavimas;

(24) bet koks biometrinių duomenų ir kitų asmens duomenų, susijusių su DI sistemų naudojimu biometrinio tapatybės nustatymo tikslais, naudojimas, išskyrus atvejus, kai viešosiose erdvėse teisėsaugos tikslais naudojamos tikralaikės nuotolinio biometrinio tapatybės nustatymo sistemos, kaip nustatyta šiame reglamente, ir kai šias sistemas viešosiose erdvėse kitais nei teisėsaugos tikslais naudoja kompetentingos institucijos, toliau turi derėti su visais reikalavimais, taikomais pagal Reglamento (ES) 2016/679 9 straipsnio 1 dalį, Reglamento (ES) 2018/1725 10 straipsnio 1 dalį ir Direktyvos (ES) 2016/680 10 straipsnį;

(25) pagal prie ES sutarties ir SESV pridėto Protokolo Nr. 21 dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės 6a straipsnį Airijai nėra privalomos šio reglamento 5 straipsnio 1 dalies d punkte, 2 ir 3 dalyse nustatytos taisyklės, priimtos remiantis SESV 16 straipsniu, kurios yra susijusios su valstybių narių vykdomu asmens duomenų tvarkymu vykdant veiklą, kuriai taikomas SESV trečiosios dalies V antraštinės dalies 4 arba 5 skyrius, tais atvejais, kai Airijai nėra privalomos taisyklės, kuriomis reglamentuojamos teisminio bendradarbiavimo baudžiamosiose bylose ar policijos bendradarbiavimo, kurį vykdant turi būti laikomasi pagal SESV 16 straipsnį nustatytų nuostatų, formos;

(26) pagal prie ES sutarties ir SESV pridėto Protokolo Nr. 22 dėl Danijos pozicijos 2 ir 2a straipsnius Danijai nėra privalomos ar taikomos šio reglamento 5 straipsnio 1 dalies d punkte, 2 ir 3 dalyse nustatytos taisyklės, priimtos remiantis SESV 16 straipsniu, kurios yra susijusios su valstybių narių vykdomu asmens duomenų tvarkymu atliekant veiklą, kuriai taikomas SESV trečiosios dalies V antraštinės dalies 4 arba 5 skyrius;

(27) didelės rizikos DI sistemos Sąjungos rinkai turėtų būti pateikiamos arba pradedamos naudoti tik jeigu jos atitinka tam tikrus privalomus reikalavimus. Šiais reikalavimais turėtų būti užtikrinama, kad Sąjungoje prieinamos didelės rizikos DI sistemos arba sistemos, kurių išvedinys kitu atveju naudojamas Sąjungoje, nekeltų nepriimtinos rizikos svarbiems Sąjungos interesams, kurie pripažįstami ir saugomi pagal Sąjungos teisę. DI sistemos, kurios įvardytos kaip keliančios didelę riziką, turėtų apimti tik tas sistemas, kurios daro didelį žalingą poveikį Sąjungoje esančių asmenų sveikatai,

saugumui ir pagrindinėms teisėms, ir tokiu apribojimu kuo labiau sumažinamas galimas tarptautinės prekybos suvaržymas, jei toks yra;

(28) DI sistemos galėtų sukelti neigiamas pasekmes asmenų sveikatai ir saugumui, visų pirma tais atvejais, kai tokios sistemos veikia kaip gaminių komponentai. atsižvelgiant į Sąjungos derinamųjų teisės aktų tikslus, kuriais siekiama palengvinti laisvą gaminių judėjimą vidaus rinkoje ir užtikrinti, kad tik saugūs ir kitus reikalavimus atitinkantys gaminiai patektų į rinką, svarbu, kad būtų tinkamai užkirstas kelias ir sumažinta saugumo rizika, kurią gali sukelti visas gaminys dėl savo skaitmeninių komponentų, įskaitant DI sistemas. Pavyzdžiui, vis savarankiškesni robotai, veikiantys gamybos ar asmeninės pagalbos ir priežiūros srityje, turėtų sugebėti saugiai veikti ir atlikti savo funkcijas sudėtingomis sąlygomis. Taip pat sveikatos sektoriuje, kuriame pasekmės gyvybei ir sveikatai yra itin rimtos, vis dažniau naudojamos sudėtingos diagnozavimo sistemos ir žmonėms sprendimus padedančios priimti sistemos turėtų būti patikimos ir tikslios. DI sistemos neigiamas poveikis pagal Chartiją saugomoms pagrindinėms teisėms yra ypač svarbus tuomet, kai DI sistema klasifikuojama kaip kelianti didelę riziką. Šioms teisėms priklauso teisė į žmogaus orumą, teisė į privatų ir šeimos gyvenimą, teisė į asmens duomenų apsaugą, saviraiškos laisvė ir teisė gauti informaciją, susirinkimų ir asociacijų laisvė, taip pat nediskriminavimas, vartotojų apsauga, darbuotojų teisės, neįgaliųjų teisės, teisė į veiksmingą teisių gynimą ir teisingą bylos nagrinėjimą, teisė į gynybą ir nekaltumo prezumpcija, teisė į gerą administravimą. Be šių teisių, svarbu atkreipti dėmesį į tai, kad vaikai turi specialias teises, kaip numatyta ES chartijos 24 straipsnyje ir Jungtinių Tautų vaiko teisių konvencijoje (šios teisės išplėtotos JT VTK bendrojoje pastaboje Nr. 25 dėl skaitmeninės aplinkos), pagal kuriuos reikia atsižvelgti į vaikų pažeidžiamumo aspektus ir suteikti tokią apsaugą ir priežiūrą, kuri yra būtina jų gerovei užtikrinti. Vertinant žalos, kurią gali sukelti DI sistema, rimtumą, įskaitant žalą asmenų sveikatai ir saugumui, taip pat reikėtų atsižvelgti į pagrindinę teisę į aukšto lygio aplinkos apsaugą, kaip numatyta Chartijoje ir įgyvendinta Sąjungos politikoje;

(29) dėl didelės rizikos DI sistemų, kurios yra gaminių arba sistemų saugos komponentai, arba pačios yra gaminiai arba sistemos, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008[39], Europos Parlamento ir Tarybos reglamentas (ES) Nr. 167/2013[40], Europos Parlamento ir Tarybos reglamentas (ES) Nr. 168/2013[41], Europos Parlamento ir Tarybos direktyva 2014/90/ES[42], Europos Parlamento ir Tarybos reglamentas direktyva (ES) 2016/797[43], Europos Parlamento ir Tarybos reglamentas (ES) 2018/858[44], Europos Parlamento ir Tarybos reglamentas

---

39 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

40 2013 m. vasario 5 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 167/2013 dėl žemės ir miškų ūkio transporto priemonių patvirtinimo ir rinkos priežiūros (OL L 60, 2013 3 2, p. 1).

41 2013 m. sausio 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 168/2013 dėl dviračių ir triračių transporto priemonių bei keturračių patvirtinimo ir rinkos priežiūros (OL L 60, 2013 3 2, p. 52).

42 2014 m. liepos 23 d. Europos Parlamento ir Tarybos direktyva 2014/90/ES dėl laivų įrenginių, kuria panaikinama Tarybos direktyva 96/98/EB (OL L 257, 2014 8 28, p. 146).

43 2016 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/797 dėl geležinkelių sistemos sąveikos Europos Sąjungoje (OL L 138, 2016 5 26, p. 44).

44 2018 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/858 dėl motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, komponentų ir atskirų techninių mazgų patvirtinimo ir rinkos priežiūros, kuriuo iš dalies keičiami reglamentai (EB) Nr. 715/2007 ir (EB) Nr. 595/2009 bei panaikinama Direktyva 2007/46/EB (OL L 151, 2018 6 14, p. 1).

(ES) 2018/1139[45] ir Europos Parlamento ir Tarybos reglamentas (ES) 2019/2144[46], tinkama iš dalies pakeisti šiuos aktus, siekiant užtikrinti, kad Komisija, paisydama kiekvieno sektoriaus techninių ir reglamentavimo ypatumų ir nedarydama poveikio esamiems valdymo, atitikties vertinimo ir vykdymo užtikrinimo mechanizmams ir jais nustatytiems įgaliojimams, atsižvelgia į šiame reglamente nustatytus privalomus reikalavimus didelės rizikos DI sistemoms tuo atveju, kai, remdamasi šiais išvardytais aktais, priima bet kokį būsimą deleguotąjį ar įgyvendinimo aktą;

(30) dėl DI sistemų, kurios yra gaminių saugos komponentai arba kurios pačios yra gaminiai, kuriems taikomi tam tikri Sąjungos derinamieji teisės aktai, pažymėtina, kad jas pagal šį reglamentą tinkama klasifikuoti kaip keliančias didelę riziką, jeigu atitinkamam gaminiui taikoma atitikties vertinimo procedūra, kurią pagal tą atitinkamą Sąjungos derinamąjį teisės aktą atlieka trečiosios šalies atitikties vertinimas įstaiga. Tokie gaminiai visų pirma yra mašinos, žaislai, liftai, įranga ir apsaugos sistemos, skirtos naudoti potencialiai sprogioje aplinkoje, radijo įranga, slėginiai įrenginiai, pramoginių laivų įreginiai, lynų kelio įrenginiai, dujinį kurą deginantys prietaisai, medicininiai prietaisai ir *in vitro* diagnostiniai medicinos prietaisai;

(31) DI sistemos klasifikavimas kaip keliančios didelę riziką pagal šį reglamentą nebūtinai turėtų reikšti, kad gaminys, kurio saugos komponentas yra DI sistema, arba pati DI sistema yra gaminys, laikomas keliančiu didelę riziką pagal atitinkamame Sąjungos derinamajame teisės akte nustatytus kriterijus, kurie taikomi gaminiui. Tai visų pirma pasakytina apie Europos Parlamento ir Tarybos reglamentą (ES) 2017/745[47] ir Europos Parlamento ir Tarybos reglamentą (ES) 2017/746[48], kuriuose numatyta galimybė trečiajai šaliai atlikti vidutinės rizikos ir didelės rizikos gaminių atitikties vertinimą;

(32) atskiras DI sistemas, t. y. didelės rizikos DI sistemas, išskyrus sistemas, kurios yra gaminių saugos komponentai arba kurios pačios yra gaminiai, tinkama klasifikuoti kaip keliančias didelę riziką, jeigu, atsižvelgiant į jų numatytąją paskirtį, jos kelia žalos asmenų sveikatai ir saugumui arba pagrindinėms teisėms riziką, atsižvelgiant į

---

45 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 (OL L 212, 2018 8 22, p. 1).

46 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/2144 dėl variklinių transporto priemonių, jų priekabų ir joms skirtų sistemų, sudėtinių dalių bei atskirų techninių mazgų tipo patvirtinimo reikalavimų, susijusių su jų bendrąja sauga ir transporto priemonėse esančių asmenų bei pažeidžiamų eismo dalyvių apsauga, kuriuo iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) 2018/858 ir panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 78/2009, (EB) Nr. 79/2009 ir (EB) Nr. 661/2009 ir Komisijos reglamentai (EB) 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 ir (ES) 2015/166 (OL L 325, 2019 12 16, p. 1).

47 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB (OL L 117, 2017 5 5, p. 1).

48 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES (OL L 117, 2017 5 5, p. 176).

galimos žalos dydį ir jos pasireiškimo tikimybę, ir į tai, kad šios sistemos naudojamos įvairiose šiame reglamente iš anksto konkrečiai apibrėžtose srityse. Šių sistemų identifikavimas yra grindžiamas ta pačia metodika ir kriterijais, kurie taip pat numatyti bet kuriuose būsimuose didelės rizikos DI sistemų sąrašo pakeitimuose;

(33) DI sistemų, skirtų nuotoliniam fizinių asmenų biometriniam tapatybės nustatymui, techniniai netikslumai gali lemti šališkus rezultatus ir daryti diskriminacinį poveikį. Tai ypač svarbu tuomet, kai kalbama apie amžių, tautybę, lytį arba negalią. Todėl tikralaikės ir netikralaikės nuotolinio biometrinio tapatybės nustatymo sistemos turėtų būti klasifikuojamos kaip keliančios didelę riziką. Atsižvelgiant į riziką, kurią jos gali kelti, abiejų rūšių nuotolinio biometrinio tapatybės nustatymo sistemoms turėtų būti taikomi konkretūs reikalavimai dėl registravimo pajėgumų ir žmogaus atliekamos priežiūros;

(34) dėl ypatingos svarbos infrastruktūros objektų valdymo ir veikimo pažymėtina, kad juos tinkama klasifikuoti kaip didelės rizikos DI sistemas, skirtas naudoti kaip saugos komponentus valdant ir naudojant kelių transportą ir vandens, dujų, šilumos ir elektros energijos tiekimą, nes joms sugedus arba sutrikus gali kilti rizika daugelio žmonių gyvybei ir sveikatai ir sukelti didelių įprastos socialinės ir ekonominės veiklos sutrikimų;

(35) švietimo ar profesinio mokymo srityje naudojamos DI sistemos, visų pirma suteikiant prieigą arba skiriant asmenis į švietimo ir profesinio mokymo įstaigas arba siekiant įvertinti asmenis įpareigojant juos atlikti priėmimo į švietimo įstaigą testus, turėtų būti laikomos keliančiomis didelę riziką, nes gali nulemti asmens švietimo ir profesinio kelio kryptį, taigi ir daryti poveikį jų gebėjimui užsitikrinti pragyvenimo šaltinį. Tokios sistemos, jeigu jos netinkamai sukuriamos ir naudojamos, gali pažeisti teisę į švietimą ir mokymą, taip pat teisę nebūti diskriminuojamam ir jose gali būti atkartojami istoriniai diskriminacijos modeliai;

(36) užimtumo, darbuotojų valdymo ir galimybės dirbti savarankiškai srityse naudojamos DI sistemos, visų pirma susijusios su asmenų įdarbinimu ir atranka, sprendimų dėl paaukštinimo ir darbo sutarties nutraukimo, užduočių paskirstymo, asmenų stebėsena ar vertinimu sutartiniuose darbo santykiuose priėmimu, taip pat turėtų būti klasifikuojamos kaip keliančios didelę riziką, nes tos sistemos gali daryti pastebimą poveikį tų asmenų būsimoms karjeros galimybėms ir pragyvenimo šaltiniui. Atitinkamuose sutartiniuose darbo santykiuose turėtų dalyvauti darbuotojai ir per platformas paslaugas teikiantys asmenys, kaip nurodyta 2021 m. Komisijos darbo programoje. Tokie asmenys iš esmės neturėtų būti laikomi naudotojais pagal šį reglamentą. Per darbuotojų įdarbinimo procesą ir juos vertinant, paaukštinant arba išsaugant darbo vietą, atsižvelgiant į sutartinius darbo santykius, tokios sistemos gali atkartoti istorinius diskriminacijos modelius, pavyzdžiui, tai pasakytina apie moteris, tam tikras amžiaus grupes, neįgaliuosius arba tam tikros rasinės ar etninės kilmės arba seksualinės orientacijos asmenis. DI sistemos, kurios naudojamos šių asmenų veiklos rezultatams ir elgesiui stebėti, taip pat gali daryti poveikį jų teisėms į duomenų apsaugą ir privatumą;

(37) kita sritis, kurioje DI sistemų naudojimui reikia skirti ypatingą dėmesį, yra prieiga prie tam tikrų esminių privačių ir viešųjų paslaugų ir išmokų, būtinų žmonėms tam, kad jie galėtų visapusiškai dalyvauti visuomenėje arba pagerinti savo pragyvenimo lygį, ir galimybė jomis pasinaudoti. Visų pirma DI sistemos, kurios naudojamos fizinių asmenų kredito reitingui arba kreditingumui įvertinti, turėtų būti klasifikuojamos kaip didelės rizikos DI sistemos, nes jomis remiantis asmenims suteikiama prieiga prie

finansinių išteklių arba esminių paslaugų, pavyzdžiui, apgyvendinimo, elektros energijos ir telekomunikacijų paslaugų. Dėl šiuo tikslu naudojamų DI sistemų gali būti diskriminuojami asmenys arba grupės ir atkartojami istoriniai diskriminacijos modeliai, pavyzdžiui, dėl rasinės ar etninės kilmės, negalios, amžiaus, seksualinės orientacijos, arba gali būti sukuriamos naujas diskriminacinis poveikis. Atsižvelgiant į labai ribotą poveikio mastą ir rinkoje prieinamas alternatyvas, tinkama taikyti išimtį DI sistemoms, kurias kreditingumo patikimumo ir vertinimo tikslu pradėjo naudoti smulkieji tiekėjai savo reikmėms. Fiziniai asmenys, prašantys valdžios institucijų suteikti viešosios paramos išmokas ir paslaugas, paprastai yra priklausomi nuo šių išmokų ir paslaugų ir santykyje su atsakingomis institucijomis yra pažeidžiamoje padėtyje. Jeigu DI sistemos naudojamos siekiant nustatyti, ar institucija turėtų neskirti tokių išmokų ir paslaugų, sumažinti jų dydį ar apimtį, panaikinti arba susigrąžinti, tai gali turėti reikšmingą poveikį asmenų pragyvenimui ir gali pažeisti jų pagrindines teises, pavyzdžiui, teisę į socialinę apsaugą, nediskriminavimą, žmogaus orumą arba veiksmingą teisių gynimą. Todėl šios sistemos turėtų būti klasifikuojamos kaip keliančios didelę riziką. Vis dėlto šis reglamentas neturėtų trukdyti kurti ir naudoti naujoviškus viešojo administravimo metodus, kuriuos būtų galima pritaikyti platesniu mastu naudojant reikalavimus atitinkančias ir saugias DI sistemas, jeigu jos nekelia didelės rizikos juridiniams ir fiziniams asmenims. Galiausiai DI sistemos, kurios naudojamos suteikiant arba nustatant prioritetą teikiant pirmojo skubaus atsako į incidentą paslaugą, taip pat turėtų būti klasifikuojamos kaip keliančios didelę riziką, nes jos sprendimus priima ypač kritinėse situacijose, susijusiose su asmenų gyvybe ir sveikata bei jų turtu;

(38) teisėsaugos institucijų veiksmams, kuriuos vykdant tam tikru būdu naudojamos DI sistemos, būdingas didelis galios disbalanso laipsnis ir po šių veiksmų fizinis asmuo gali būti sekamas, areštuojamas arba gali būti apribota jo laisvė, taip pat daromas kitoks neigiamas poveikis Chartijoje garantuojamoms pagrindinėms teisėms. Jeigu DI sistema mokoma naudojant nekokybiškus duomenis, jeigu ji neatitinka jai keliamų pakankamų tikslumo ar patikimumo reikalavimų arba nėra tinkamai sukurta ir išbandyta prieš pateikiant ją rinkai arba kitaip pradedant naudoti, ji gali atrinkti asmenis diskriminuojančiai arba kitokiu neteisingu arba nesąžiningu būdu. Be to, tuo atveju, kai DI sistemos nėra pakankamai skaidrios, suprantamos ir dokumentuojamos, gali būti trukdoma užtikrinti svarbias procesines pagrindines teises, pavyzdžiui, teisę į veiksmingą teisių gynimo priemonę ir sąžiningą bylos nagrinėjimą, taip pat teisę į gynybą ir nekaltumo prezumpciją. Todėl įvairias DI sistemas, skirtas naudoti teisėsaugos tikslais, kai tikslumas, patikimumas ir skaidrumas yra ypač svarbūs siekiant išvengti neigiamų pasekmių, išlaikyti visuomenės pasitikėjimą ir užtikrinti atskaitomybę bei veiksmingą teisių gynimą, tinkama klasifikuoti kaip keliančias didelę riziką. Atsižvelgiant į aptariamos veiklos pobūdį ir su ja susijusią riziką, šios didelės rizikos DI sistemos visų pirma turėtų apimti DI sistemas, skirtas naudoti teisėsaugos institucijose individualios rizikos vertinimams, poligrafams ir panašioms priemonėms, arba DI sistemas, skirtas fizinio asmens emocinei būklei nustatyti, sintetinei sankaitai nustatyti, įrodymų baudžiamojoje byloje patikimumui įvertinti, faktinių ar potencialių nusikalstamų veikų padarymo arba pakartotinio padarymo tikimybei įvertinti, remiantis fizinių asmenų profiliavimu, arba asmenybės savybėms ir bruožams arba ankstesniam fizinių asmenų ar grupių nusikalstamam elgesiui įvertinti, profiliavimui nustatant, tiriant nusikalstamas veikas arba vykdant jų baudžiamąjį persekiojimą, taip pat fizinių asmenų nusikaltimų analizės tikslais. DI sistemos, kurios skirtos konkrečiai naudoti mokesčių inspekcijų ir muitinių administracinėse bylose, neturėtų būti laikomos didelės rizikos DI sistemomis, teisėsaugos institucijų naudojamomis

nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo tikslais;

(39) migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos daro poveikį žmonėms, kurie dažnai būna ypač pažeidžiamoje padėtyje ir yra priklausomi nuo kompetentingų valdžios institucijų veiksmų rezultato. Todėl šiomis aplinkybėmis naudojamų DI sistemų tikslumas, nediskriminacinis pobūdis ir skaidrumas yra labai svarbūs, siekiant garantuoti pagarbą asmenų, kuriems daromas poveikis, pagrindinėms teisėms, ypač jų teisei laisvai judėti, teisei nebūti diskriminuojamiems, teisei į privataus gyvenimo ir asmens duomenų apsaugą, teisei į tarptautinę apsaugą ir gerą administravimą. Todėl DI sistemas, skirtas naudoti kompetentingoms institucijoms, kurioms pavestos užduotys migracijos, prieglobsčio ir sienų valdymo srityje, kaip poligrafus ir panašias priemones arba siekiant nustatyti fizinio asmens emocinę būklę, įvertinti tam tikrą riziką, kurią fiziniai asmenys kelia atvykdami į valstybės narės teritoriją arba prašydami išduoti vizą arba suteikti prieglobstį, patikrinti fizinių asmenų dokumentų autentiškumą, padėti kompetentingoms valdžios institucijoms išnagrinėti prašymus suteikti prieglobstį, išduoti vizą ir leidimą gyventi, ir susijusius skundus, siekiant nustatyti fizinių asmenų tinkamumą prašyti suteikti pabėgėlio statusą, tinkama klasifikuoti kaip didelės rizikos DI sistemas. Migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos, kurioms taikomas šis reglamentas, turėtų atitikti susijusius procedūrinius reikalavimus, nustatytus Europos Parlamento ir Tarybos direktyvoje 2013/32/ES[49], Europos Parlamento ir Tarybos reglamente (EB) Nr. 810/2009[50] ir kituose susijusiuose teisės aktuose;

(40) tam tikros DI sistemos, skirtos teisingumui vykdyti ir demokratiniams procesams, turėtų būti klasifikuojamos kaip keliančios didelę riziką, atsižvelgiant į tai, kad jos gali daryti reikšmingą poveikį demokratijai, teisinės valstybės principui, individualioms laisvėms, taip pat teisei į veiksmingą teisių gynimo priemonę ir teisingą bylos nagrinėjimą. Visų pirma siekiant šalinti galimą šališkumo, klaidų ir neskaidrumo riziką, didelės rizikos DI sistemoms tinkama priskirti sistemas, kurių paskirtis – padėti teisminėms institucijoms tirti ir aiškinti faktus ir teisės aktus ir taikyti įstatymus konkretiems faktų rinkiniams. Tačiau toks klasifikavimas neturėtų būti taikomas DI sistemoms, skirtoms tik papildomai administracinei veiklai, kuri nedaro poveikio faktiniam teisingumo vykdymui individualiais atvejais, pavyzdžiui, teismo sprendimų, dokumentų arba duomenų anoniminimui arba pseudoniminimui, darbuotojų tarpusavio ryšiams, administracinėms užduotims arba išteklių paskirstymui;

(41) tai, kad DI sistema pagal šį reglamentą klasifikuojama kaip kelianti didelę riziką, neturėtų būti vertinama kaip požymis, iš kurio matyti, kad sistemos naudojimas būtinai yra teisėtas pagal kitus Sąjungos teisės aktus arba nacionalinę teisę, kuri yra suderinama su Sąjungos teise, pavyzdžiui, dėl asmens duomenų apsaugos, poligrafų ir panašių priemonių ar kitų sistemų naudojimo siekiant nustatyti fizinių asmenų emocinę būklę. Bet kuris toks naudojimas turėtų būti tęsiamas tik laikantis iš Chartijos ir taikomų Sąjungos antrinės teisės aktų ir nacionalinės teisės kylančių taikytinų reikalavimų. Nereikėtų manyti, kad šiame reglamente nustatytas teisinis asmens

[49] 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/32/ES dėl tarptautinės apsaugos suteikimo ir panaikinimo bendros tvarkos (OL L 180, 2013 6 29, p. 60).

[50] 2009 m. liepos 13 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 810/2009, nustatantis Bendrijos vizų kodeksą (Vizų kodeksas) (OL L 243, 2009 9 15, p. 1).

duomenų, kai tinkama, įskaitant specialias asmens duomenų kategorijas, tvarkymo pagrindas;

(42) siekiant sumažinti didelės rizikos DI sistemų, pateikiamų arba kitaip pradėtų naudoti Sąjungos rinkoje, naudotojams arba paveiktiems asmenims keliamą riziką, reikėtų taikyti tam tikrus privalomus reikalavimus, atsižvelgiant į numatytąją sistemos naudojimo paskirtį ir paisant rizikos valdymo sistemos, kurią privalo nustatyti tiekėjas;

(43) reikalavimai turėtų būti taikomi didelės rizikos DI sistemoms tiek, kiek tai susiję su naudojamų duomenų rinkinių kokybe, techniniais dokumentais ir įrašų saugojimu, skaidrumu ir informacijos teikimu naudotojams, žmogaus vykdoma priežiūra, patikimumu, tikslumu ir kibernetiniu saugumu. Šie reikalavimai yra būtini siekiant veiksmingai sumažinti riziką sveikatai, saugumui ir pagrindinėms teisėms kartu atsižvelgiant į numatytąją sistemos paskirtį, ir jeigu nėra pagrįstai prieinamų jokių kitų mažiau prekybą ribojančių priemonių, taip išvengiant nepagrįstų prekybos apribojimų;

(44) kokybiški duomenys turi esminę reikšmę užtikrinant daugybės DI sistemų efektyvų veikimą, ypač tais atvejais, kai naudojami su mokymo modeliais susiję metodai, siekiant užtikrinti, kad didelės rizikos DI sistema veiktų kaip numatyta ir saugiai ir netaptų pagal Sąjungos teisę draudžiamos diskriminacijos šaltiniu. Kokybiškų mokymų, validavimo ir bandymo duomenų rinkinių srityje reikia įgyvendinti tinkamą duomenų valdymo ir administravimo praktiką. Mokymų, validavimo ir bandymo duomenų rinkiniai turėtų būti pakankamai aktualūs, reprezentatyvūs ir be klaidų bei išsamūs, kad būtų užtikrinta numatytoji sistemos paskirtis. Jie taip pat turėtų turėti tinkamus statistinius ypatumus, įskaitant duomenis apie asmenis arba asmenų grupes, kurių atžvilgiu numatyta naudoti didelės rizikos DI sistemą. Visų pirma reikėtų atsižvelgti į mokymų, validavimo ir bandymo duomenų rinkinius tiek, kiek to reikia atsižvelgiant į jų numatytąją paskirtį, ypatumus, savybes arba elementus, kurie yra būdingi konkrečioje geografinėje, elgsenos ar funkcinėje aplinkoje arba aplinkybėmis, kuriomis numatoma naudoti DI sistemą. Siekiant apsaugoti kitų asmenų teises nuo diskriminacijos, kurią gali sukelti šališkos DI sistemos, tiekėjai turėtų turėti galimybę tvarkyti ir specialių kategorijų asmens duomenis, jei tai yra susiję su esminiu viešuoju interesu, siekdami užtikrinti didelės rizikos DI sistemų šališkumo stebėseną, nustatymą ir ištaisymą;

(45) kad galėtų kurti didelės rizikos DI sistemas, tam tikri subjektai, pavyzdžiui, tiekėjai, notifikuotosios įstaigos ir kiti susiję subjektai, pavyzdžiui, skaitmeninių inovacijų centrai, bandymų vykdymo institucijos ir tyrėjai, turėtų turėti galimybę naudoti kokybiškus duomenų rinkinius savo atitinkamose veiklos srityse, susijusiose su šiuo reglamentu. Komisijos sukurtos Europos bendros duomenų erdvės ir dalijimosi duomenimis tarp įmonių ir vyriausybės viešojo intereso labui palengvinimas bus labai svarbus suteikiant patikimą, atskaitingą ir nediskriminuojančią prieigą prie kokybiškų duomenų, reikalingų DI sistemų mokymui, validavimui ir bandymui. Pavyzdžiui, sveikatos sektoriuje Europos sveikatos duomenų erdvė palengvins nediskriminacinę prieigą prie sveikatos duomenų ir dirbtinio intelekto algoritmų mokymą naudojant šiuos duomenų rinkinius užtikrinant privatumą, saugumą, savalaikiškumą, skaidrumą ir patikimumą ir numatant tinkamą institucinį valdymą. Atitinkamos kompetentingos institucijos, įskaitant sektorių institucijas, teikiančios arba padedančios gauti prieigą prie duomenų, taip pat gali remti kokybiškų duomenų teikimą DI sistemų mokymo, validavimo ir bandymo tikslais;

(46) informacijos apie tai, kaip buvo sukurtos didelės rizikos DI sistemos ir kaip jos veikia per visą savo gyvavimo ciklą, turėjimas yra labai svarbus siekiant patikrinti atitiktį šio

reglamento reikalavimams. Šiuo tikslu reikia saugoti įrašus ir užtikrinti techninių dokumentų, kuriuose pateikiama informacija, būtina DI sistemos atitikčiai atitinkamiems reikalavimams įvertinti, prieinamumą. Tokią informaciją turėtų sudaryti bendrieji sistemos ypatumai, pajėgumai ir apribojimai, algoritmai, duomenys, mokymai, bandymai ir naudojami validavimo procesai, taip pat dokumentacija apie atitinkamą rizikos valdymo sistemą. Techniniai dokumentai turėtų būti nuolat atnaujinama;

(47) siekiant spręsti neskaidrumo problemą, dėl kurios tam tikros DI sistemos fiziniams asmenims gali būti nesuprantamos arba pernelyg sudėtingos, didelės rizikos DI sistemoms reikėtų nustatyti reikalavimus dėl tam tikro skaidrumo lygio. Naudotojai turėtų turėti galimybę aiškinti sistemos išvedinį ir jį tinkamai panaudoti. Todėl dėl didelės rizikos DI sistemų turėtų būti parengiama atitinkama dokumentacija ir naudojimo instrukcijos, įskaitant nuoseklią ir aiškią informaciją, be kita ko, susijusią su galima rizika pagrindinėms teisėms ir, kai tinkama, diskriminacija;

(48) didelės rizikos DI sistemos turėtų būti kuriamos ir plėtojamos taip, kad fiziniai asmenys galėtų prižiūrėti jų veikimą. Šiuo tikslu sistemos tiekėjas prieš pateikdamas sistemą rinkai arba pradėdamas ją naudoti turėtų nustatyti atitinkamas žmogaus atliekamos priežiūros priemones. Visų pirma, kai tinkama, tokiomis priemonėmis turėtų būti garantuojama, kad sistemai būtų taikomi integruoti veikimo apribojimai, kurie būtų nepriklausomi nuo pačios sistemos ir kuriuos galėtų kontroliuoti žmogus, ir kad fiziniai asmenys, kuriems pavesta atlikti žmogaus priežiūrą, turėtų būtiną kompetenciją, kvalifikaciją ir įgaliojimus atlikti tą funkciją;

(49) didelės rizikos DI sistemos turėtų veikti nuosekliai per visą savo gyvavimo ciklą ir atitikti atitinkamą tikslumo, patvarumo ir kibernetinio saugumo lygį, kuris derėtų su visuotinai pripažintomis naujausiomis technologijomis. Naudotojus reikėtų informuoti apie tikslumo lygį ir tikslumo metriką;

(50) techninis patvarumas yra pagrindinis didelės rizikos DI sistemoms keliamas reikalavimas. DI sistemos turėtų būti atsparios su sistema susijusių apribojimų keliamai rizikai (pvz., klaidoms, triktims, nesuderinamumo atvejams, netikėtoms situacijoms), taip pat kenkėjiškiems veiksmams, dėl kurių gali būti pažeistas DI sistemos saugumas ir atsirasti žalingas arba kitoks nepageidaujamas elgesys. Nesugebėjimas apsisaugoti nuo šios rizikos galėtų sukelti pasekmių saugumui arba daryti neigiamą poveikį pagrindinėms teisėms, pavyzdžiui, dėl klaidingų sprendimų arba neteisingų arba šališkų DI sistemos sugeneruotų išvedinių;

(51) kibernetinis saugumas atlieka esminį vaidmenį užtikrinant, kad DI sistemos būtų atsparios bandymams pakeisti jų naudojimo būdą, elgseną, veikimą arba jų saugumo funkcijų pažeidimui trečiosioms šalims imantis kenkėjiškų veiksmų sistemos pažeidžiamumui išnaudoti. Kibernetiniai išpuoliai prieš DI sistemas gali turėti įtakos konkrečiam DI turtui, pavyzdžiui, mokymo duomenų rinkiniams (pvz., klaidingų duomenų įrašymas, angl. *data poisoning*) arba išmokytiems modeliams (pvz., priešiški pavyzdžiai), arba gali būti išnaudojamas DI sistemos skaitmeninio turto arba pagrindinės IRT infrastruktūros pažeidžiamumas. Todėl didelės rizikos DI sistemų tiekėjai, siekdami užtikrinti tokį kibernetinio saugumo lygį, kuris atitiktų riziką, turėtų imtis tinkamų priemonių kartu, kai tinkama, atsižvelgdami į pagrindinę IRT infrastruktūrą;

(52) atsižvelgiant į Sąjungos derinamuosius teisės aktus, didelės rizikos DI sistemų pateikimui rinkai, pradėjimui naudoti ir naudojimui taikytinos taisyklės turėtų derėti su Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008[51], kuriuo nustatomi su gaminių prekyba susiję akreditavimo ir rinkos priežiūros reikalavimai, Europos Parlamento ir Tarybos sprendimu 768/2008/EB[52] dėl bendrosios gaminių pardavimo sistemos ir Europos Parlamento ir Tarybos reglamentu (ES) 2019/1020[53] dėl rinkos priežiūros ir gaminių atitikties (naujoji gaminių pardavimo teisės aktų sistema);

(53) būtų tinkama, kad konkretus fizinis arba juridinis asmuo, kuris apibrėžiamas kaip tiekėjas, prisiimtų atsakomybę už didelės rizikos DI sistemos pateikimą rinkai arba pradėjimą naudoti, nepaisant to, ar fizinis arba juridinis asmuo yra sistemą sukūręs ar išplėtojęs asmuo;

(54) tiekėjas turėtų sukurti patikimą kokybės valdymo sistemą, užtikrinti, kad būtų įgyvendinta reikalaujama atitikties vertinimo procedūra, parengta atitinkama dokumentacija ir sukurta patikima priežiūros po pateikimo rinkai sistema. Valdžios institucijos, kurios pradėjo naudoti didelės rizikos DI sistemas savo reikmėms, atsižvelgdamos į sektoriaus specifiką ir atitinkamos valdžios institucijos kompetenciją ir organizacijos struktūrą, gali priimti ir įgyvendinti kokybės valdymo sistemos taisykles, kurios yra atitinkamai nacionaliniu arba regioniniu lygmeniu nustatytos kokybės valdymo sistemos komponentas;

(55) jeigu didelės rizikos DI sistema, kuri yra gaminio, kuriam taikomas naujosios teisės aktų sistemos teisės aktas, saugos komponentas, rinkai nepateikiama arba nepradedama naudoti nepriklausomai nuo gaminio, galutinio gaminio gamintojas, kaip apibrėžta naujosios teisės aktų sistemos teisės akte, turėtų laikytis šiame reglamente nustatytų pareigų tiekėjui, visų pirma užtikrinti, kad galutiniame gaminyje integruota DI sistema atitiktų šio reglamento reikalavimus;

(56) siekiant sudaryti sąlygas šio reglamento vykdymo užtikrinimui ir sukurti vienodas sąlygas veiklos vykdytojams ir atsižvelgiant į įvairias skaitmeninių gaminių tiekimo užtikrinimo formas, svarbu užtikrinti, kad visomis aplinkybėmis Sąjungoje įsisteigęs asmuo galėtų institucijoms pateikti visą būtiną informaciją apie DI sistemos atitiktį. Todėl prieš užtikrinant DI sistemų prieinamumą Sąjungoje, jeigu negalima nustatyti importuotojo tapatybės, už Sąjungos ribų įsisteigę tiekėjai rašytiniu įgaliojimu paskiria Sąjungoje įsisteigusį įgaliotąjį atstovą;

(57) laikantis naujosios teisės aktų sistemos principų, atitinkamiems ekonominės veiklos vykdytojams, pavyzdžiui, importuotojams ir platintojams, reikėtų nustatyti konkrečias pareigas, kad būtų užtikrintas teisinis tikrumas ir palengvinta šių atitinkamų veiklos vykdytojų atitiktis reglamentavimo reikalavimams;

(58) atsižvelgiant į DI sistemų pobūdį ir riziką saugumui ir pagrindinėms teisėms, kurios gali būti susijusios su jų naudojimu, įskaitant poreikį užtikrinti tinkamą DI sistemos

---

51 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

52 2008 m. liepos 9 d. Europos Parlamento ir Tarybos sprendimas Nr. 768/2008/EB dėl bendrosios gaminių pardavimo sistemos ir panaikinantis Tarybos sprendimą 93/465/EEB (OL L 218, 2008 8 13, p. 82).

53 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1020 dėl rinkos priežiūros ir gaminių atitikties, kuriuo iš dalies keičiama Direktyva 2004/42/EB ir reglamentai (EB) Nr. 765/2008 ir (ES) Nr. 305/2011 (tekstas svarbus EEE) (OL L 169, 2019 6 25, p. 1–44).

efektyvų veikimą realiomis sąlygomis, tinkama naudotojams nustatyti konkrečias pareigas. Naudotojai didelės rizikos DI sistemas visų pirma turėtų naudoti laikydamiesi naudojimosi instrukcijų, be to, turėtų būti numatytos tam tikros kitos pareigos, susijusios su DI sistemų veikimo stebėsena ir, kai tinkama, įrašų tvarkymu;

(59) tinkama numatyti, kad DI sistemos naudotojas turėtų būti fizinis arba juridinis asmuo, valdžios institucija, agentūra arba kita įstaiga, kuriai vadovaujant naudojama DI sistema, išskyrus atvejus, kai DI sistema naudojama vykdant privačią neprofesinę veiklą;

(60) atsižvelgiant į sudėtingą dirbtinio intelekto vertės grandinę, atitinkamos trečiosios šalys, visų pirma dalyvaujančios parduodant ir tiekiant programinę įrangą, programinės įrangos priemones ir komponentus, iš anksto išmokytus modelius ir duomenis arba teikiant tinklo paslaugas, kai tinkama, turėtų bendradarbiauti su tiekėjais ir naudotojais, kad sudarytų jiems sąlygas laikytis pareigų pagal šį reglamentą, ir su pagal šį reglamentą įsteigtomis kompetentingomis institucijomis;

(61) standartizacija turėtų atlikti pagrindinį vaidmenį, siekiant tiekėjams suteikti techninius sprendimus ir taip užtikrinti atitiktį šiam reglamentui. Atitiktis darniesiems standartams, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) Nr. 1025/2012[54], turėtų būti viena iš priemonių tiekėjams įrodyti atitiktį šio reglamento reikalavimams. Tačiau Komisija galėtų priimti bendras techninės specifikacijas srityse, kuriose nėra darniųjų standartų arba jie yra nepakankami;

(62) siekiant užtikrinti aukšto lygio didelės rizikos DI sistemų patikimumą, šioms sistemoms turėtų būti taikomas reikalavimas atlikti atitikties vertinimą prieš pateikiant jas rinkai arba pradedant naudoti;

(63) tinkama, kad, siekiant kuo labiau sumažinti naštą veiklos vykdytojams ir išvengti bet kokio galimo dubliavimo, didelės rizikos DI sistemoms, susijusioms su gaminiais, kuriems, vadovaujantis naujosios teisės aktų sistemos principu, taikomi esami Sąjungos derinamieji teisės aktai, šių DI sistemų atitiktis šio reglamento reikalavimams turėtų būti vertinama atliekant pagal tuos teisės aktus jau numatytą atitikties vertinimą. Todėl šio reglamento reikalavimų taikymas neturėtų daryti poveikio konkrečiai atitikties vertinimo, atliekamo pagal atitinkamus naujosios teisės aktų sistemos teisės aktus, logikai, metodikai ar bendrajai struktūrai. Šis principas visiškai atsispindi atsižvelgiant į šio reglamento ir [Mašinų reglamento] sąveiką. Nors DI sistemų, kuriomis užtikrinamos saugios mašinų funkcijos, saugos rizikai taikomi šio reglamento reikalavimai, tam tikri [Mašinų reglamento] konkretūs reikalavimai padės užtikrinti saugią DI sistemos integravimą į visas mašinas, kad nebūtų pažeista visų mašinų sauga. [Mašinų reglamente] taikoma tokia pati DI sistemos apibrėžtis kaip ir šiame reglamente;

(64) atsižvelgiant į didesnę profesionalių sertifikuotojų prieš pateikiant rinkai patirtį gaminių saugos srityje ir skirtingą kylančios rizikos pobūdį, tinkama riboti (bent jau pradiniame šio reglamento taikymo etape) trečiosios šalies atliekamo didelės rizikos DI sistemų, išskyrus su gaminiais susijusias DI sistemas, atitikties vertinimo taikymo sritį. Todėl tokių sistemų atitikties vertinimą paprastai turėtų atlikti tiekėjas ir už tai

[54] 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12).

atsakyti, išskyrus vienintelę išimtį, susijusią su DI sistemomis, kurios skirtos naudoti nuotolinio biometrinio asmenų tapatybės nustatymo tikslais, kai turėtų būti numatyta notifikuotosios įstaigos galimybė dalyvauti atliekant atitikties vertinimą, jei minėtos DI sistemos nedraudžiamos;

(65) siekiant, kad trečioji šalis atliktų DI sistemų, skirtų naudoti nuotolinio biometrinio asmens tapatybės nustatymo tikslais, atitikties vertinimą, nacionalinės kompetentingos institucijos pagal šį reglamentą turėtų paskirti notifikuotąsias įstaigas, jeigu jos atitinka reikalavimų rinkinį, visų pirma nepriklausomumo, kompetencijos ir interesų konflikto nebuvimo reikalavimus;

(66) laikantis bendrai nustatytos gaminių, reglamentuojamų pagal Sąjungos derinamuosius teisės aktus, esminio pakeitimo sąvokos, tinkama, kad DI sistemos atitiktis būtų iš naujo įvertinta visais atvejais, kai jos pakeitimas gali daryti poveikį sistemos atitikčiai šiam reglamentui arba kai pasikeičia sistemos numatytoji paskirtis. Be to, dėl DI sistemų, kurios toliau mokosi po to, kai buvo pateiktos rinkai arba pradėtos naudoti (t. y. jos automatiškai pritaiko funkcijų vykdymą), būtina numatyti taisykles, kuriomis nustatoma, kad algoritmo ir jo efektyvaus veikimo, kurį iš anksto nustato tiekėjas ir kuris buvo įvertintas atitikties vertinimo metu, pakeitimai neturėtų būti esminiu pakeitimu;

(67) kad didelės rizikos DI sistemos galėtų laisvai judėti vidaus rinkoje, jos turėtų būti ženklinamos CE ženklu, iš kurio būtų matyti, kad jos atitinka šį reglamentą. Valstybės narės neturėtų sudaryti nepagrįstų kliūčių pateikti rinkai ar pradėti naudoti didelės rizikos DI sistemas, kurios atitinka šiame reglamente nustatytus reikalavimus ir yra paženklintos CE ženklu;

(68) tam tikromis sąlygomis galimybė greitai pasinaudoti inovatyviomis technologijomis gali būti labai svarbi asmenų sveikatai bei saugai ir visai visuomenei. Todėl išimtinėmis su viešuoju saugumu arba fizinių asmenų gyvybės ir sveikatos apsauga ir pramoninės bei komercinės nuosavybės apsauga susijusiomis aplinkybėmis valstybės narės galėtų leisti pateikti rinkai arba pradėti naudoti DI sistemas, kurių atitikties vertinimas nebuvo atliktas;

(69) siekiant palengvinti Komisijos ir valstybių narių darbą dirbtinio intelekto srityje, taip pat padidinti skaidrumą visuomenės atžvilgiu, turėtų būti reikalaujama, kad didelės rizikos DI sistemų, išskyrus DI sistemas, susijusias su gaminiais, kuriems taikomi atitinkami esami Sąjungos derinamieji teisės aktai, tiekėjai įregistruotų savo didelės rizikos DI sistemą Komisijos sukursimoje ir tvarkomoje duomenų bazėje. Komisija turėtų būti šios duomenų bazės valdytoja, laikantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[55]. Siekiant užtikrinti visapusišką įdiegtos duomenų bazės veikimą, pagal duomenų bazės kūrimo procedūrą turėtų būti numatyta, kad Komisija parengs funkcines specifikacijas ir kad bus parengta nepriklausomo audito ataskaita;

(70) tam tikros DI sistemos, kurių paskirtis – sąveikauti su fiziniais asmenimis arba kurti turinį, gali kelti konkrečią apsimetinėjimo arba apgaulės riziką, nepaisant to, ar jos klasifikuojamos kaip didelės rizikos DI sistemos, ar ne. Todėl šių sistemų naudojimui tam tikromis aplinkybėmis turėtų būti taikomi konkretūs skaidrumo įpareigojimai, nedarant poveikio didelės rizikos DI sistemoms taikomiems reikalavimams ir

[55] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

įpareigojimams. Visų pirma fizinius asmenis reikėtų informuoti, kad jie sąveikauja su DI sistema, išskyrus atvejus, kai tai aiškiai matyti iš aplinkybių ir naudojimo konteksto. Be to, fizinius asmenis reikėtų informuoti apie tai, kad jiems taikoma emocijų atpažinimo sistema arba biometrinio kategorizavimo sistema. Tokia informacija ir pranešimai neįgaliesiems turėtų būti teikiami prieinama forma. Be to, DI sistemų, kuriomis sukuriamas į realius asmenis, objektus, vietas ar kitus dalykus ar įvykius labai panašus judamo bei nejudamo vaizdo ir garso turinys, kurį asmuo gali klaidingai palaikyti autentišku, naudotojai turėtų nurodyti, kad tas turinys sukurtas dirbtinai arba kad su juo atliktos manipuliacijos, atitinkamai paženklinant dirbtinio intelekto išvedinį ir atskleidžiant informaciją apie jo dirbtinė kilmę;

(71) dirbtinis intelektas yra sparčiai besivystanti technologijų grupė, kuriai reikalinga naujų formų reglamentavimo priežiūra ir saugi eksperimentavimo erdvė, kartu užtikrinant atsakingas inovacijas ir tinkamų apsaugos ir rizikos mažinimo priemonių integraciją. Siekiant užtikrinti inovacijoms palankią, į ateitį orientuotą ir sutrikdymams atsparią teisinę sistemą, vienos ar daugiau valstybių narių nacionalinės kompetentingos institucijos turėtų būti skatinamos sukurti dirbtinio intelekto apribotą bandomąją reglamentavimo aplinką, kad būtų palengvintas naujoviškų DI sistemų kūrimas ir bandymas taikant griežtą reglamentavimo priežiūrą iki šių sistemų pateikimo rinkai arba pradėjimo naudoti;

(72) apribotos bandomosios reglamentavimo aplinkos tikslai turėtų būti susiję su DI inovacijų skatinimu sukuriant kontroliuojamą eksperimentavimo ir bandymų aplinką, kuri būtų taikoma kūrimo etapu ir etapu prieš pateikimą rinkai, siekiant užtikrinti naujoviškų DI sistemų atitiktį šiam reglamentui ir kitiems susijusiems Sąjungos ir valstybių narių teisės aktams. Siekiant didinti novatorių teisinį tikrumą ir kompetentingų institucijų priežiūrą ir supratimą apie galimybes, naują riziką ir DI naudojimo poveikį ir paspartinti patekimą į rinką, įskaitant kliūčių mažosioms ir vidutinėms įmonėms (MVĮ) ir startuoliams pašalinimą. Kad būtų užtikrintas vienodas įgyvendinimas visoje Sąjungoje ir masto ekonomija, tinkama sukurti bendras apribotos bandomosios reglamentavimo aplinkos įgyvendinimo taisykles ir atitinkamų institucijų, dalyvaujančių vykdant apribotos bandomosios aplinkos priežiūrą, bendradarbiavimo sistemą. Šiame reglamente turėtų būti numatytas asmens duomenų, kurie buvo surinkti kitais tikslais, siekiant DI apribotoje bandomojoje reglamentavimo aplinkoje sukurti tam tikras su viešuoju interesu susijusias DI sistemas, naudojimo teisinis pagrindas, laikantis Reglamento (ES) 2016/679 6 straipsnio 4 dalies ir Reglamento (ES) 2018/1725 6 straipsnio ir nedarant poveikio Direktyvos (ES) 2016/680 4 straipsnio 2 daliai. Bandomosios aplinkos dalyviai turėtų užtikrinti tinkamas apsaugos priemones ir bendradarbiauti su kompetentingomis institucijomis, taip pat vadovautis jų rekomendacijomis ir veikti greitai bei sąžiningai, kad sumažintų bet kokią didelę riziką saugumui ir pagrindinėms teisėms, kurios gali kilti kuriant ir eksperimentuojant bandomojoje aplinkoje. Kompetentingoms institucijoms nusprendžiant, ar skirti administracinę nuobaudą pagal Reglamento 2016/679 83 straipsnio 2 dalį ir Direktyvos 2016/680 57 straipsnį, reikėtų atsižvelgti į dalyvių elgesį bandomojoje aplinkoje;

(73) siekiant skatinti ir apsaugoti inovacijas, svarbu, kad būtų konkrečiai atsižvelgiama į DI sistemų smulkiųjų tiekėjų ir naudotojų interesus. Siekdamos šio tikslo, valstybės narės turėtų rengti šiems veiklos vykdytojams skirtas iniciatyvas, įskaitant informuotumo didinimą ir informacijos perdavimą. Be to, notifikuotosios įstaigos, nustatydamos atitikties vertinimo mokesčius, turi atsižvelgti į konkrečius smulkiųjų tiekėjų interesus ir poreikius. tiekėjai ir kiti veiklos vykdytojai, visų pirma smulkieji, gali patirti didelių

vertimo raštu išlaidų, susijusių su privaloma dokumentacija ir komunikacija su institucijomis. Valstybės narės turėtų numatyti galimybę užtikrinti, kad viena iš jų nustatytų ir priimtų kalbų, vartojamų atitinkamiems tiekėjams rengiant dokumentaciją ir bendraujant su veiklos vykdytojais, būtų plačiai suprantama kuo didesniam tarpvalstybinių naudotojų ratui;

(74) siekiant kuo labiau sumažinti įgyvendinimo riziką, kuri atsiranda dėl žinių ir patirties rinkoje trūkumo, taip pat siekiant palengvinti tiekėjų ir notifikuotųjų įstaigų pareigų pagal šį reglamentą laikymąsi, reikminė DI platforma, Europos skaitmeninių inovacijų centrai ir Komisijos, valstybių narių nacionaliniu ar ES lygmeniu sukurta bandymų ir eksperimentų infrastruktūra turėtų padėti įgyvendinti šį reglamentą. Atsižvelgiant į atitinkamą misiją ir kompetencijos sritis, jos gali teikti konkrečią techninę ir mokslinę paramą tiekėjams ir notifikuotosioms įstaigoms;

(75) Komisija, kiek įmanoma, turėtų palengvinti įstaigų, grupių arba laboratorijų, įsteigtų arba akredituotų pagal bet kurį atitinkamą Sąjungos derinamąjį aktą ir vykdančių gaminių arba prietaisų, kuriems taikomi Sąjungos derinamieji teisės aktai, atitikties vertinimą, prieigą prie bandymų ir eksperimentų infrastruktūros. Tai visų pirma pasakytina apie ekspertų kolegijas, ekspertų laboratorijas ir etalonines laboratorijas, veikiančias medicinos priemonių srityje pagal Reglamentą (ES) 2017/745 ir Reglamentą (ES) 2017/746;

(76) siekiant palengvinti sklandų, veiksmingą ir suderintą šio reglamento įgyvendinimą, reikėtų įsteigti Europos dirbtinio intelekto valdybą. Valdyba turėtų būti atsakinga už įvairias patariamąsias užduotis, taip pat nuomonių, rekomendacijų, patarimų ar gairių šio reglamento įgyvendinimo klausimais priėmimą, įskaitant klausimais dėl techninių specifikacijų arba esamų standartų, susijusių su šiame reglamente nustatytais reikalavimais, ir konsultuoti Komisiją bei jai padėti konkrečiais klausimais, susijusiais su dirbtiniu intelektu;

(77) labai svarbus vaidmuo taikant šį reglamentą ir užtikrinant jo vykdymą tenka valstybėms narėms. Šiuo atžvilgiu kiekviena valstybė narė turėtų paskirti vieną ar daugiau nacionalinių kompetentingų institucijų, kad jos prižiūrėtų, kaip taikomas ir įgyvendinamas šis reglamentas. Siekiant veiksmingesnės organizacijos valstybėse narėse ir sukurti oficialų ryšių palaikymo centrą, į kurį valstybės narės ir Sąjungos lygmeniu galėtų kreiptis valdžios ir kitos institucijos, kiekvienoje valstybėje narėje turėtų būti paskirta viena nacionalinė institucija, kuri veiktų kaip nacionalinė priežiūros institucija;

(78) siekiant užtikrinti, kad didelės rizikos DI sistemų tiekėjai galėtų atsižvelgti į didelės rizikos DI sistemų naudojimo patirtį, kad patobulintų savo sistemas ir kūrimo bei plėtojimo procesą arba laiku galėtų imtis bet kokių galimų taisomųjų veiksmų, visi tiekėjai turėtų turėti veikiančias priežiūros po pateikimo rinkai sistemas. Ši sistema taip pat yra labai svarbi užtikrinant, kad dėl DI sistemų, kurios toliau mokosi po to, kai buvo pateiktos rinkai arba pradėtos naudoti, galinti kilti nauja rizika būtų šalinama veiksmingiau ir laiku. Šiomis aplinkybėmis tiekėjai taip pat turėtų turėti sistemą, kurią naudodami praneštų atitinkamoms institucijoms apie bet kokius didelius incidentus arba bet kokius nacionalinės ar Sąjungos teisės, kuria apsaugomos pagrindinės teisės, pažeidimus, padarytus naudojant savo DI sistemas;

(79) siekiant užtikrinti tinkamą ir veiksmingą šiame reglamente, kuris yra Sąjungos derinamasis teisės aktas, nustatytų reikalavimų ir pareigų vykdymą, turėtų būti visa apimtimi taikoma rinkos priežiūros ir gaminių atitikties sistema, nustatyta Reglamentu (ES) 2019/1020. Jei tai būtina atsižvelgiant į nacionalinių valdžios institucijų ar

įstaigų, prižiūrinčių Sąjungos teisės aktų, kuriais apsaugomos pagrindinės teisės, taikymą, įskaitant lygybės institucijas, įgaliojimus, šios institucijos ir įstaigos taip pat turėtų turėti prieigą prie bet kokių pagal šį reglamentą sukurtų dokumentų;

(80) Sąjungos teisės aktuose dėl finansinių paslaugų nustatytos vidaus valdymo ir rizikos valdymo taisyklės ir reikalavimai, kurie yra taikomi reguliuojamoms finansų įstaigoms joms teikiant paslaugas, įskaitant atvejus, kai jos naudoja DI sistemas. Siekiant užtikrinti nuoseklų pareigų pagal šį reglamentą ir Sąjungos finansinių paslaugų teisės aktuose nustatytų taisyklių ir reikalavimų taikymą ir vykdymo užtikrinimą, už finansinių paslaugų teisės aktų priežiūrą ir vykdymo užtikrinimą atsakingos institucijos įskaitant, kai taikoma, Europos Centrinį Banką, turėtų būti paskirtos kompetentingomis institucijomis, atsakingomis už šio reglamento įgyvendinimo priežiūrą, taip pat rinkos priežiūros veiklos vykdymą, kiek tai susiję su DI sistemomis, kurias tiekia arba naudoja reguliuojamos ir prižiūrimos finansų įstaigos. Siekiant toliau didinti šio reglamento ir pagal Europos Parlamento ir Tarybos direktyvą 2013/36/ES[56] reglamentuojamoms kredito įstaigoms taikomų taisyklių nuoseklumą, taip pat yra tinkama atitikties vertinimo procedūrą ir kai kurias tiekėjų procedūrines pareigas, susijusias su rizikos valdymu, priežiūra po pateikimo rinkai ir dokumentacija, integruoti į Direktyvoje 2013/36/ES nustatytas esamas pareigas ir procedūras. Siekiant išvengti sutapimų, taip pat reikėtų numatyti ribotas nukrypti leidžiančias nuostatas, susijusias su tiekėjų kokybės valdymo sistema, ir didelės rizikos DI sistemų naudotojams nustatyti stebėsenos pareigą tiek, kiek ji taikoma pagal Direktyvą 2013/36/ES reglamentuojamoms kredito įstaigoms;

(81) DI sistemų, išskyrus didelės rizikos DI sistemas, kūrimas laikantis šio reglamento reikalavimų gali prisidėti prie platesnio masto patikimo dirbtinio intelekto naudojimo Sąjungoje. Didelės rizikos nekeliančių DI sistemų tiekėjai turėtų būti skatinami kurti elgesio kodeksus, kuriais siekiama remti savanorišką privalomų reikalavimų, nustatytų didelės rizikos DI sistemoms, taikymą. Tiekėjai taip pat turėtų būti skatinami savanoriškai taikyti papildomus reikalavimus, susijusius, pavyzdžiui, su aplinkos tvarumu, neįgaliųjų asmenų prieiga, suinteresuotųjų subjektų dalyvavimu projektuojant ir kuriant DI sistemas ir kūrimo komandų įvairove. Komisija gali sukurti iniciatyvas, įskaitant sektorines iniciatyvas, kad palengvintų techninių kliūčių, trukdančių tarpvalstybiniu lygmeniu keistis DI kūrimo duomenimis, sumažinimą, įskaitant kliūtis, susijusias su duomenimis apie galimybes pasinaudoti infrastruktūra, semantine ir technine įvairių rūšių duomenų sąveika;

(82) svarbu, kad DI sistemos, susijusios su gaminiais, kurie, remiantis šiuo reglamentu, nekelia didelės rizikos ir todėl neturi atitikti jame nustatytų reikalavimų, vis tiek būtų saugios jas pateikiant rinkai arba pradedant naudoti. Siekiant prisidėti prie šio tikslo, Europos Parlamento ir Tarybos direktyva 2001/95/EB[57] turėtų būti taikoma kaip saugumo sistema;

(83) siekdamos užtikrinti patikimą ir konstruktyvų kompetentingų institucijų bendradarbiavimą Sąjungos ir nacionaliniu lygmenimis, visos šalys, kurios dalyvauja

---

[56] 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

[57] 2001 m. gruodžio 3 d. Europos Parlamento ir Tarybos direktyva 2001/95/EB dėl bendros gaminių saugos (OL L 11, 2002 1 15, p. 4).

taikant šį reglamentą, turėtų užtikrinti informacijos ir duomenų, gautų vykdant savo užduotis, konfidencialumą;

(84) valstybės narės turėtų imtis visų reikiamų priemonių siekdamos užtikrinti, kad būtų įgyvendintos šio reglamento nuostatos, be kita ko, nustatydamos veiksmingas, proporcingas ir atgrasomas sankcijas už jų pažeidimą. Dėl tam tikrų konkrečių pažeidimų valstybės narės turėtų atsižvelgti į šiame reglamente nustatytas ribas ir kriterijus. Europos duomenų apsaugos priežiūros pareigūnas taip pat turėtų turėti įgaliojimus skirti baudas Sąjungos institucijoms, agentūroms ir įstaigoms, kurios patenka į šio reglamento taikymo sritį;

(85) siekiant užtikrinti, kad reglamentavimo sistemą prireikus būtų galima pritaikyti, įgaliojimai priimti aktus pagal SESV 290 straipsnį turėtų būti deleguoti Komisijai, kad ji galėtų iš dalies pakeisti I priede nurodytus metodus ir principus, siekiant apibrėžti DI sistemas, II priede išvardytus Sąjungos derinamuosius teisės aktus, III priede išvardytas didelės rizikos DI sistemas, IV priede išvardytas nuostatas dėl techninės dokumentacijos, V priedo pateiktos ES atitikties deklaracijos turinį, VI ir VII priedų nuostatas dėl atitikties vertinimo procedūrų ir nuostatas, kuriomis nustatomos didelės rizikos DI sistemos, kurioms turėtų būti taikoma atitikties vertinimo procedūra, pagrįsta kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat su ekspertais ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais[58]. Visų pirma siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(86) Siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011[59];

(87) kadangi šio reglamento tikslo valstybės narės negali deramai pasiekti, tačiau to tikslo dėl veiksmo masto ar poveikio būtų geriau siekti Sąjungos lygmeniu, pagal ES sutarties 5 straipsnyje nustatytą subsidiarumo principą Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti;

(88) šis reglamentas taikomas nuo … [*LB prašoma įrašyti 85 straipsnyje nurodytą datą*]. Tačiau valdymo struktūra ir atitikties vertinimo sistema turėtų veikti iki minėtos datos, todėl su notifikuotosiomis įstaigomis ir valdymo struktūra susijusios nuostatos turėtų būti taikomos nuo … [*LB prašoma įrašyti datą – trys mėnesiai nuo šio reglamento įsigaliojimo dienos*]. Be to, valstybės narės turėtų nustatyti ir pranešti Komisijai apie baudų, įskaitant administracines nuobaudas, taisykles ir užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendintos iki šio reglamento taikymo pradžios datos. Todėl nuostatos dėl baudų turėtų būti taikomos nuo [*LB prašoma įrašyti datą – dvylika mėnesių nuo šio reglamento įsigaliojimo dienos*];

---

58 OL L 123, 2016 5 12, p. 1.

59 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13).

(89) pagal Reglamento (ES) 2018/1725 42 straipsnio 2 dalį buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir Europos duomenų apsaugos valdyba ir jie pateikė nuomonę [...];

PRIĖMĖ ŠĮ REGLAMENTĄ:

I ANTRAŠTINĖ DALIS

BENDROSIOS NUOSTATOS

1 straipsnis
Dalykas

Šiuo reglamentu nustatoma:

(a) suderintos dirbtinio intelekto sistemų (toliau – DI sistemos) pateikimo rinkai, pradėjimo naudoti ir naudojimo Sąjungoje taisyklės;

(a) tam tikros su dirbtiniu intelektu susijusios praktikos draudimai;

(b) konkretūs didelės rizikos DI sistemoms taikomi reikalavimai ir su tokiomis sistemomis susijusios veiklos vykdytojų pareigos;

(c) suderintos skaidrumo taisyklės, taikomos DI sistemoms, skirtoms sąveikai su fiziniais asmenimis, emocijų atpažinimo sistemoms ir biometrinio kategorizavimo sistemoms, taip pat DI sistemoms, naudojamoms garso ar vaizdo turiniui generuoti ar juo manipuliuoti;

(d) rinkos stebėsenos ir priežiūros taisyklės.

2 straipsnis
Taikymo sritis

1. Šis reglamentas taikomas:

(a) tiekėjams, pateikiantiems rinkai arba pradedantiems naudoti Sąjungoje DI sistemas, nepriklausomai nuo to, ar tie tiekėjai įsisteigę Sąjungoje, ar trečiojoje valstybėje;

(b) Sąjungoje esantiems DI sistemų naudotojams;

(c) trečiojoje valstybėje esantiems DI sistemų, kurių sugeneruoti išvediniai naudojami Sąjungoje, tiekėjams ir naudotojams.

2. Didelės rizikos DI sistemoms taikomas tik šio reglamento 84 straipsnis, jei jos yra saugos komponentai gaminių arba sistemų arba pačios yra gaminiai ar sistemos, kuriems taikomi šie teisės aktai:

(a) Reglamentas (EB) Nr. 300/2008,

(b) Reglamentas (ES) Nr. 167/2013;

(c) Reglamentas (ES) Nr. 168/2013;

(d) Direktyva 2014/90/ES;

(e) Direktyva (ES) 2016/797;

(f) Reglamentas (ES) 2018/858;

(g) Reglamentas (ES) 2018/1139;

(h) Reglamentas (ES) 2019/2144.

3. Šis reglamentas netaikomas DI sistemoms, kurios sukurtos ar naudojamos tik karinėms reikmėms.

4. Šis reglamentas netaikomas trečiosios valstybės valdžios institucijoms ir tarptautinėms organizacijoms, kurios pagal 1 dalį patenka į šio reglamento taikymo sritį, kai tos institucijos ar organizacijos DI sistemas naudoja pagal tarptautinius susitarimus teisėsaugos ir teisminio bendradarbiavimo su Sąjunga arba su viena ar daugiau valstybių narių tikslais.

5. Šis reglamentas nedaro poveikio Europos Parlamento ir Tarybos direktyvos 2000/31/EB[60] II skyriaus IV skirsnio nuostatų dėl tarpinių paslaugų teikėjų atsakomybės [*jos bus pakeistos atitinkamomis Skaitmeninių paslaugų akto nuostatomis*] taikymui.

3 straipsnis
Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

(1) dirbtinio intelekto sistema (DI sistema) – programinė įranga, sukurta taikant vieną ar daugiau I priede išvardytų metodų ir principų ir gebanti pagal tam tikrus žmogaus nustatytus tikslus generuoti išvedinius, pavyzdžiui, turinį, predikcijas, rekomendacijas, arba sprendimus, turinčius įtakos aplinkai, su kuria ji sąveikauja;

(2) tiekėjas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kurie kuria arba užsako sukurti DI sistemą, siekdami už atlygį arba nemokamai pateikti ją rinkai arba pradėti naudoti savo vardu ar su savo prekių ženklu;

(3) smulkusis tiekėjas – tiekėjas, kuris yra labai maža arba mažoji įmonė, apibrėžta Komisijos rekomendacijoje 2003/361/EB[61];

(4) naudotojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita jų įgaliota įstaiga, naudojantys DI sistemą kitais nei asmeniniais neprofesinės veiklos tikslais;

(5) įgaliotasis atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, turintis raštišką DI sistemos tiekėjo įgaliojimą jo vardu vykdyti šiame reglamente nustatytas pareigas ir procedūras;

(6) importuotojas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, rinkai pateikiantis arba pradedantis naudoti DI sistemą, kurios pavadinimas arba prekių ženklas priklauso ne Sąjungoje įsisteigusiam fiziniam arba juridiniam asmeniui;

(7) platintojas – tiekimo grandinėje veikiantis fizinis arba juridinis asmuo (išskyrus tiekėją ir importuotoją), kuris tiekia DI sistemą Sąjungos rinkai nepakeisdamas jos savybių;

(8) veiklos vykdytojas – tiekėjas, naudotojas, įgaliotasis atstovas, importuotojas arba platintojas;

---

60 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) (OL L 178, 2000 7 17, p. 1).

61 2003 m. gegužės 6 d. Komisijos rekomendacija dėl labai mažų, mažųjų ir vidutinio dydžio įmonių apibrėžties (OL L 124, 2003 5 20, p. 36).

(9) pateikimas rinkai – DI sistemos tiekimas Sąjungos rinkai pirmą kartą;

(10) tiekimas rinkai – DI sistemos tiekimas už atlygį arba nemokamai siekiant ją platinti arba naudoti Sąjungos rinkoje vykdant komercinę veiklą;

(11) pradėjimas naudoti – tiesiogiai naudotojui arba savo reikmėms tiekiamos DI sistemos pirmasis panaudojimas Sąjungos rinkoje pagal numatytąją paskirtį;

(12) numatytoji paskirtis – tiekėjo numatyta DI sistemos paskirtis, įskaitant konkrečias naudojimo aplinkybes ir sąlygas, nurodyta informacijoje, kurią tiekėjas pateikė naudojimo instrukcijose, reklaminėje ar pardavimo medžiagoje bei teiginiuose ir techniniuose dokumentuose;

(13) pagrįstai numatomas netinkamas naudojimas – DI sistemos naudojimas ne pagal numatytąją paskirtį, kurį gali nulemti pagrįstai numatomas žmogaus elgesys ar sąveika su kitomis sistemomis;

(14) gaminio arba sistemos saugos komponentas – gaminio arba sistemos komponentas, kuris atlieka to gaminio ar sistemos saugos funkciją arba dėl kurio gedimo ar veikimo sutrikimo kyla rizika žmonių sveikatai ir saugai arba turtui;

(15) naudojimo instrukcija – informacija, kurią tiekėjas pateikia visų pirma siekdamas informuoti naudotoją apie numatytąją DI sistemos paskirtį bei tinkamą naudojimą, įskaitant informaciją apie konkrečią geografinę, elgsenos ar funkcinę aplinką, kurioje ketinama naudoti didelės rizikos DI sistemą;

(16) DI sistemos atšaukimas – priemonės, kuriomis siekiama, kad naudotojams jau pateikta DI sistema būtų grąžinta tiekėjui;

(17) DI sistemos pašalinimas – priemonės, kuriomis siekiama neleisti DI sistemos platinti, eksponuoti ir siūlyti;

(18) DI sistemos veikimas – DI sistemos gebėjimas veikti pagal numatytąją paskirtį;

(19) notifikuojančioji institucija – nacionalinė institucija, atsakinga už atitikties vertinimo įstaigoms vertinti, skirti ir notifikuoti būtinų procedūrų nustatymą bei vykdymą ir už tų įstaigų stebėseną;

(20) atitikties vertinimas – tikrinimo, ar įvykdyti šio reglamento III antraštinės dalies 2 skyriuje nustatyti DI sistemai taikytini reikalavimai, procesas;

(21) atitikties vertinimo įstaiga – įstaiga, kaip trečioji šalis vykdanti atitikties vertinimo veiklą, įskaitant bandymus, sertifikavimą ir tikrinimą;

(22) notifikuotoji įstaiga – atitikties vertinimo įstaiga, paskirta pagal šį reglamentą ir kitus atitinkamus Sąjungos derinamuosius teisės aktus;

(23) esminis pakeitimas – rinkai pateiktos arba pradėtos naudoti DI sistemos pakeitimas, kuris daro poveikį DI sistemos atitikčiai šio reglamento III antraštinės dalies 2 skyriuje nustatytiems reikalavimams arba dėl kurio pasikeičia numatytoji įvertintos DI sistemos paskirtis;

(24) CE atitikties ženklas (CE ženklas) – ženklas, kuriuo tiekėjas nurodo, kad DI sistema atitinka reikalavimus, nustatytus šio reglamento III antraštinės dalies 2 skyriuje ir kituose taikytinuose Sąjungos teisės aktuose, kuriais suderinamos prekybos šiuo ženklu ženklinamais gaminiais sąlygos (Sąjungos derinamuosiuose teisės aktuose);

(25) priežiūra po pateikimo rinkai – visa DI sistemų tiekėjų atliekama veikla, skirta rinkai pateiktų arba pradėtų naudoti DI sistemų naudojimo patirčiai aktyviai rinkti ir

peržiūrėti, siekiant nustatyti, ar yra poreikis nedelsiant imtis būtinų taisomųjų ar prevencinių veiksmų;

(26) rinkos priežiūros institucija – nacionalinė institucija, vykdanti veiklą ir taikanti priemones pagal Reglamentą (ES) 2019/1020;

(27) darnusis standartas – Europos standartas, apibrėžtas Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 dalies c punkte;

(28) bendrosios specifikacijos – dokumentas, kuris nėra standartas ir kuriame pateikiami techniniai sprendimai, kuriais užtikrinama, kad būtų laikomasi tam tikrų šiuo reglamentu nustatytų reikalavimų ir pareigų;

(29) mokymo duomenys – duomenys, naudojami DI sistemai mokyti pritaikant jos mokymosi parametrus, įskaitant neuroninio tinklo parametrus;

(30) validavimo duomenys – duomenys, naudojami išmokytai DI sistemai įvertinti ir jos kitiems nei mokymosi parametrams bei mokymosi procesui suderinti, be kita ko, siekiant išvengti persimokymo. Validavimo duomenų rinkinys gali būti atskiras duomenų rinkinys arba pastovi ar kintama mokymo duomenų rinkinio dalis;

(31) bandymo duomenys – duomenys, naudojami nepriklausomam išmokytos ir validuotos DI sistemos vertinimui atlikti siekiant patvirtinti numatomą tos sistemos veikimą prieš ją pateikiant rinkai arba pradedant naudoti;

(32) įvesties duomenys – DI sistemai teikiami arba jos tiesiogiai gaunami duomenys, kuriais remdamasi ji generuoja išvedinį;

(33) biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys;

(34) emocijų atpažinimo sistema – DI sistema, kurios paskirtis – atpažinti arba nuspėti fizinių asmenų emocijas ar ketinimus remiantis jų biometriniais duomenimis;

(35) biometrinio kategorizavimo sistema – DI sistema, kurios paskirtis – fizinius asmenis remiantis jų biometriniais duomenimis suskirstyti į tam tikras kategorijas, pvz., pagal lytį, amžių, plaukų spalvą, akių spalvą, tatuiruotes, etninę kilmę, lytinę orientaciją ar politines pažiūras;

(36) nuotolinio biometrinio tapatybės nustatymo sistema – DI sistema, kurios paskirtis – nuotoliniu būdu nustatyti fizinių asmenų tapatybę lyginant jų biometrinius duomenis su informacinėje duomenų bazėje esančiais biometriniais duomenimis, DI sistemos naudotojui iš anksto nežinant nei asmenų, kurių tapatybė bus nustatoma, nei to, ar jų tapatybė gali būti nustatyta;

(37) tikralaikio nuotolinio biometrinio tapatybės nustatymo sistema – nuotolinio biometrinio tapatybės nustatymo sistema, biometrinius duomenis fiksuojanti, lyginanti ir tapatybę nustatanti be didelės delsos. Kad būtų išvengta reikalavimų apėjimo, prie šių sistemų priskiriamos ne tik sistemos, gebančios tapatybę nustatyti akimirksniu, bet ir sistemos su tam tikra nedidele delsa;

(38) netikralaikio nuotolinio biometrinio tapatybės nustatymo sistema – kita nei tikralaikio nuotolinio biometrinio tapatybės nustatymo sistema;

(39) viešoji erdvė – vieša fizinė vieta, neatsižvelgiant į tai, ar taikomos tam tikros prieigos prie jos sąlygos;

(40) teisėsaugos institucija:

(a) valdžios institucija, kurios kompetencijai priklauso nusikalstamos veikos prevencija, tyrimas, atskleidimas ar baudžiamasis persekiojimas už ją arba bausmių vykdymas, be kita ko, apsauga nuo grėsmių visuomenės saugumui ir jų prevencija, arba

(b) kita įstaiga arba subjektas, kuriems pagal valstybės narės teisę pavesta vykdyti viešosios valdžios funkcijas ir naudotis viešaisiais įgaliojimais nusikalstamos veikos prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už ją arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais;

(41) teisėsauga – veikla, kurią teisėsaugos institucijos vykdo nusikalstamos veikos prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už ją arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais;

(42) nacionalinė priežiūros institucija – institucija, kurią valstybė narė paskiria atsakinga už šio reglamento įgyvendinimą ir taikymą, už tai valstybei narei pavestos veiklos koordinavimą, už vieno bendro ryšių su Komisija palaikymo punkto funkcijų vykdymą ir už valstybės narės atstovavimą Europos dirbtinio intelekto valdyboje;

(43) nacionalinė kompetentinga institucija – nacionalinė priežiūros institucija, notifikuojančioji institucija arba rinkos priežiūros institucija;

(44) didelis incidentas – incidentas, kuris tiesiogiai ar netiesiogiai nulemia, galėjo arba gali nulemti:

(a) asmens mirtį arba didelę žalą asmens sveikatai, turtui ar aplinkai,

(b) didelį ir negrįžtamą ypatingos svarbos infrastruktūros objektų valdymo ir eksploatavimo sutrikimą.

4 straipsnis
I priedo pakeitimai

Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais iš dalies keičiamas I priede pateiktas metodų ir principų sąrašas siekiant jį pritaikyti prie rinkos ir technologijų pokyčių remiantis charakteristikomis, kurios yra panašios į tame priede išvardytų metodų ir principų charakteristikas.

II ANTRAŠTINĖ DALIS

DRAUDŽIAMA SU DIRBTINIU INTELEKTU SUSIJUSI PRAKTIKA

5 straipsnis

1. Draudžiama taikyti šią su dirbtiniu intelektu susijusią praktiką:

(a) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kuria, pasitelkiant pasąmonę veikiančius metodus, kurių asmuo nesuvokia, jo elgesys iš esmės pakeičiamas taip, kad jis pats arba kitas asmuo patirtų fizinę ar psichologinę žalą arba būtų tikėtina, kad jis ar kitas asmuo tokią žalą patirs;

(b) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kuria, pasinaudojant konkrečios asmenų grupės pažeidžiamumu dėl jų amžiaus arba fizinės ar

protinės negalios, tai grupei priklausančio asmens elgesys iš esmės pakeičiamas taip, kad jis pats arba kitas asmuo patirtų fizinę ar psichologinę žalą arba būtų tikėtina, kad jis ar kitas asmuo tokią žalą patirs;

(c) valdžios institucijoms arba jų vardu pateikti rinkai, pradėti naudoti arba naudoti DI sistemas fizinių asmenų patikimumui tam tikru laikotarpiu vertinti ar klasifikuoti pagal jų socialinę elgseną arba žinomus ar nuspėjamus asmeninius ar asmenybės bruožus, jei socialinis reitingas lemia vieną arba abu toliau išvardytus dalykus:

i) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar tokių asmenų grupėmis socialinėmis aplinkybėmis, kurios nėra panašios į aplinkybes, kuriomis duomenys buvo iš pradžių generuojami ar renkami;

ii) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar tokių asmenų grupėmis, kuris yra nepagrįstas arba neproporcingas jų socialinei elgsenai ar jos svarbumui;

(d) viešosiose erdvėse teisėsaugos tikslais naudoti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas, išskyrus tuo atveju, kai tikrai būtina, siekiant vieno iš šių tikslų:

i) vykdant tikslinę konkrečių galimų nusikaltimo aukų, įskaitant dingusius vaikus, paiešką;

ii) siekiant išvengti konkrečios didelės artėjančios grėsmės fizinių asmenų gyvybei ar fizinei saugai arba teroristinio išpuolio;

iii) siekiant išaiškinti asmenis, padariusius Tarybos pagrindų sprendimo 2002/584/TVR[62] 2 straipsnio 2 dalyje nurodytą nusikalstamą veiką, už kurią atitinkamoje valstybėje narėje jos teisėje nustatyta tvarka baudžiama laisvės atėmimo bausme arba įkalinimu, kurio ilgiausias terminas – bent treji metai, arba asmenis, įtariamus tokios veikos padarymu, nustatyti jų buvimo vietą ar tapatybę arba patraukti juos baudžiamojon atsakomybėn.

2. Kai tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos viešosiose erdvėse teisėsaugos tikslais naudojamos siekiant kurio nors iš 1 dalies d punkte nurodytų tikslų, atsižvelgiama į šiuos aspektus:

(a) padėties, dėl kurios gali tekti pasinaudoti tokia sistema, pobūdį, visų pirma žalos, kuri būtų padaryta nenaudojant tokios sistemos, dydį, tikimybę ir mastą;

(b) sistemos naudojimo pasekmes, susijusias su visų atitinkamų asmenų teisėmis ir laisvėmis, visų pirma tų pasekmių rimtumą, tikimybę ir mastą.

Be to, kai tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos viešosiose erdvėse teisėsaugos tikslais naudojamos siekiant kurio nors iš 1 dalies d punkte nurodytų tikslų, taikomos būtinos ir proporcingos su jų naudojimu susijusios apsaugos priemonės ir sąlygos, visų pirma laiko, geografiniai ir su asmenimis susiję apribojimai.

[62] 2002 m. birželio 13 d. Tarybos pagrindų sprendimas 2002/584/TVR dėl Europos arešto orderio ir perdavimo tarp valstybių narių tvarkos (OL L 190, 2002 7 18, p. 1).

3. Taikant 1 dalies d punktą ir 2 dalį, tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą naudoti viešosiose erdvėse teisėsaugos tikslais galima tik kiekvienu atskiru atveju gavus išankstinį valstybės narės, kurioje tą sistemą ketinama naudoti, teisminės institucijos arba nepriklausomos administracinės institucijos leidimą, išduotą pagal pagrįstą prašymą ir 4 dalyje nurodytas išsamias nacionalinės teisės taisykles. Tačiau tinkamai pagrįstais skubos atvejais sistemą galima pradėti naudoti be leidimo, o leidimo prašyti tik naudojant sistemą arba baigus ją naudoti.

   Kompetentinga teisminė arba administracinė institucija išduoda leidimą tik tuo atveju, jei, remdamasi jai pateiktais objektyviais duomenimis arba akivaizdžiais įrodymais, įsitikina, kad atitinkamos tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos naudojimas yra būtinas ir proporcingas siekiant prašyme nurodyto kurio nors iš 1 dalies d punkte nustatytų tikslų. Priimdama sprendimą dėl prašymo, kompetentinga teisminė arba administracinė institucija atsižvelgia į 2 dalyje nurodytus elementus.

4. Valstybė narė gali nuspręsti numatyti galimybę suteikti visišką arba dalinį leidimą tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas naudoti viešosiose erdvėse teisėsaugos tikslais, laikantis 1 dalies d punkte ir 2 bei 3 dalyse nurodytų apribojimų ir sąlygų. Ta valstybė narė savo nacionalinėje teisėje nustato būtinas išsamias taisykles, kuriomis reglamentuojama 3 dalyje nurodytų leidimų prašymo, išdavimo, vykdymo ir su jais susijusios priežiūros tvarka. Tose taisyklėse taip pat nurodoma, kurių iš 1 dalies d punkte išvardytų ir su kuria to punkto iii papunktyje nurodyta nusikalstama veika susijusių tikslų kompetentingoms institucijoms gali būti leidžiama siekti naudojant tas sistemas teisėsaugos tikslais.

III ANTRAŠTINĖ DALIS

DIDELĖS RIZIKOS DI SISTEMOS

1 SKYRIUS

DI SISTEMŲ PRISKYRIMAS DIDELĖS RIZIKOS SISTEMŲ KATEGORIJAI

6 straipsnis

DI sistemų priskyrimo didelės rizikos sistemų kategorijai taisyklės

1. Nepriklausomai nuo to, ar DI sistema pateikiama rinkai ar pradedama naudoti atskirai nuo a ir b punktuose nurodytų gaminių, ta DI sistema laikoma didelės rizikos sistema, jei tenkinamos abi šios sąlygos:

   (a) DI sistema yra skirta naudoti kaip gaminio, kuriam taikomi II priede išvardyti Sąjungos derinamieji teisės aktai, saugos komponentas arba pati yra toks gaminys;

   (b) reikalaujama, kad gaminio, kurio saugos komponentas yra DI sistema, arba pačios DI sistemos kaip gaminio atitikties vertinimą, kurio reikia, kad tą gaminį būtų galima pateikti rinkai arba pradėti naudoti, atliktų trečioji šalis pagal II priede išvardytus Sąjungos derinamuosius teisės aktus.

2. Be nurodytųjų 1 dalyje, didelės rizikos DI sistemomis taip pat laikomos III priede nurodytos DI sistemos.

7 straipsnis
III priedo pakeitimai

1. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais III priede pateiktas sąrašas atnaujinamas įtraukiant didelės rizikos DI sistemas, kurios atitinka abi šias sąlygas:

   (a) DI sistemos yra skirtos naudoti bet kurioje iš III priedo 1–8 punktuose išvardytų sričių;

   (b) DI sistemos kelia žalos sveikatai ir saugai arba neigiamo poveikio pagrindinėms teisėms riziką, kuri, atsižvelgiant į jos dydį ir tikimybę, yra lygiavertė III priede jau nurodytų didelės rizikos DI sistemų keliamai žalos ar neigiamo poveikio rizikai arba yra už ją didesnė.

2. 1 dalies taikymo tikslais vertindama, ar DI sistemos keliama žalos sveikatai ir saugai arba neigiamo poveikio pagrindinėms teisėms rizika yra lygiavertė III priede jau nurodytų didelės rizikos DI sistemų keliamai žalos rizikai arba yra už ją didesnė, Komisija atsižvelgia į šiuos kriterijus:

   (a) numatytąją DI sistemos paskirtį;

   (b) kokiu mastu DI sistema buvo arba, tikėtina, bus naudojama;

   (c) kokiu mastu DI sistemos naudojimas jau padarė žalą sveikatai ir saugai arba neigiamą poveikį pagrindinėms teisėms arba sukėlė didelį susirūpinimą dėl tokios žalos ar neigiamo poveikio padarymo, kaip matyti iš nacionalinėms kompetentingoms institucijoms pateiktų pranešimų arba dokumentais pagrįstų įtarimų;

   (d) galimą tokios žalos arba tokio neigiamo poveikio mastą, visų pirma atsižvelgiant į jų dydį ir galėjimą paveikti daugelį asmenų;

   (e) kiek asmenys, kuriems gali būti padaryta žala arba neigiamas poveikis, priklauso nuo DI sistemos padarinių, visų pirma todėl, kad dėl praktinių ar teisinių priežasčių pagrįstai neįmanoma tų padarinių išvengti;

   (f) kiek asmenys, kuriems gali būti padaryta žala arba neigiamas poveikis, yra pažeidžiami DI sistemos naudotojo atžvilgiu, visų pirma dėl galios, žinių, ekonominių ar socialinių aplinkybių arba amžiaus disbalanso;

   (g) kaip lengvai DI sistemos padarinius galima ištaisyti (padariniai, darantys poveikį žmonių sveikatai ar saugai, nelaikomi lengvai ištaisomais);

   (h) kiek galiojančiuose Sąjungos teisės aktuose numatyta:

      i) veiksmingų teisių gynimo priemonių, susijusių su DI sistemos keliama rizika, išskyrus reikalavimus atlyginti žalą;

      ii) veiksmingų priemonių, kuriomis galima išvengti tokios rizikos arba ją iš esmės sumažinti.

2 SKYRIUS

DIDELĖS RIZIKOS DI SISTEMOMS TAIKOMI REIKALAVIMAI

8 straipsnis
Atitiktis reikalavimams

1. Didelės rizikos DI sistemos turi atitikti šiame skyriuje nustatytus reikalavimus.

2. Užtikrinant atitiktį tiems reikalavimams atsižvelgiama į didelės rizikos DI sistemos ir 9 straipsnyje nurodytos rizikos valdymo sistemos numatytąją paskirtį.

9 straipsnis
Rizikos valdymo sistema

1. Turi būti sukurta, įgyvendinta, dokumentuojama ir prižiūrima didelės rizikos DI sistemų keliamos rizikos valdymo sistema.

2. Rizikos valdymo sistema yra per visą didelės rizikos DI sistemos gyvavimo ciklą vykstantis nuolatinis kartotinis procesas, kurį reikia reguliariai sistemingai atnaujinti. Ją sudaro šie etapai:

   (a) kiekvienos didelės rizikos DI sistemos keliamos žinomos ir numatomos rizikos nustatymas ir analizė;

   (b) rizikos, kuri gali kilti didelės rizikos DI sistemą naudojant pagal numatytąją paskirtį ir pagrįstai numatomo netinkamo naudojimo sąlygomis, nustatymas ir vertinimas;

   (c) kitos galinčios kilti rizikos vertinimas remiantis duomenų, surinktų taikant 61 straipsnyje nurodytą priežiūros po pateikimo rinkai sistemą, analize;

   (d) tinkamų rizikos valdymo priemonių priėmimas pagal tolesnių dalių nuostatas.

3. Priimant 2 dalies d punkte nurodytas rizikos valdymo priemones deramai atsižvelgiama į poveikį ir galimą sąveiką, kuriuos lemia bendras šiame 2 skyriuje nustatytų reikalavimų taikymas. Jas priimant atsižvelgiama ir į visuotinai pripažintus pažangiausius metodus, be kita ko, nurodytus atitinkamuose darniuosiuose standartuose arba bendrosiose specifikacijose.

4. 2 dalies d punkte nurodytos rizikos valdymo priemonės turi būti tokios, kad su kiekvienu pavojumi susijusi liekamoji rizika ir bendra didelės rizikos DI sistemų liekamoji rizika būtų laikoma priimtina, jeigu didelės rizikos DI sistema naudojama pagal numatytąją paskirtį arba pagrįstai numatomo netinkamo naudojimo sąlygomis. Apie tą liekamąją riziką pranešama naudotojui.

   Nustatant tinkamiausias rizikos valdymo priemones, užtikrinama, kad:

   (a) rizika būtų pašalinta arba kuo labiau sumažinta tinkamomis projektavimo ir kūrimo priemonėmis;

   (b) jei rizikos pašalinti neįmanoma, prireikus būtų įgyvendintos tinkamos rizikos mažinimo ir kontrolės priemonės;

   (c) pagal 13 straipsnį būtų teikiama tinkama informacija, visų pirma apie šio straipsnio 2 dalies b punkte nurodytą riziką, ir prireikus naudotojams būtų rengiami mokymai.

Šalinant arba mažinant didelės rizikos DI sistemos naudojimo keliamą riziką turi būti tinkamai atsižvelgiama į technines žinias, patirtį, išsilavinimą ir mokymą, kurių tikimasi iš naudotojo, ir į aplinką, kurioje sistemą ketinama naudoti.

5. Siekiant nustatyti tinkamiausias rizikos valdymo priemones, didelės rizikos DI sistemos išbandomos. Bandymais užtikrinama, kad didelės rizikos DI sistemos visą laiką veiktų pagal numatytąją paskirtį ir atitiktų šiame skyriuje nustatytus reikalavimus.

6. Bandymų procedūros turi būti tinkamos užtikrinti, kad DI sistema veiktų pagal numatytąją paskirtį, ir neviršyti to, kas būtina tam tikslui pasiekti.

7. Prireikus didelės rizikos DI sistemų bandymai atliekami bet kuriuo jų kūrimo proceso etapu ir bet kuriuo atveju prieš jas pateikiant rinkai arba pradedant naudoti. Bandymai atliekami taikant preliminariai nustatytus parametrus ir tikimybines ribines vertes, atitinkančius didelės rizikos DI sistemos numatytąją paskirtį.

8. Įgyvendinant 1–7 dalyse aprašytą rizikos valdymo sistemą, ypatingas dėmesys skiriamas tam, ar didelės rizikos DI sistema gali būti prieinama vaikams arba daryti jiems poveikį.

9. 1–8 dalyse aprašyti aspektai įtraukiami į kredito įstaigų, kurių veikla reglamentuojama Direktyva 2013/36/ES, pagal tos direktyvos 74 straipsnį nustatytas rizikos valdymo procedūras.

10 straipsnis
Duomenys ir jų valdymas

1. Didelės rizikos DI sistemos, kuriose naudojami metodai, pagal kuriuos modeliai mokomi pasitelkiant duomenis, kuriamos remiantis mokymo, validavimo ir bandymo duomenų rinkiniais, atitinkančiais 2–5 dalyse nurodytus kokybės kriterijus.

2. Mokymo, validavimo ir bandymo duomenų rinkiniams taikoma atitinkama duomenų valdymo ir tvarkymo praktika. Ta praktika visų pirma susijusi su:

   (a) atitinkamais projektavimo sprendimais;

   (b) duomenų rinkimu;

   (c) atitinkamomis paruošiamosiomis duomenų tvarkymo operacijomis, pvz., anotavimu, žymėjimu, valymu, papildymu ir agregavimu;

   (d) atitinkamų prielaidų, visų pirma susijusių su informacija, kuri turėtų būti išreikšta ir perteikta duomenimis, formulavimu;

   (e) išankstiniu reikiamų duomenų rinkinių prieinamumo, kiekio ir tinkamumo vertinimu;

   (f) nagrinėjimu atsižvelgiant į galimą šališkumą;

   (g) galimų duomenų spragų ar trūkumų ir galimų jų šalinimo būdų nustatymu.

3. Mokymo, validavimo ir bandymo duomenų rinkiniai turi būti tinkami, reprezentatyvūs, be klaidų ir išsamūs. Jie turi turėti tinkamas statistines savybes, įskaitant, kai taikoma, susijusias su asmenimis ar asmenų grupėmis, kurių atžvilgiu ketinama naudoti didelės rizikos DI sistemą. Šias charakteristikas gali turėti atskiri duomenų rinkiniai arba jų derinys.

4. Kiek to reikia atsižvelgiant į numatytąją paskirtį, mokymo, validavimo ir bandymo duomenų rinkiniai turi būti grindžiami charakteristikomis ar elementais, būdingais konkrečiai geografinei, elgsenos ar funkcinei aplinkai, kurioje didelės rizikos DI sistemą ketinama naudoti.

5. Didelės rizikos DI sistemų tiekėjai, kiek tai tikrai būtina siekiant užtikrinti tų sistemų šališkumo stebėseną, aptikimą ir ištaisymą, gali tvarkyti specialių kategorijų asmens duomenis, nurodytus Reglamento (ES) 2016/679 9 straipsnio 1 dalyje, Direktyvos (ES) 2016/680 10 straipsnyje ir Reglamento (ES) 2018/1725 10 straipsnio 1 dalyje, taikydami tinkamas fizinių asmenų pagrindinių teisių ir laisvių apsaugos priemones, įskaitant pažangiausių saugumo ir privatumo užtikrinimo priemonių, pvz., pseudoniminimo arba šifravimo, kai anoniminimas gali labai pakenkti siekiamam tikslui, naudojimo ir pakartotinio naudojimo techninius apribojimus.

6. Kuriant didelės rizikos DI sistemas (išskyrus sistemas, kuriose naudojami modelių mokymo metodai) taikoma tinkama duomenų valdymo ir tvarkymo praktika, siekiant užtikrinti, kad tos didelės rizikos DI sistemos atitiktų 2 dalies reikalavimus.

11 straipsnis
Techniniai dokumentai

1. Didelės rizikos DI sistemos techniniai dokumentai parengiami prieš tą sistemą pateikiant rinkai arba pradedant ją naudoti ir nuolat atnaujinami.

   Techniniai dokumentai parengiami taip, kad jais būtų galima įrodyti, jog didelės rizikos DI sistema atitinka šiame skyriuje nustatytus reikalavimus, ir nacionalinėms kompetentingoms institucijoms bei notifikuotosioms įstaigoms juose būtų pateikta visa informacija, būtina DI sistemos atitikčiai tiems reikalavimams įvertinti. Tuos dokumentus turi sudaryti bent IV priede nustatyti elementai.

2. Kai rinkai pateikiama arba pradedama naudoti su gaminiu, kuriam taikomi II priedo A skirsnyje išvardyti teisės aktai, susijusi didelės rizikos DI sistema, parengiamas vienas bendras techninis dokumentas, kuriame pateikiama visa IV priede nustatyta informacija ir pagal tuos teisės aktus reikalaujama informacija.

3. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais prireikus iš dalies keičiamas IV priedas siekiant užtikrinti, kad, atsižvelgiant į technikos pažangą, techniniuose dokumentuose būtų pateikta visa informacija, būtina sistemos atitikčiai šiame skyriuje nustatytiems reikalavimams įvertinti.

12 straipsnis
Registravimas

1. Didelės rizikos DI sistemos projektuojamos ir kuriamos taip, kad joms veikiant įvykiai būtų registruojami automatiškai (žurnaluose). Tie registravimo pajėgumai turi atitikti pripažintus standartus arba bendrąsias specifikacijas.

2. Registravimo pajėgumais turi būti užtikrinamas tam tikras DI sistemos veikimo per visą jos gyvavimo ciklą atsekamumo lygis, atitinkantis numatytąją sistemos paskirtį.

3. Registravimo pajėgumais visų pirma turi būti sudarytos sąlygos stebėti didelės rizikos DI sistemos veikimą, susijusį su situacijomis, kuriose ta sistema gali kelti 65 straipsnio 1 dalyje apibrėžtą riziką arba dėl kurių gali prireikti atlikti esminį pakeitimą, ir palengvinti 61 straipsnyje nurodytą priežiūrą po pateikimo rinkai.

4. III priedo 1 dalies a punkte nurodyti didelės rizikos DI sistemų registravimo pajėgumai apima bent:

(a) kiekvieno sistemos naudojimo laikotarpio (kiekvieno naudojimo pradžios datos ir laiko, taip pat pabaigos datos ir laiko) registravimą;

(b) informacinę duomenų bazę, su kurios duomenimis sistema sutikrino įvesties duomenis;

(c) įvesties duomenis, kurių atitikmenys rasti atlikus paiešką;

(d) 14 straipsnio 5 dalyje nurodytų fizinių asmenų, dalyvaujančių tikrinant rezultatus, tapatybės duomenis.

13 straipsnis
Skaidrumas ir informacijos teikimas naudotojams

1. Projektuojant ir kuriant didelės rizikos DI sistemas užtikrinama, kad jos veiktų pakankamai skaidriai, kad naudotojai galėtų tinkamai interpretuoti ir naudoti sistemos išvedinius. Turi būti užtikrintas atitinkamos rūšies ir lygio skaidrumas, kad naudotojai ir tiekėjai galėtų įvykdyti atitinkamas šios antraštinės dalies 3 skyriuje nustatytas pareigas.

2. Su didelės rizikos DI sistemomis pateikiamos tinkamo skaitmeninio arba kitokio formato naudojimo instrukcijos, kuriose pateikiama glausta, išsami, teisinga ir aiški naudotojams svarbi, prieinama ir suprantama informacija.

3. 2 dalyje nurodyta informacija apima:

(a) tiekėjo ir, jei taikoma, jo įgaliotojo atstovo tapatybę ir kontaktinius duomenis;

(b) didelės rizikos DI sistemos charakteristikas, pajėgumus ir veikimo apribojimus, įskaitant:

i) jos numatytąją paskirtį;

ii) 15 straipsnyje nurodytą didelės rizikos DI sistemos tikslumo, patikimumo ir kibernetinio saugumo lygį, kuris buvo išbandytas ir validuotas ir kurio galima tikėtis, taip pat visas žinomas ir numatomas aplinkybes, galinčias daryti poveikį numatomam tikslumo, patvarumo ir kibernetinio saugumo lygiui;

iii) visas žinomas ir numatomas aplinkybes, susijusias su didelės rizikos DI sistemos naudojimu pagal numatytąją paskirtį arba pagrįstai numatomo netinkamo naudojimo sąlygomis, dėl kurio gali kilti rizika sveikatai ir saugai arba pagrindinėms teisėms;

iv) jos veikimą, susijusį su asmenimis ar asmenų grupėmis, kurių atžvilgiu ją ketinama naudoti;

v) kai tinkama, įvesties duomenų specifikacijas arba visą kitą svarbią informaciją, susijusią su naudojamais mokymo, validavimo ir bandymo duomenų rinkiniais, atsižvelgiant į numatytąją DI sistemos paskirtį;

(c) didelės rizikos DI sistemos ir jos veikimo, kurį tiekėjas iš anksto nustatė per pirminį atitikties vertinimą, pokyčius, jei taikoma;

(d) 14 straipsnyje nurodytas žmogaus vykdomos priežiūros priemones, įskaitant technines priemones, įdiegtas tam, kad naudotojams būtų lengviau interpretuoti DI sistemų išvedinius;

(e) numatomą didelės rizikos DI sistemos gyvavimo laiką ir visas techninės ir kitos priežiūros priemones, būtinas tinkamam tos DI sistemos veikimui užtikrinti, įskaitant programinės įrangos atnaujinimą.

14 straipsnis
Žmogaus vykdoma priežiūra

1. Didelės rizikos DI sistemos projektuojamos ir kuriamos taip (įskaitant tinkamas žmogaus ir mašinos sąsajos priemones), kad tuo metu, kai tos DI sistemos naudojamos, jas galėtų veiksmingai prižiūrėti fiziniai asmenys.

2. Žmogaus vykdoma priežiūra turi būti siekiama išvengti rizikos sveikatai, saugai ar pagrindinėms teisėms, kuri gali kilti didelės rizikos DI sistemą naudojant pagal numatytąją paskirtį arba pagrįstai numatomo netinkamo naudojimo sąlygomis, arba tą riziką kuo labiau sumažinti, visų pirma tais atvejais, kai ji išlieka nepaisant kitų šiame skyriuje nustatytų reikalavimų taikymo.

3. Žmogaus vykdoma priežiūra užtikrinama viena arba visomis šiomis priemonėmis:

(a) priemonėmis, kurias tiekėjas nustatė ir, kai techniškai įmanoma, įdiegė į didelės rizikos DI sistemą prieš ją pateikdamas rinkai arba pradėdamas naudoti;

(b) priemonėmis, kurias tiekėjas nustatė prieš didelės rizikos DI sistemą pateikdamas rinkai arba pradėdamas ją naudoti ir kurios yra tinkamos naudotojui įgyvendinti.

4. Asmenims, kuriems pavesta vykdyti tokią priežiūrą, 3 dalyje nurodytomis priemonėmis turi būti sudarytos sąlygos, jei tai tinkama pagal aplinkybes:

(a) visiškai suprasti didelės rizikos DI sistemos pajėgumus ir apribojimus ir sugebėti tinkamai stebėti jos veikimą, kad būtų galima kuo greičiau aptikti ir pašalinti anomalijų, sutrikimų ir netikėto veikimo apraiškas;

(b) nepamiršti galimos tendencijos automatiškai arba pernelyg pasikliauti didelės rizikos DI sistemos išvediniais (automatiško šališkumo), visų pirma tais atvejais, kai didelės rizikos DI sistemos naudojamos informacijai arba rekomendacijoms, kuriomis remdamiesi fiziniai asmenys turi priimti sprendimus, teikti;

(c) sugebėti teisingai interpretuoti didelės rizikos DI sistemos išvedinius, visų pirma atsižvelgiant į sistemos charakteristikas ir turimas interpretavimo priemones bei metodus;

(d) gebėti nuspręsti nenaudoti didelės rizikos DI sistemos tam tikroje situacijoje arba kitaip nepaisyti tos sistemos išvedinių, juos panaikinti ar ištaisyti;

(e) sugebėti įsikišti į didelės rizikos DI sistemos veikimą arba sistemą išjungti tam skirtu mygtuku ar panašiu būdu.

5. III priedo 1 punkto a papunktyje nurodytoms didelės rizikos DI sistemoms taikomomis 3 dalyje nurodytomis priemonėmis turi būti užtikrinta, kad, be minėtų dalykų, naudotojas nesiimtų jokių veiksmų ir nepriimtų sprendimų remdamasis sistemos pateiktu identifikavimo rezultatu, išskyrus tuo atveju, jei jį patikrino ir patvirtino bent du fiziniai asmenys.

15 straipsnis
Tikslumas, patikimumas ir kibernetinis saugumas

1. Didelės rizikos DI sistemos projektuojamos ir kuriamos taip, kad atsižvelgiant į numatytąją jų paskirtį būtų pasiektas tinkamas tikslumo, patvarumo ir kibernetinio saugumo lygis ir kad šiuo atžvilgiu tos sistemos veiktų nuosekliai per visą jų gyvavimo ciklą.

2. Didelės rizikos DI sistemų tikslumo lygiai ir atitinkami tikslumo parametrai nurodomi pridedamose naudojimo instrukcijose.

3. Didelės rizikos DI sistemos turi būti atsparios klaidoms, triktims ar nesuderinamumo atvejams, kurių gali atsirasti sistemoje arba jos veikimo aplinkoje, visų pirma dėl sistemos sąveikos su fiziniais asmenimis ar kitomis sistemomis.

4. Didelės rizikos DI sistemų patikimumą galima užtikrinti techniniais perteklumo sprendimais, kurie gali apimti atsarginio kopijavimo arba veikimo be gedimų planus.

5. Kuriant didelės rizikos DI sistemas, kurios pateiktos rinkai arba pradėtos naudoti toliau mokosi, turi būti užtikrinama, kad išvediniams, kurie gali būti šališki dėl to, kad yra naudojami kaip būsimų operacijų įvediniai (grįžtamojo ryšio grandinės), būtų deramai taikomos tinkamos rizikos mažinimo priemonės.

6. Didelės rizikos DI sistemos turi būti atsparios leidimo neturinčių trečiųjų šalių bandymams pakeisti jų naudojimo paskirtį ar veikimą pasinaudojant sistemų pažeidžiamumu.

   Techniniai sprendimai, kuriais siekiama užtikrinti didelės rizikos DI sistemų kibernetinį saugumą, turi atitikti konkrečias aplinkybes ir riziką.

   Techniniai DI būdingų pažeidžiamumo problemų sprendimai, kai tinkama, turi apimti priemones, padedančias išvengti išpuolių, kuriais bandoma manipuliuoti mokymo duomenų rinkiniu (klaidingų duomenų įrašymo), įvedinių, kurių paskirtis – priversti modelį padaryti klaidą (priešiškų pavyzdžių), arba modelių trūkumų ir juos kontroliuoti.

3 SKYRIUS

DIDELĖS RIZIKOS DI SISTEMŲ TIEKĖJŲ BEI NAUDOTOJŲ IR KITŲ ŠALIŲ PAREIGOS

16 straipsnis
Didelės rizikos DI sistemų tiekėjų pareigos

Didelės rizikos DI sistemų tiekėjai:

(a) užtikrina, kad jų didelės rizikos DI sistemos atitiktų šios antraštinės dalies 2 skyriuje nustatytus reikalavimus;

(b) įdiegia 17 straipsnio reikalavimus atitinkančią kokybės valdymo sistemą;

(c) parengia didelės rizikos DI sistemos techninius dokumentus;

(d) saugo savo didelės rizikos DI sistemų automatiškai generuojamus žurnalus, jei tik tie žurnalai yra jų žinioje;

(e) užtikrina, kad prieš pateikiant rinkai arba pradedant naudoti didelės rizikos DI sistemą būtų atliekama atitinkama jos atitikties vertinimo procedūra;

(f) laikosi 51 straipsnyje nustatytos pareigos įregistruoti sistemą;

(g) jei didelės rizikos DI sistema neatitinka šios antraštinės dalies 2 skyriuje nustatytų reikalavimų, imasi būtinų taisomųjų veiksmų;

(h) apie neatitiktį ir taisomuosius veiksmus, kurių buvo imtasi, informuoja valstybių narių, kuriose jie tiekė DI sistemą arba pradėjo ją naudoti, nacionalines kompetentingas institucijas ir, kai taikoma, notifikuotąją įstaigą;

(i) siekdami įrodyti, kad jų didelės rizikos DI sistemos atitinka šio reglamento reikalavimus, jie jas paženklina CE ženklu pagal 49 straipsnį;

(j) nacionalinės kompetentingos institucijos prašymu įrodo, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus.

17 straipsnis
Kokybės valdymo sistema

1. Didelės rizikos DI sistemų tiekėjai įdiegia kokybės valdymo sistemą, kuria užtikrinama atitiktis šiam reglamentui. Ta sistema sistemingai ir tvarkingai įtvirtinama rašytinės politikos, procedūrų ir nurodymų dokumentuose ir apima bent šiuos aspektus:

   (a) atitikties reglamentuojamiems reikalavimams strategiją, apimančią atitikties vertinimo procedūrų ir didelės rizikos DI sistemos pakeitimų valdymo procedūrų laikymąsi;

   (b) metodus, procedūras ir sistemingus veiksmus, taikytinus projektuojant didelės rizikos DI sistemą, vykdant jos projekto kontrolę ir tikrinimą;

   (c) metodus, procedūras ir sistemingus veiksmus, taikytinus kuriant didelės rizikos DI sistemą, vykdant jos kokybės kontrolę ir užtikrinant jos kokybę;

   (d) tikrinimo, bandymo ir validavimo procedūras, atliktinas prieš kuriant didelės rizikos DI sistemą, jos kūrimo metu ir ją sukūrus, ir jų atlikimo dažnumą;

   (e) taikytinas technines specifikacijas, įskaitant standartus, ir, jei atitinkami darnieji standartai taikomi ne visa apimtimi, priemones, naudotinas siekiant užtikrinti, kad didelės rizikos DI sistema atitiktų šios antraštinės dalies 2 skyriuje nustatytus reikalavimus;

   (f) duomenų tvarkymo sistemas ir procedūras, įskaitant duomenų rinkimo, duomenų analizės, duomenų žymėjimo, duomenų laikymo, duomenų filtravimo, duomenų gavybos, duomenų apibendrinimo, duomenų saugojimo ir bet kokią kitą su duomenimis susijusią veiklą, kuri atliekama prieš didelės rizikos DI sistemą pateikiant rinkai arba pradedant naudoti ir kuri atliekama tuo tikslu;

   (g) 9 straipsnyje nurodytą rizikos valdymo sistemą;

   (h) priežiūros po pateikimo rinkai sistemos nustatymą, įgyvendinimą ir priežiūrą pagal 61 straipsnį;

   (i) pranešimo apie didelius incidentus ir veikimo sutrikimus pagal 62 straipsnį procedūras;

   (j) ryšių su nacionalinėmis ir kitomis kompetentingomis institucijomis, įskaitant sektorių kompetentingas institucijas, teikiančiomis arba palaikančiomis prieigą

prie duomenų, notifikuotosiomis įstaigomis, kitais veiklos vykdytojais, klientais ar kitais suinteresuotaisiais subjektais palaikymą;

(k) visų svarbių dokumentų ir informacijos registravimo sistemas ir procedūras;

(l) išteklių valdymą, įskaitant su tiekimo saugumu susijusias priemones;

(m) atskaitomybės sistemą, kurioje nustatyta vadovybės ir kitų darbuotojų atsakomybė, apimanti visus šioje dalyje išvardytus aspektus.

2. 1 dalyje nurodyti aspektai įgyvendinami proporcingai tiekėjo organizacijos dydžiui.

3. Jei tiekėjai yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, pareiga įdiegti kokybės valdymo sistemą laikoma įvykdyta, jei laikomasi tos direktyvos 74 straipsnyje nustatytų taisyklių dėl vidaus valdymo priemonių, procesų ir mechanizmų. Tuo atveju atsižvelgiama į visus šio reglamento 40 straipsnyje nurodytus darniuosius standartus.

18 straipsnis
Pareiga parengti techninius dokumentus

1. Didelės rizikos DI sistemų tiekėjai pagal IV priedą parengia 11 straipsnyje nurodytus techninius dokumentus.

2. Tiekėjai, kurie yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, techninius dokumentus saugo kartu su dokumentais, susijusiais su tos direktyvos 74 straipsnyje nurodytomis vidaus valdymo priemonėmis, procesais ir mechanizmais.

19 straipsnis
Atitikties vertinimas

1. Didelės rizikos DI sistemų tiekėjai užtikrina, kad prieš tas sistemas pateikiant rinkai arba pradedant naudoti būtų pagal 43 straipsnį atliekama atitinkama jų atitikties vertinimo procedūra. Jeigu atlikus tą atitikties vertinimą nustatoma, kad DI sistemos atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, tiekėjai parengia ES atitikties deklaraciją pagal 48 straipsnį ir pažymi sistemą CE atitikties ženklu pagal 49 straipsnį.

2. Jei III priedo 5 punkto b papunktyje nurodytas didelės rizikos DI sistemas rinkai pateikia arba pradeda naudoti tiekėjai, kurie yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, atitikties vertinimas atliekamas vykdant tos direktyvos 97–101 straipsniuose nurodytą procedūrą.

20 straipsnis
Automatiškai generuojami žurnalai

1. Didelės rizikos DI sistemų tiekėjai saugo savo sistemų automatiškai generuojamus žurnalus, jei tik tokie žurnalai yra jų žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus. Žurnalų saugojimo laikotarpis turi būti tinkamas atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį ir į pagal Sąjungos ar nacionalinę teisę taikomas teisines pareigas.

2. Tiekėjai, kurie yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, savo didelės rizikos DI sistemų automatiškai generuojamus žurnalus saugo kartu su tos direktyvos 74 straipsnyje nurodytais dokumentais.

21 straipsnis
Taisomieji veiksmai

Didelės rizikos DI sistemų tiekėjai, manantys arba turintys pagrindo manyti, kad didelės rizikos DI sistema, kurią jie pateikė rinkai arba pradėjo naudoti, neatitinka šio reglamento, nedelsdami imasi taisomųjų veiksmų, kurie, priklausomai nuo atvejo, būtini tos sistemos atitikčiai užtikrinti arba tai sistemai pašalinti ar atšaukti. Jie apie tai informuoja atitinkamos didelės rizikos DI sistemos platintojus ir, kai taikoma, įgaliotuosius atstovus bei importuotojus.

22 straipsnis
Pareiga informuoti

Jei didelės rizikos DI sistema kelia 65 straipsnio 1 dalyje apibrėžtą riziką ir ta rizika yra žinoma sistemos tiekėjui, tas tiekėjas nedelsdamas informuoja valstybių narių, kurių rinkai jis tą sistemą tiekia, nacionalines kompetentingas institucijas ir, kai taikoma, notifikuotąją įstaigą, išdavusią didelės rizikos DI sistemos sertifikatą, visų pirma apie neatitiktį ir taisomuosius veiksmus, kurių buvo imtasi.

23 straipsnis
Bendradarbiavimas su kompetentingomis institucijomis

Gavę nacionalinės kompetentingos institucijos prašymą, didelės rizikos DI sistemų tiekėjai viena iš oficialiųjų Sąjungos kalbų, kurią nustato atitinkama valstybė narė, tai institucijai pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. Gavę pagrįstą nacionalinės kompetentingos institucijos prašymą, tiekėjai tai institucijai taip pat suteikia galimybę susipažinti su savo didelės rizikos DI sistemos automatiškai generuojamais žurnalais, jei tik tokie žurnalai yra jų žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus.

24 straipsnis
Gaminių gamintojų pareigos

Jei su gaminiais, kuriems taikomi II priedo A skirsnyje išvardyti teisės aktai, susijusi didelės rizikos DI sistema rinkai pateikiama arba naudoti pradedama gaminio gamintojo vardu kartu su gaminiu, pagamintu laikantis tų teisės aktų, gaminio gamintojas prisiima atsakomybę už DI sistemos atitiktį šiam reglamentui ir turi vykdyti tokias pačias su DI sistema susijusias pareigas, kokias pagal šį reglamentą turi vykdyti tiekėjas.

25 straipsnis
Įgaliotieji atstovai

1. Tais atvejais, kai neįmanoma nustatyti importuotojo, prieš pateikdami savo sistemas Sąjungos rinkai, už Sąjungos ribų įsisteigę tiekėjai rašytiniu įgaliojimu paskiria Sąjungoje įsisteigusį įgaliotąjį atstovą.

2. Įgaliotasis atstovas atlieka tiekėjo suteiktame įgaliojime nurodytas užduotis. Įgaliojimu įgaliotajam atstovui suteikiama teisė atlikti šias užduotis:

   (a) saugoti ES atitikties deklaracijos ir techninių dokumentų kopijas, kad jas galėtų patikrinti 63 straipsnio 7 dalyje nurodytos nacionalinės kompetentingos institucijos ir nacionalinės institucijos;

(b) gavus pagrįstą prašymą, pateikti nacionalinei kompetentingai institucijai visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, be kita ko, suteikti galimybę susipažinti su didelės rizikos DI sistemos automatiškai generuojamais žurnalais, jei tik tokie žurnalai yra tiekėjo žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus;

(c) gavus pagrįstą prašymą, bendradarbiauti su nacionalinėmis kompetentingomis institucijomis įgyvendinant veiksmus, kurių jos imasi dėl didelės rizikos DI sistemų.

26 straipsnis
Importuotojų pareigos

1. Prieš pateikdami rinkai didelės rizikos DI sistemą, tokios sistemos importuotojai užtikrina, kad:

(a) tos DI sistemos tiekėjas būtų atlikęs reikiamą atitikties vertinimo procedūrą;

(b) tiekėjas būtų pagal IV priedą parengęs techninius dokumentus;

(c) sistema būtų pažymėta reikiamu atitikties ženklu ir kartu su ja būtų pateikiami reikiami dokumentai ir naudojimo instrukcijos.

2. Jei importuotojas mano arba turi pagrindo manyti, kad didelės rizikos DI sistema neatitinka šio reglamento reikalavimų, jis nepateikia tos sistemos rinkai tol, kol neužtikrinama jos atitiktis. Jei didelės rizikos DI sistema kelia riziką, kaip apibrėžta 65 straipsnio 1 dalyje, importuotojas apie tai informuoja DI sistemos tiekėją ir rinkos priežiūros institucijas.

3. Importuotojai ant didelės rizikos DI sistemos arba, jei to padaryti neįmanoma, atitinkamai ant jos pakuotės arba prie jos pridedamuose dokumentuose nurodo savo pavadinimą, registruotą prekybinį pavadinimą arba registruotą prekių ženklą ir adresą, kuriuo su jais galima susisiekti.

4. Kol atsakomybė už didelės rizikos DI sistemą tenka importuotojams, jie užtikrina, kad laikymo ar transportavimo sąlygos (jei taikytina) nepakenktų jos atitikčiai šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams.

5. Gavę pagrįstą prašymą importuotojai nacionalinei kompetentingai institucijai pateikia visą tai institucijai lengvai suprantama kalba parengtą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, be kita ko, suteikia galimybę susipažinti su didelės rizikos DI sistemos automatiškai generuojamais žurnalais, jei tik tokie žurnalai yra tiekėjo žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus. Be to, jie bendradarbiauja su nacionalinėmis kompetentingomis institucijomis įgyvendinant veiksmus, kurių jos imasi dėl tos sistemos.

27 straipsnis
Platintojų pareigos

1. Prieš tiekdami didelės rizikos DI sistemą rinkai, platintojai patikrina, ar ji pažymėta reikiamu CE atitikties ženklu, ar kartu su ja pateikiami reikiami dokumentai ir naudojimo instrukcijos ir ar sistemos tiekėjas ir importuotojas (jei taikytina) įvykdė šiame reglamente nustatytas pareigas.

2. Jei platintojas mano arba turi pagrindo manyti, kad didelės rizikos DI sistema neatitinka šios antraštinės dalies 2 skyriuje nustatytų reikalavimų, jis netiekia tos sistemos rinkai tol, kol neužtikrinama jos atitiktis tiems reikalavimams. Be to, jei sistema kelia riziką, kaip apibrėžta 65 straipsnio 1 dalyje, platintojas apie tai informuoja atitinkamai sistemos tiekėją arba importuotoją.

3. Kol atsakomybė už didelės rizikos DI sistemą tenka platintojams, jie užtikrina, kad laikymo ar transportavimo sąlygos (jei taikytina) nepakenktų tos sistemos atitikčiai šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams.

4. Platintojas, manantis arba turintis pagrindo manyti, kad rinkai jo tiekiama didelės rizikos DI sistema neatitinka šios antraštinės dalies 2 skyriuje nustatytų reikalavimų, imasi taisomųjų veiksmų, reikalingų siekiant užtikrinti tos sistemos atitiktį tiems reikalavimams, ją pašalinti iš rinkos arba atšaukti, arba užtikrina, kad tų taisomųjų veiksmų imtųsi atitinkamai tiekėjas, importuotojas arba atitinkamas veiklos vykdytojas. Jei didelės rizikos DI sistema kelia riziką, kaip apibrėžta 65 straipsnio 1 dalyje, platintojas nedelsdamas apie tai praneša valstybių narių, kurių rinkoms jis tiekia gaminį, nacionalinėms kompetentingoms institucijoms ir pateikia išsamią informaciją, visų pirma apie neatitiktį ir taisomuosius veiksmus, kurių imtasi.

5. Gavę pagrįstą nacionalinės kompetentingos institucijos prašymą, didelės rizikos DI sistemos platintojai jai pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. Be to, platintojai bendradarbiauja su ta nacionaline kompetentinga institucija įgyvendinant veiksmus, kurių ji imasi.

28 straipsnis

Platintojų, importuotojų, naudotojų ar bet kurių kitų trečiųjų šalių pareigos

1. Taikant šį reglamentą, platintojas, importuotojas, naudotojas ar kita trečioji šalis laikomi tiekėjais ir turi vykdyti 16 straipsnyje nustatytas tiekėjo pareigas bet kuriuo iš šių atvejų:

   (a) jei jie didelės rizikos DI sistemą rinkai pateikia arba pradeda naudoti savo vardu arba naudodami savo prekių ženklą;

   (b) jei jie pakeičia jau rinkai pateiktos arba pradėtos naudoti didelės rizikos DI sistemos numatytąją paskirtį;

   (c) jei jie iš esmės pakeičia didelės rizikos DI sistemą.

2. Didelės rizikos DI sistemą iš pradžių rinkai pateikęs arba pradėjęs naudoti tiekėjas 1 punkto b ir c papunkčiuose nurodytais atvejais šio reglamento taikymo tikslais nustojamas laikyti tiekėju.

29 straipsnis

Didelės rizikos DI sistemų naudotojų pareigos

1. Didelės rizikos DI sistemų naudotojai tokias sistemas naudoja laikydamiesi kartu su jomis pateiktų naudojimo instrukcijų ir 2–5 dalių nuostatų.

2. 1 dalyje nustatytos pareigos nedaro poveikio kitoms naudotojų pareigoms pagal Sąjungos ar nacionalinę teisę ir naudotojų laisvei savo nuožiūra organizuoti savo išteklius ir veiklą siekiant taikyti tiekėjo nurodytas žmogaus vykdomos priežiūros priemones.

3. Nepažeidžiant 1 dalies, jei naudotojas kontroliuoja įvesties duomenis, jis užtikrina, kad tie įvesties duomenys būtų aktualūs atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį.

4. Naudotojai stebi didelės rizikos DI sistemos veikimą, atsižvelgdami į jos naudojimo instrukcijas. Jei jie turi pagrindo manyti, kad pagal naudojimo instrukcijas naudojama DI sistema gali kelti riziką, kaip apibrėžta 65 straipsnio 1 dalyje, jie apie tai informuoja tiekėją arba platintoją ir sustabdo sistemos naudojimą. Be to, nustatę 62 straipsnyje apibrėžtų didelių incidentų ar veikimo sutrikimų, jie apie tai informuoja tiekėją arba platintoją ir nutraukia DI sistemos naudojimą. Jei naudotojas negali susisiekti su tiekėju, *mutatis mutandis* taikomas 62 straipsnis.

5. Jei naudotojas yra kredito įstaiga, kurios veikla reglamentuojama Direktyva 2013/36/ES, pirmoje pastraipoje nustatyta stebėjimo pareiga laikoma įvykdyta, jei laikomasi tos direktyvos 74 straipsnyje nustatytų taisyklių dėl vidaus valdymo priemonių, procesų ir mechanizmų.

6. Didelės rizikos DI sistemos naudotojai saugo tos sistemos automatiškai generuojamus žurnalus, jei tik tokie žurnalai yra jų žinioje. Žurnalų saugojimo laikotarpis turi būti tinkamas atsižvelgiant į didelės rizikos DI sistemos numatytąją paskirtį ir į taikytinas Sąjungos ar nacionalinėje teisėje nustatytas teisines pareigas.

   Naudotojai, kurie yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, žurnalus saugo kartu su dokumentais, susijusiais su tos direktyvos 74 straipsnyje nurodytomis vidaus valdymo priemonėmis, procesais ir mechanizmais.

7. Naudodamiesi pagal 13 straipsnį pateikta informacija, didelės rizikos DI sistemų naudotojai, jei taikytina, įvykdo Reglamento (ES) 2016/679 35 straipsnyje arba Direktyvos (ES) 2016/680 27 straipsnyje nustatytą pareigą atlikti poveikio duomenų apsaugai vertinimą.

4 SKYRIUS

NOTIFIKUOJANČIOSIOS INSTITUCIJOS IR NOTIFIKUOTOSIOS ĮSTAIGOS

30 straipsnis
Notifikuojančiosios institucijos

1. Kiekviena valstybė narė paskiria arba įsteigia notifikuojančiąją instituciją, atsakingą už reikiamų atitikties vertinimo įstaigų vertinimo, paskyrimo, notifikavimo ir stebėjimo procedūrų nustatymą ir vykdymą.

2. Valstybės narės notifikuojančiosiomis institucijomis gali paskirti Reglamente (EB) Nr. 765/2008 nurodytas nacionalines akreditacijos įstaigas.

3. Notifikuojančiosios institucijos įsteigiamos, jų veikla organizuojama ir vykdoma taip, kad nekiltų jokių interesų konfliktų su atitikties vertinimo įstaigomis ir būtų užtikrintas jų veiklos objektyvumas ir nešališkumas.

4. Notifikuojančiųjų institucijų veikla organizuojama taip, kad su atitikties vertinimo įstaigų notifikavimu susijusius sprendimus priimtų kompetentingi asmenys, nedalyvavę atliekant tų įstaigų vertinimą.

5. Notifikuojančiosios institucijos nesisiūlo vykdyti ir nevykdo jokios veiklos, kurią vykdo atitikties vertinimo įstaigos, taip pat neteikia konsultavimo paslaugų komerciniu arba konkurenciniu pagrindu.

6. Notifikuojančiosios institucijos užtikrina savo gaunamos informacijos konfidencialumą.

7. Notifikuojančiosiose institucijose turi būti pakankamai kompetentingų darbuotojų, galinčių tinkamai atlikti jų užduotis.

8. Notifikuojančiosios institucijos užtikrina, kad atitikties vertinimas būtų atliekamas proporcingai, neužkraunant nereikalingos naštos tiekėjams, ir kad vykdydamos savo veiklą notifikuotosios įstaigos deramai atsižvelgtų į įmonės dydį, sektorių, kuriame ji veikia, jos struktūrą, ir konkrečios DI sistemos sudėtingumo laipsnį.

31 straipsnis
Atitikties vertinimo įstaigos notifikavimo paraiška

1. Atitikties vertinimo įstaigos notifikavimo paraišką pateikia valstybės narės, kurioje jos yra įsisteigusios, notifikuojančiajai institucijai.

2. Prie notifikavimo paraiškos pridedamas atitikties vertinimo veiklos, atitikties vertinimo modulio ar modulių ir dirbtinio intelekto technologijų, kurias vertinti ta įstaiga teigia turinti kompetencijos, aprašas, taip pat nacionalinės akreditacijos įstaigos išduotas akreditacijos pažymėjimas (jei toks yra), kuriuo patvirtinama, kad atitikties vertinimo įstaiga atitinka 33 straipsnyje nustatytus reikalavimus. Jei paraišką teikianti įstaiga jau yra paskirta notifikuotąja įstaiga pagal kitus Sąjungos derinamuosius teisės aktus, kartu pateikiami galiojantys su tuo susiję dokumentai.

3. Jei atitikties vertinimo įstaiga negali pateikti akreditacijos pažymėjimo, ji notifikuojančiajai institucijai pateikia patvirtinamuosius dokumentus, būtinus jos atitikčiai 33 straipsnyje nustatytiems reikalavimams patikrinti, patvirtinti ir reguliariai stebėti. Jei įstaiga yra paskirta notifikuotąja įstaiga pagal kitus Sąjungos derinamuosius teisės aktus, visi su tais paskyrimais susiję dokumentai ir sertifikatai prireikus gali būti naudojami pagal šį reglamentą atliekamai jos paskyrimo procedūrai pagrįsti.

32 straipsnis
Notifikavimo procedūra

1. Notifikuojančiosios institucijos gali notifikuoti tik 33 straipsnyje nustatytus reikalavimus atitinkančias atitikties vertinimo įstaigas.

2. Notifikavimo pranešimą Komisijai ir kitoms valstybėms narėms notifikuojančiosios institucijos pateikia naudodamosi Komisijos sukurta ir administruojama elektronine notifikavimo priemone.

3. Notifikavimo pranešime pateikiama išsami informacija apie atitikties vertinimo veiklą, atitikties vertinimo modulį ar modulius ir atitinkamas dirbtinio intelekto technologijas.

4. Atitinkama atitikties vertinimo įstaiga notifikuotosios įstaigos veiklą gali vykdyti tik tuo atveju, jei nei Komisija, nei kitos valstybės narės per vieną mėnesį nuo notifikavimo nepareiškia prieštaravimų.

5. Notifikuojančiosios institucijos praneša Komisijai ir kitoms valstybėms narėms apie visus paskesnius notifikavimo galiojimo pokyčius.

33 straipsnis
Notifikuotosios įstaigos

1. Notifikuotosios įstaigos, laikydamosi 43 straipsnyje nurodytų atitikties vertinimo procedūrų, tikrina didelės rizikos DI sistemų atitiktį.

2. Notifikuotosios įstaigos turi atitikti organizacinius, kokybės valdymo, išteklių ir procesų reikalavimus, būtinus siekiant užtikrinti, kad jos galėtų vykdyti savo užduotis.

3. Notifikuotųjų įstaigų organizacinė struktūra, atsakomybės paskirstymas, atskaitomybės ryšiai ir veikla turi būti tokie, kad būtų užtikrintas pasitikėjimas notifikuotųjų įstaigų vykdomos atitikties vertinimo veiklos veiksmingumu ir rezultatais.

4. Notifikuotosios įstaigos turi būti nepriklausomos nuo tiekėjo, kurio didelės rizikos DI sistemos atitikties vertinimą jos atlieka. Notifikuotosios įstaigos turi būti nepriklausomos ir nuo kitų veiklos vykdytojų, turinčių su vertinama didelės rizikos DI sistema susijusių ekonominių interesų, taip pat nuo tiekėjo konkurentų.

5. Notifikuotųjų įstaigų veikla organizuojama ir vykdoma taip, kad būtų užtikrintas jos nepriklausomumas, objektyvumas ir nešališkumas. Notifikuotosios įstaigos dokumentuoja ir įdiegia struktūrą bei procedūras, kuriomis užtikrinamas nešališkumas ir nešališkumo principų propagavimas ir taikymas visoje jų organizacinėje struktūroje, tarp jų darbuotojų ir jų vertinimo veikloje.

6. Notifikuotosios įstaigos taiko dokumentuotas procedūras, kuriomis užtikrinama, kad jų darbuotojai, komitetai, pavaldžiosios įstaigos, subrangovai, visos susijusios įstaigos ar išorės įstaigų darbuotojai laikytųsi informacijos, kurią jie gauna vykdydami atitikties vertinimo veiklą, konfidencialumo reikalavimų, išskyrus atvejus, kai ją atskleisti reikalaujama pagal teisės aktus. Notifikuotųjų įstaigų darbuotojai visą informaciją, kurią jie gauna atlikdami savo užduotis pagal šį reglamentą, saugo kaip profesinę paslaptį – tai netaikoma tik valstybės narės, kurioje tos įstaigos vykdo savo veiklą, notifikuojančiųjų institucijų atžvilgiu.

7. Notifikuotosios įstaigos savo veiklą vykdo taikydamos procedūras, kuriomis deramai atsižvelgiama į įmonės dydį, sektorių, kuriame ji veikia, jos struktūrą ir konkrečios DI sistemos sudėtingumo laipsnį.

8. Notifikuotosios įstaigos turi turėti tinkamą su jų vykdoma atitikties vertinimo veikla susijusį civilinės atsakomybės draudimą, išskyrus atvejus, kai šią atsakomybę pagal nacionalinę teisę prisiima atitinkama valstybė narė arba kai ta valstybė narė tiesiogiai atsako už atitikties vertinimą.

9. Notifikuotosios įstaigos turi būti pajėgios atlikti visas pagal šį reglamentą joms tenkančias užduotis užtikrindamos aukščiausio laipsnio profesinį sąžiningumą ir reikiamą konkrečios srities kompetenciją, nesvarbu, ar tas užduotis vykdytų pačios notifikuotosios įstaigos, ar jos būtų vykdomos jų vardu ir jų atsakomybe.

10. Notifikuotosios įstaigos turi turėti pakankamai vidinės kompetencijos, kad galėtų veiksmingai įvertinti jų vardu užduotis atliekančių išorės subjektų darbą. Tuo tikslu notifikuotoji įstaiga turi visada turėti pakankamai kiekvienai atitikties vertinimo procedūrai atlikti ir kiekvienos rūšies didelės rizikos DI sistemos, kurios atitiktį vertinti ji paskirta, atitikčiai įvertinti reikalingų administracinių, techninių ir mokslinių darbuotojų, turinčių patirties ir žinių, susijusių su atitinkamomis dirbtinio

intelekto technologijomis, duomenimis, duomenų kompiuterija ir šios antraštinės dalies 2 skyriuje nustatytais reikalavimais.

11. Notifikuotosios įstaigos dalyvauja 38 straipsnyje nurodytoje koordinavimo veikloje. Jos taip pat turi tiesiogiai dalyvauti arba būti atstovaujamos Europos standartizacijos organizacijų veikloje arba užtikrinti, kad visada žinotų apie atitinkamus standartus ir jų naujoves.

12. Notifikuotosios įstaigos sudaro 30 straipsnyje nurodytai notifikuojančiajai institucijai sąlygas susipažinti su visa reikiama dokumentacija, įskaitant tiekėjo dokumentus, ir gavusios prašymą juos jai pateikia, kad ji galėtų vykdyti vertinimo, paskyrimo, notifikavimo, stebėsenos ir priežiūros veiklą ir kad būtų lengviau atlikti šiame skyriuje aprašytą vertinimą.

34 straipsnis

Notifikuotųjų įstaigų pavaldžiosios įstaigos ir subrangovai

1. Jei notifikuotoji įstaiga tam tikras su atitikties vertinimu susijusias užduotis paveda atlikti subrangovui ar pavaldžiajai įstaigai, ji užtikrina, kad tas subrangovas ar pavaldžioji įstaiga atitiktų 33 straipsnyje nustatytus reikalavimus, ir apie tai informuoja notifikuojančiąją instituciją.

2. Notifikuotosios įstaigos prisiima visą atsakomybę už subrangovų ar pavaldžiųjų įstaigų atliekamas užduotis, neatsižvelgiant į tai, kur jie yra įsisteigę.

3. Pavesti veiklą vykdyti subrangovui ar pavaldžiajai įstaigai galima tik gavus tiekėjo sutikimą.

4. Notifikuotosios įstaigos saugo aktualius dokumentus, susijusius su subrangovo ar pavaldžiosios įstaigos kvalifikacijos įvertinimu ir jų pagal šį reglamentą atliktu darbu, kad notifikuojančioji institucija galėtų juos patikrinti.

35 straipsnis

Pagal šį reglamentą paskirtų notifikuotųjų įstaigų identifikaciniai numeriai ir sąrašai

1. Komisija notifikuotosioms įstaigoms suteikia identifikacinius numerius. Komisija vienai įstaigai suteikia tik vieną numerį, net jei ji yra notifikuota pagal kelis Sąjungos aktus.

2. Komisija viešai paskelbia pagal šį reglamentą notifikuotų įstaigų sąrašą, kuriame taip pat nurodomi joms suteikti identifikaciniai numeriai ir veikla, kurią joms pavesta vykdyti kaip notifikuotosioms įstaigoms. Komisija užtikrina, kad tas sąrašas būtų nuolat atnaujinamas.

36 straipsnis

Notifikavimo galiojimo pokyčiai

1. Jei notifikuojančioji institucija įtaria arba jai yra pranešama, kad notifikuotoji įstaiga nebeatitinka 33 straipsnyje nustatytų reikalavimų arba nevykdo savo pareigų, ta institucija nedelsdama atlieka nuodugnų su tuo susijusį tyrimą. Tokiu atveju ji informuoja atitinkamą notifikuotąją įstaigą apie pareikštą kritiką ir suteikia jai galimybę pateikti savo nuomonę. Jei notifikuojančioji institucija padaro išvadą, kad tiriama notifikuotoji įstaiga nebeatitinka 33 straipsnyje nustatytų reikalavimų arba nevykdo savo pareigų, ji, priklausomai nuo pažeidimo rimtumo, apriboja, laikinai

sustabdo arba panaikina notifikavimo galiojimą. Ji taip pat nedelsdama apie tai informuoja Komisiją ir kitas valstybes nares.

2. Tais atvejais, kai notifikavimo galiojimas apribojamas, laikinai sustabdomas ar panaikinamas arba notifikuotoji įstaiga nutraukia savo veiklą, notifikuojančioji institucija imasi tinkamų veiksmų, skirtų užtikrinti, kad tos notifikuotosios įstaigos dokumentus perimtų kita notifikuotoji įstaiga arba kad jie būtų saugomi ir paprašius pateikiami atsakingoms notifikuojančiosioms institucijoms.

37 straipsnis
Notifikuotųjų įstaigų kompetencijos užginčijimas

1. Prireikus Komisija ištiria visus atvejus, kuriais esama pagrindo abejoti, kad notifikuotoji įstaiga atitinka 33 straipsnyje nustatytus reikalavimus.

2. Paprašyta notifikuojančioji institucija pateikia Komisijai visą aktualią informaciją, susijusią su atitinkamos notifikuotosios įstaigos notifikavimu.

3. Komisija užtikrina, kad visa konfidenciali informacija, gaunama atliekant šiame straipsnyje nurodytus tyrimus, būtų tvarkoma konfidencialiai.

4. Jei Komisija nustato, kad notifikuotoji įstaiga neatitinka arba nebeatitinka 33 straipsnyje nustatytų reikalavimų, ji priima pagrįstą sprendimą, kuriuo notifikuojančiosios valstybės narės paprašo imtis būtinų taisomųjų priemonių, įskaitant, jei būtina, notifikavimo galiojimo panaikinimą. Tas įgyvendinimo aktas priimamas laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

38 straipsnis
Notifikuotųjų įstaigų veiklos koordinavimas

1. Komisija užtikrina, kad srityse, kurioms taikomas šis reglamentas, per sektoriaus notifikuotųjų įstaigų grupę būtų organizuojamas ir tinkamai vykdomas notifikuotųjų įstaigų, pagal šį reglamentą atliekančių DI sistemų atitikties vertinimo procedūras, veiklos koordinavimas ir jų bendradarbiavimas.

2. Valstybės narės užtikrina, kad jų notifikuotos įstaigos tiesiogiai arba per paskirtus atstovus dalyvautų tos grupės veikloje.

39 straipsnis
Trečiųjų valstybių atitikties vertinimo įstaigos

Pagal trečiųjų valstybių, su kuriomis Sąjunga yra sudariusi susitarimus, teisę įsteigtoms atitikties vertinimo įstaigoms gali būti leista vykdyti šiame reglamente nurodytą notifikuotųjų įstaigų veiklą.

5 SKYRIUS

STANDARTAI, ATITIKTIES VERTINIMAS, SERTIFIKATAI, REGISTRACIJA

40 straipsnis
Darnieji standartai

Didelės rizikos DI sistemos, atitinkančios darniuosius standartus ar jų dalis, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, laikomos atitinkančiomis šios

antraštinės dalies 2 skyriuje nustatytus reikalavimus, jei tik tie reikalavimai yra įtraukti į tuos standartus.

41 straipsnis
Bendrosios specifikacijos

1. Jei 40 straipsnyje nurodytų darniųjų standartų nėra arba Komisija mano, kad atitinkami darnieji standartai yra nepakankami arba kad būtina spręsti konkrečius susirūpinimą keliančius saugos ir pagrindinių teisių klausimus, ji gali priimti įgyvendinimo aktus, kuriuose būtų nustatytos su šios antraštinės dalies 2 skyriuje nustatytais reikalavimais susijusios bendrosios specifikacijos. Tie įgyvendinimo aktai priimami laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.
2. Rengdama 1 dalyje nurodytas bendrąsias specifikacijas, Komisija sužino atitinkamų įstaigų arba ekspertų grupių, įsteigtų pagal atitinkamus sektorinius Sąjungos teisės aktus, nuomones.
3. 1 dalyje nurodytas bendrąsias specifikacijas atitinkančios didelės rizikos DI sistemos laikomos atitinkančiomis šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, jei tik tie reikalavimai yra įtraukti į tas bendrąsias specifikacijas.
4. Jei tiekėjai nesilaiko 1 dalyje nurodytų bendrųjų specifikacijų, jie tinkamai pagrindžia, kad yra įdiegę bent joms lygiaverčius techninius sprendimus.

42 straipsnis
Atitikties tam tikriems reikalavimams prielaida

1. Jei didelės rizikos DI sistema buvo mokoma ir bandoma naudojant duomenis, susijusius su konkrečia geografine, elgsenos ir funkcine aplinka, kurioje ją ketinama naudoti, atsižvelgiant į jos numatytąją paskirtį, daroma prielaida, kad ji atitinka 10 straipsnio 4 dalyje nustatytą reikalavimą.
2. Jei didelės rizikos DI sistema yra, laikantis Europos Parlamento ir Tarybos reglamento (ES) 2019/881[63], sertifikuota pagal kibernetinio saugumo sertifikavimo schemą, kurios nuoroda yra paskelbta *Europos Sąjungos oficialiajame leidinyje*, arba jai pagal šią schemą yra išduotas atitikties pareiškimas, daroma prielaida, kad ji atitinka šio reglamento 15 straipsnyje nustatytus kibernetinio saugumo reikalavimus, jei tik tas kibernetinio saugumo sertifikatas, atitikties pareiškimas arba jų dalys apima tuos reikalavimus.

43 straipsnis
Atitikties vertinimas

1. Dėl III priedo 1 punkte išvardytų didelės rizikos DI sistemų pažymėtina, kad tais atvejais, kai tiekėjas, siekdamas įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, taiko 40 straipsnyje nurodytus darniuosius standartus arba, jei taikytina, 41 straipsnyje nurodytas bendrąsias specifikacijas, jis taiko vieną iš šių procedūrų:

[63] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 1).

(a) VI priede nurodytą vidaus kontrole grindžiamą atitikties vertinimo procedūrą;

(b) VII priede nurodytą kokybės valdymo sistemos ir techninių dokumentų vertinimu grindžiamą atitikties vertinimo procedūrą, kurioje dalyvauja notifikuotoji įstaiga.

Jei tiekėjas, siekdamas įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, 40 straipsnyje nurodytų darniųjų standartų netaiko arba juos taiko tik iš dalies arba jei tokių darniųjų standartų ir 41 straipsnyje nurodytų bendrųjų specifikacijų nėra, tiekėjas taiko VII priede nurodytą atitikties vertinimo procedūrą.

VII priede nurodytai atitikties vertinimo procedūrai atlikti tiekėjas gali pasirinkti bet kurią notifikuotąją įstaigą. Tačiau jei sistema yra skirta naudoti teisėsaugos, imigracijos arba prieglobsčio institucijoms, taip pat ES institucijoms, įstaigoms ar agentūroms, notifikuotosios įstaigos funkcijas atlieka atitinkamai 63 straipsnio 5 arba 6 dalyje nurodyta rinkos priežiūros institucija.

2. III priedo 2–8 punktuose nurodytoms didelės rizikos DI sistemoms tiekėjai taiko VI priede nurodytą vidaus kontrole grindžiamą atitikties vertinimo procedūrą, kurioje notifikuotosios įstaigos dalyvavimas nenumatytas. III priedo 5 punkto b papunktyje nurodytų didelės rizikos DI sistemų, kurias rinkai pateikia arba pradeda naudoti kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, atitiktis įvertinama atliekant tos direktyvos 97–101 straipsniuose nurodytą procedūrą.

3. Didelės rizikos DI sistemoms, kurioms taikomi II priedo A skirsnyje išvardyti teisės aktai, tiekėjas taiko atitinkamas tuose teisės aktuose reikalaujamas atitikties vertinimo procedūras. Toms didelės rizikos DI sistemoms taikomi šios antraštinės dalies 2 skyriuje nustatyti reikalavimai, todėl per tuos vertinimus patikrinama ir atitiktis šiems reikalavimams. Taip pat taikomi VII priedo 4.3, 4.4, 4.5 punktai ir 4.6 punkto penkta pastraipa.

Teisę per tuos vertinimus tikrinti didelės rizikos DI sistemų atitiktį šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams turi pagal tuos teisės aktus paskirtos notifikuotosios įstaigos su sąlyga, kad atliekant notifikavimo pagal tuos teisės aktus procedūrą buvo įvertinta tų notifikuotųjų įstaigų atitiktis 33 straipsnio 4, 9 ir 10 dalyse nustatytiems reikalavimams.

Jei II priedo A skirsnyje išvardytuose teisės aktuose yra numatyta, kad tuo atveju, kai gaminio gamintojas taiko visus darniuosius standartus, apimančius visus atitinkamus reikalavimus, jis gali netaikyti trečiosios šalies atliekamo atitikties vertinimo procedūros, tas gamintojas ta galimybe gali pasinaudoti tik jei jis taip pat taiko darniuosius standartus arba, jei taikytina, 41 straipsnyje nurodytas bendrąsias specifikacijas, apimančius šios antraštinės dalies 2 skyriuje nustatytus reikalavimus.

4. Kas kartą iš esmės pakeitus didelės rizikos DI sistemą, atliekama nauja jos atitikties vertinimo procedūra, neatsižvelgiant į tai, ar pakeistą sistemą ketinama papildomai platinti, ar ja toliau naudosis dabartinis naudotojas.

Jei didelės rizikos DI sistema mokosi ir po to, kai buvo pateikta rinkai arba pradėta naudoti, tos sistemos ir jos veikimo pakeitimai, kuriuos tiekėjas buvo iš anksto numatęs tada, kai buvo atliekamas pirminis atitikties vertinimas, ir kurie yra paminėti į techninius dokumentus įtrauktoje IV priedo 2 punkto f papunktyje nurodytoje informacijoje, nelaikomi esminiais pakeitimais.

5. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kurių tikslas – atnaujinti VI ir VII priedus siekiant į atitikties vertinimo procedūras įtraukti elementus, kurie tampa būtini atsižvelgiant į technikos pažangą.

6. Komisijai suteikiami įgaliojimai priimti deleguotuosius aktus, kurių tikslas – iš dalies pakeisti 1 ir 2 dalis siekiant III priedo 2–8 punktuose nurodytoms didelės rizikos DI sistemoms taikyti VII priede arba jo dalyse nurodytą atitikties vertinimo procedūrą. Tokius deleguotuosius aktus Komisija priima atsižvelgdama į VI priede nurodytos vidaus kontrole grindžiamos atitikties vertinimo procedūros veiksmingumą siekiant užtikrinti, kad tokios sistemos nekeltų rizikos sveikatai, saugai ir pagrindinių teisių apsaugai, arba tokią riziką mažinti, taip pat į tai, ar notifikuotosios įstaigos turi pakankamai pajėgumų ir išteklių.

44 straipsnis
Sertifikatai

1. Pagal VII priedą notifikuotųjų įstaigų išduodami sertifikatai parengiami viena iš oficialiųjų Sąjungos kalbų, kurią nustato valstybė narė, kurioje yra įsisteigusi notifikuotoji įstaiga, arba viena iš oficialiųjų Sąjungos kalbų, kuri yra kitais atžvilgiais priimtina notifikuotajai įstaigai.

2. Sertifikatai galioja juose nurodytą laikotarpį, kuris negali būti ilgesnis nei penkeri metai. Tiekėjui pateikus paraišką, remiantis pakartotiniu vertinimu pagal taikytinas atitikties vertinimo procedūras, sertifikato galiojimas gali būti pratęstas papildomiems laikotarpiams, kurių nė vienas negali būti ilgesnis nei penkeri metai.

3. Jei notifikuotoji įstaiga nustato, kad DI sistema nebeatitinka šios antraštinės dalies 2 skyriuje nustatytų reikalavimų, ji, atsižvelgdama į proporcingumo principą, laikinai sustabdo arba panaikina išduoto sertifikato galiojimą arba nustato jo galiojimo apribojimus, išskyrus atvejus, kai sistemos tiekėjas per atitinkamą notifikuotosios įstaigos nustatytą laikotarpį imasi tinkamų taisomųjų veiksmų, kuriais užtikrinama atitiktis tiems reikalavimams. Notifikuotoji įstaiga nurodo savo sprendimo priežastis.

45 straipsnis
Notifikuotųjų įstaigų sprendimų apskundimas

Valstybės narės užtikrina, kad būtų nustatyta notifikuotųjų įstaigų sprendimų apskundimo procedūra, kuria galėtų pasinaudoti su konkrečiu sprendimu susijusių teisėtų interesų turinčios šalys.

46 straipsnis
Notifikuotųjų įstaigų pareiga informuoti

1. Notifikuotoji įstaiga informuoja notifikuojančiąją instituciją apie:

   (a) visus Sąjungos techninių dokumentų įvertinimo sertifikatus, tų sertifikatų papildymus ir kokybės valdymo sistemų patvirtinimus, išduotus pagal VII priedo reikalavimus;

   (b) kiekvieną atsisakymą pagal VII priedo reikalavimus išduoti Sąjungos techninių dokumentų įvertinimo sertifikatą arba kokybės sistemos patvirtinimą ir apie kiekvieno tokio pagal tuos reikalavimus išduoto dokumento galiojimo apribojimą, laikiną sustabdymą ar panaikinimą;

(c) visas aplinkybes, turinčias įtakos jos kaip notifikuotosios įstaigos įgaliojimų apimčiai ar jų suteikimo sąlygoms;

(d) kiekvieną iš rinkos priežiūros institucijų gautą prašymą pateikti informacijos, susijusios su atitikties vertinimo veikla;

(e) jei prašoma, atitikties vertinimo veiklą, vykdytą pagal jai kaip notifikuotajai įstaigai suteiktus įgaliojimus, ir bet kokią kitą vykdytą, pavyzdžiui, tarpvalstybinę ir subrangos, veiklą.

2. Kiekviena notifikuotoji įstaiga informuoja kitas notifikuotąsias įstaigas apie:

(a) kokybės valdymo sistemų patvirtinimus, kuriuos ji atsisakė išduoti arba kurių galiojimą ji laikinai sustabdė arba panaikino, o gavusi prašymą – ir apie išduotus kokybės sistemų patvirtinimus;

(b) ES techninių dokumentų įvertinimo sertifikatus arba jų papildymus, kuriuos ji atsisakė išduoti arba kurių galiojimą ji panaikino, laikinai sustabdė arba kitaip apribojo, o gavusi prašymą – ir apie išduotus sertifikatus ir (arba) jų papildymus.

3. Kiekviena notifikuotoji įstaiga kitoms notifikuotosioms įstaigoms, vykdančioms panašią tokių pačių dirbtinio intelekto technologijų atitikties vertinimo veiklą, teikia aktualią informaciją klausimais, susijusiais su neigiamais ir, jei prašoma, teigiamais atitikties vertinimo rezultatais.

47 straipsnis

Nukrypti nuo atitikties vertinimo procedūros leidžianti nuostata

1. Nukrypdama nuo 43 straipsnio, bet kuri rinkos priežiūros institucija gali dėl išskirtinių priežasčių, susijusių su visuomenės saugumu arba žmonių gyvybės ir sveikatos, aplinkos ir svarbiausių pramonės ir infrastruktūros objektų apsauga, leisti atitinkamos valstybės narės teritorijoje rinkai pateikti arba pradėti naudoti konkrečias didelės rizikos DI sistemas. Tas leidimas išduodamas ribotam laikotarpiui, per kurį atliekamos būtinos atitikties vertinimo procedūros, ir nustoja galioti užbaigus tas procedūras. Tos procedūros užbaigiamos nepagrįstai nedelsiant.

2. 1 dalyje nurodytas leidimas išduodamas tik jei rinkos priežiūros institucija padaro išvadą, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. Rinkos priežiūros institucija nedelsdama informuoja Komisiją ir kitas valstybes nares apie visus pagal 1 dalį išduotus leidimus.

3. Jei per 15 kalendorinių dienų nuo 2 dalyje nurodytos informacijos gavimo nei nė viena valstybė narė, nei Komisija nepareiškia prieštaravimų dėl valstybės narės rinkos priežiūros institucijos pagal 1 dalį išduoto leidimo, tas leidimas laikomas pagrįstu.

4. Jei per 15 kalendorinių dienų nuo 2 dalyje nurodyto pranešimo gavimo kuri nors valstybė narė pareiškia prieštaravimų dėl kitos valstybės narės rinkos priežiūros institucijos išduoto leidimo arba jei Komisija mano, kad leidimas prieštarauja Sąjungos teisei arba kad pagal 2 dalį valstybių narių padaryta išvada dėl sistemos atitikties yra nepagrįsta, Komisija nedelsdama pradeda konsultacijas su atitinkama valstybe nare; pasikonsultuojama su atitinkamu veiklos vykdytoju (-ais) ir suteikiama galimybė jam (jiems) pareikšti savo nuomonę. Atsižvelgdama į tai, Komisija nusprendžia, ar leidimas yra pagrįstas. Savo sprendimą Komisija skiria atitinkamai valstybei narei ir atitinkamam veiklos vykdytojui ar vykdytojams.

5. Jei nusprendžiama, kad leidimas nepagrįstas, atitinkamos valstybės narės rinkos priežiūros institucija jį panaikina.

6. Jei didelės rizikos DI sistema yra skirta naudoti kaip priemonių, kurioms taikomas Reglamentas (ES) 2017/745 ir Reglamentas (ES) 2017/746, saugos komponentas arba ji pati yra tokia priemonė, nukrypstant nuo 1–5 dalių, kartu su nuostata, leidžiančia nukrypti nuo atitikties šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams vertinimo procedūros, taikomi Reglamento (ES) 2017/745 59 straipsnis ir Reglamento (ES) 2017/746 54 straipsnis.

48 straipsnis
ES atitikties deklaracija

1. Tiekėjas parengia rašytinę kiekvienos DI sistemos ES atitikties deklaraciją ir saugo ją 10 metų nuo DI sistemos pateikimo rinkai arba pradėjimo naudoti dienos, kad nacionalinės kompetentingos institucijos galėtų ją patikrinti. ES atitikties deklaracijoje nurodoma DI sistema, dėl kurios ji parengta. Gavus prašymą, ES atitikties deklaracijos kopija pateikiama atitinkamoms nacionalinėms kompetentingoms institucijoms.

2. ES atitikties deklaracijoje nurodoma, kad atitinkama didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. ES atitikties deklaracijoje pateikiama V priede nurodyta informacija ir ta deklaracija išverčiama į valstybės (-ių) narės (-ių), kurioje (-iose) didelės rizikos DI sistema tiekiama, reikalaujamą oficialiąją Sąjungos kalbą ar kalbas.

3. Jei didelės rizikos DI sistemai taikomi ir kiti Sąjungos derinamieji teisės aktai, kuriuose taip pat reikalaujama pateikti ES atitikties deklaraciją, parengiama viena bendra su visais Sąjungos teisės aktais, taikomais tai didelės rizikos DI sistemai, susijusi ES atitikties deklaracija. Deklaracijoje pateikiama visa informacija, būtina norint nustatyti Sąjungos derinamuosius teisės aktus, su kuriais ta deklaracija yra susijusi.

4. Parengdamas ES atitikties deklaraciją tiekėjas prisiima atsakomybę už atitiktį šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams. Tiekėjas užtikrina, kad ES atitikties deklaracija prireikus būtų atnaujinama.

5. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kurių tikslas – atnaujinti V priede nustatytą ES atitikties deklaracijos turinį siekiant į jį įtraukti elementus, kurie tampa būtini atsižvelgiant į technikos pažangą.

49 straipsnis
CE atitikties ženklas

1. Didelės rizikos DI sistemos CE ženklu žymimos taip, kad jis būtų matomas, įskaitomas ir nenutrinamas. Jei taip žymėti neįmanoma arba negalima dėl didelės rizikos DI sistemos pobūdžio, šiuo ženklu pažymima atitinkamai pakuotė arba pridedami dokumentai.

2. 1 dalyje nurodytas žymėjimas CE ženklu atliekamas laikantis Reglamento (EB) Nr. 765/2008 30 straipsnyje nustatytų bendrųjų principų.

3. Jei taikytina, greta CE ženklo nurodomas notifikuotosios įstaigos, atsakingos už 43 straipsnyje nustatytas atitikties vertinimo procedūras, identifikacinis numeris. Identifikacinis numeris taip pat nurodomas visoje reklaminėje medžiagoje, kurioje

užsimenama, kad didelės rizikos DI sistema atitinka žymėjimo CE ženklu reikalavimus.

50 straipsnis
Dokumentų saugojimas

Tiekėjas 10 metų nuo DI sistemos pateikimo rinkai arba pradėjimo naudoti dienos saugo toliau nurodytus dokumentus, kad nacionalinės kompetentingos institucijos galėtų juos patikrinti:

(a) 11 straipsnyje nurodytus techninius dokumentus;

(b) su 17 straipsnyje nurodyta kokybės valdymo sistema susijusius dokumentus;

(c) jei taikytina, su notifikuotųjų įstaigų patvirtintais pakeitimais susijusius dokumentus;

(d) jei taikytina, notifikuotųjų įstaigų priimtus sprendimus ir kitus jų išduotus dokumentus;

(e) 48 straipsnyje nurodytą ES atitikties deklaraciją.

51 straipsnis
Registracija

Prieš pateikdamas rinkai arba pradėdamas naudoti 6 straipsnio 2 dalyje nurodytą didelės rizikos DI sistemą, tiekėjas arba, jei taikytina, įgaliotasis atstovas tą sistemą užregistruoja 60 straipsnyje nurodytoje ES duomenų bazėje.

IV ANTRAŠTINĖ DALIS

TAM TIKROMS DI SISTEMOMS TAIKOMI SKAIDRUMO REIKALAVIMAI

52 straipsnis
Tam tikroms DI sistemoms taikomi skaidrumo reikalavimai

1. Tiekėjai užtikrina, kad DI sistemos, kurių paskirtis – bendrauti su fiziniais asmenimis, būtų suprojektuotos ir sukurtos taip, kad fiziniai asmenys būtų informuojami apie tai, kad bendrauja su DI sistema, nebent tai būtų akivaizdu iš aplinkybių ir naudojimo konteksto. Šis reikalavimas netaikomas DI sistemoms, kurias pagal teisės aktus leidžiama naudoti siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ir už jas patraukti baudžiamojon atsakomybėn, išskyrus atvejus, kai tomis sistemomis pranešimo apie nusikalstamą veiką tikslais leidžiama naudotis visuomenei.

2. Emocijų atpažinimo arba biometrinio kategorizavimo sistemų naudotojai informuoja fizinius asmenis, kurių atžvilgiu jos naudojamos, apie tokių sistemų veikimą. Šis reikalavimas netaikomas biometrinio kategorizavimo DI sistemoms, kurias pagal teisės aktus leidžiama naudoti siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią ir jas tirti.

3. DI sistemų, kuriomis sukuriamas į realius asmenis, objektus, vietas ar kitus dalykus ar įvykius labai panašus judamo bei nejudamo vaizdo ir garso turinys, kurį asmuo gali klaidingai palaikyti autentišku ar tikru (sintetinė sankaita), arba tokiu turiniu

manipuliuojama, naudotojai nurodo, kad tas turinys sukurtas dirbtinai arba kad su juo atliktos manipuliacijos.

Tačiau pirma pastraipa netaikoma tais atvejais, kai toks naudojimas yra leidžiamas pagal teisės aktus siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ir už jas patraukti baudžiamojon atsakomybėn arba kai tai būtina norint naudotis ES pagrindinių teisių chartijoje įtvirtintomis teisėmis į saviraiškos laisvę bei menų ir mokslo laisvę, su sąlyga, kad taikomos tinkamos trečiųjų šalių teisių ir laisvių apsaugos priemonės.

4. 1, 2 ir 3 dalių nuostatomis nedaromas poveikis šio reglamento III antraštinėje dalyje nustatytiems reikalavimams ir pareigoms.

V ANTRAŠTINĖ DALIS

INOVACIJŲ RĖMIMO PRIEMONĖS

53 straipsnis
DI srities apribotos bandomosios reglamentavimo aplinkos

1. Vienos ar kelių valstybių narių kompetentingų institucijų arba Europos duomenų apsaugos priežiūros pareigūno sukurta DI srities apribota bandomoji reglamentavimo aplinka yra kontroliuojama aplinka, sudaranti palankesnes sąlygas, prieš pateikiant novatoriškas DI sistemas rinkai arba pradedant jas naudoti, tam tikrą laiką jas kurti, bandyti ir validuoti pagal konkretų planą. Siekiant užtikrinti atitiktį šio reglamento ir atitinkamais atvejais kitų Sąjungos ir valstybių narių teisės aktų, kurių laikymasis prižiūrimas konkrečioje apribotoje bandomojoje aplinkoje, reikalavimams, nurodyta veikla vykdoma tiesiogiai prižiūrint ir vadovaujant kompetentingoms institucijoms.

2. Valstybės narės užtikrina, kad tais atvejais, kai novatoriškos DI sistemos apima asmens duomenų tvarkymą arba kitaip patenka į kitų nacionalinių institucijų ar kompetentingų institucijų, teikiančių arba remiančių prieigą prie duomenų, priežiūros sritį, nacionalinės duomenų apsaugos institucijos ir tos kitos nacionalinės institucijos būtų įtrauktos į DI srities apribotos bandomosios reglamentavimo aplinkos veiklą.

3. DI srities apribotos bandomosios reglamentavimo aplinkos nedaro poveikio su priežiūra ir taisomaisiais veiksmais susijusiems kompetentingų institucijų įgaliojimams. Kuriant ir bandant tokias sistemas nustatyta didelė sveikatai bei saugai ir pagrindinėms teisėms kylanti rizika turi būti nedelsiant sumažinama – priešingu atveju kūrimo ir bandymo procesas sustabdomas iki tol, kol ta rizika bus sumažinta.

4. DI srities apribotos bandomosios reglamentavimo aplinkos dalyviai lieka pagal taikytinus Sąjungos ir valstybių narių teisės aktus, kuriais reglamentuojama atsakomybė, atsakingi už trečiosioms šalims padarytą žalą, kurios priežastis – bandymai apribotoje bandomojoje aplinkoje.

5. DI srities apribotas bandomąsias reglamentavimo aplinkas sukūrusios valstybių narių kompetentingos institucijos tarpusavyje koordinuoja savo veiklą ir bendradarbiauja Europos dirbtinio intelekto valdyboje. Jos teikia šiai valdybai ir Komisijai metines ataskaitas, kuriose informuoja apie tokių programų įgyvendinimo rezultatus, be kita ko, pateikia gerosios praktikos pavyzdžių, aprašo įgytą patirtį ir pateikia rekomendacijų dėl jų struktūros, ir atitinkamais atvejais apie šio reglamento ir kitų Sąjungos teisės aktų, kurių laikymasis prižiūrimas konkrečioje apribotoje bandomojoje aplinkoje, taikymą.

6. DI srities apribotų bandomųjų reglamentavimo aplinkų veikimo tvarka ir sąlygos, be kita ko, tinkamumo kriterijai, paraiškų teikimo, atrankos, dalyvavimo apribotoje bandomojoje aplinkoje ir pasitraukimo iš jos tvarka ir dalyvių teisės ir pareigos, nustatomos įgyvendinimo aktuose. Tie įgyvendinimo aktai priimami laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

54 straipsnis

Papildomas asmens duomenų tvarkymas DI srities apribotoje bandomojoje reglamentavimo aplinkoje siekiant kurti tam tikras viešąjį interesą tenkinančias DI sistemas

1. Kitais tikslais teisėtai surinkti asmens duomenys gali būti tvarkomi DI srities apribotoje bandomojoje reglamentavimo aplinkoje siekiant joje kurti ir bandyti tam tikras novatoriškas DI sistemas, jei laikomasi šių sąlygų:

   (a) novatoriškos DI sistemos kuriamos siekiant apsaugoti svarbų viešąjį interesą vienoje ar keliose iš šių sričių:

      i) nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo už jas baudžiamojon atsakomybėn arba baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją (prižiūrint ir atsakomybę prisiimant kompetentingoms institucijoms). Duomenys tvarkomi remiantis valstybės narės arba Sąjungos teise;

      ii) visuomenės saugumo ir visuomenės sveikatos, įskaitant ligų prevenciją, kontrolę ir gydymą;

      iii) aukšto aplinkos apsaugos lygio užtikrinimo ir aplinkos kokybės gerinimo;

   (b) tvarkomi duomenys yra būtini siekiant laikytis vieno ar daugiau III antraštinės dalies 2 skyriuje nurodytų reikalavimų tais atvejais, kai tų reikalavimų neįmanoma veiksmingai įvykdyti tvarkant anoniminius, sintetinius ar kitus ne asmens duomenis;

   (c) yra taikomi veiksmingi stebėsenos mechanizmai, kurių tikslas – nustatyti, ar atliekant bandymus apribotoje bandomojoje aplinkoje gali kilti didelė rizika duomenų subjektų pagrindinėms teisėms, taip pat atsako mechanizmas, skirtas tai rizikai greitai sumažinti ir prireikus duomenų tvarkymui sustabdyti;

   (d) visi apribotoje bandomojoje aplinkoje tvarkytini asmens duomenys saugomi funkciniu požiūriu atskirtoje, izoliuotoje ir apsaugotoje dalyvių prižiūrimoje duomenų tvarkymo aplinkoje ir prieigą prie tų duomenų turi tik įgalioti asmenys;

   (e) jokie asmens duomenys neperduodami kitiems subjektams ir jiems nesuteikiama kitokia prieiga prie tų duomenų;

   (f) asmens duomenų tvarkymo apribotoje bandomojoje aplinkoje rezultatas nėra priemonės ar sprendimai, turintys įtakos duomenų subjektams;

   (g) apribotoje bandomojoje aplinkoje tvarkomi asmens duomenys pašalinami pasibaigus dalyvavimui apribotoje bandomojoje aplinkoje arba asmens duomenų saugojimo laikotarpiui;

   (h) asmens duomenų tvarkymo apribotoje bandomojoje aplinkoje žurnalai saugomi visą dalyvavimo apribotoje bandomojoje aplinkoje laikotarpį ir vienus metus po jo pabaigos – tai daroma tik tam, kad būtų įvykdytos šiame straipsnyje ar

kituose taikytinuose Sąjungos ar valstybių narių teisės aktuose nustatytos atskaitomybės ir dokumentavimo pareigos, ir tik jei to reikia toms pareigoms įvykdyti;

(i) kaip vienas iš IV priede nurodytų techninių dokumentų, kartu su bandymų rezultatais saugomas išsamus ir detalus DI sistemos mokymo, bandymo ir validavimo procesų ir loginio pagrindo aprašas;

(j) kompetentingų institucijų svetainėje yra paskelbtas glaustas apribotoje bandomojoje aplinkoje įgyvendinamo DI projekto, jo tikslų ir numatomų rezultatų aprašas.

2. 1 dalimi nepažeidžiami Sąjungos ar valstybių narių teisės aktai, kuriuose nenumatomas duomenų tvarkymas kitais nei tuose teisės aktuose aiškiai nurodytais tikslais.

55 straipsnis
Smulkiesiems tiekėjams ir naudotojams skirtos priemonės

1. Valstybės narės imasi šių veiksmų:

(a) suteikia tinkamumo sąlygas atitinkantiems smulkiesiems tiekėjams ir startuoliams pirmenybę dalyvauti DI srities apribotose bandomosiose reglamentavimo aplinkose;

(b) organizuoja specialią informuotumo apie šio reglamento taikymą didinimo veiklą, pritaikytą prie smulkiųjų tiekėjų ir naudotojų poreikių;

(c) prireikus sukuria specialų ryšių su smulkiaisiais tiekėjais, naudotojais ir kitais novatoriais palaikymo kanalą, kuriuo būtų teikiamos rekomendacijos ir atsakoma į užklausas dėl šio reglamento įgyvendinimo.

2. Nustatant rinkliavas už 43 straipsnyje nurodytą atitikties vertinimą atsižvelgiama į konkrečius smulkiųjų tiekėjų interesus ir poreikius – šios rinkliavos sumažinamos proporcingai jų dydžiui ir rinkos dydžiui.

VI ANTRAŠTINĖ DALIS

VALDYMAS

1 SKYRIUS

EUROPOS DIRBTINIO INTELEKTO VALDYBA

56 straipsnis
Europos dirbtinio intelekto valdybos įsteigimas

1. Įsteigiama Europos dirbtinio intelekto valdyba (toliau – Valdyba).

2. Valdyba teikia Komisijai rekomendacijas ir jai padeda, siekdama:

(a) skatinti veiksmingą nacionalinių priežiūros institucijų ir Komisijos bendradarbiavimą klausimais, kuriems taikomas šis reglamentas;

(b) koordinuoti Komisijos, nacionalinių priežiūros institucijų ir kitų kompetentingų institucijų rekomendacijas dėl vidaus rinkoje kylančių problemų, susijusių su klausimais, kuriems taikomas šis reglamentas, ir jų analizę ir padėti jas rengti;

(c) padėti nacionalinėms priežiūros institucijoms ir Komisijai užtikrinti nuoseklų šio reglamento taikymą.

57 straipsnis
Valdybos struktūra

1. Valdybą sudaro nacionalinės priežiūros institucijos, kurioms atstovauja tų institucijų vadovai arba lygiaverčiai aukšto rango pareigūnai, ir Europos duomenų apsaugos priežiūros pareigūnas. Kitos nacionalinės institucijos gali būti kviečiamos į posėdžius, kuriuose nagrinėjami joms svarbūs klausimai.

2. Valdyba, gavusi Komisijos pritarimą, paprasta savo narių balsų dauguma patvirtina darbo tvarkos taisykles. Darbo tvarkos taisyklėse taip pat nurodomi veiklos aspektai, susiję su 58 straipsnyje išvardytų Valdybos užduočių vykdymu. Valdyba prireikus gali įsteigti pogrupius konkretiems klausimams spręsti.

3. Valdybai pirmininkauja Komisija. Komisija sušaukia posėdžius ir rengia darbotvarkę atsižvelgdama į Valdybos užduotis pagal šį reglamentą ir darbo tvarkos taisykles. Komisija teikia administracinę ir analitinę paramą Valdybos veiklai pagal šį reglamentą.

4. Siekdama surinkti pakankamai informacijos, reikalingos savo veiklai vykdyti, Valdyba į savo posėdžius gali kviesti išorės ekspertus ir stebėtojus ir gali keistis informacija su suinteresuotomis trečiosiomis šalimis. Tuo tikslu Komisija gali sudaryti palankias sąlygas Valdybos ir kitų Sąjungos įstaigų, biurų, agentūrų ir patariamųjų grupių tarpusavio mainams.

58 straipsnis
Valdybos užduotys

Teikdama rekomendacijas ir pagalbą Komisijai pagal 56 straipsnio 2 dalį, Valdyba visų pirma:

(a) renka ekspertines žinias ir geriausią patirtį ir ja dalijasi su valstybėmis narėmis;

(b) prisideda prie vienodos administracinės praktikos valstybėse narėse, be kita ko, susijusios su 53 straipsnyje nurodytos apribotos bandomosios reglamentavimo aplinkos veikimu;

(c) teikia nuomones, rekomendacijas arba rašytines pastabas klausimais, susijusiais su šio reglamento įgyvendinimu, visų pirma dėl

i) techninių specifikacijų arba esamų standartų, susijusių su III antraštinės dalies 2 skyriuje nustatytais reikalavimais,

ii) 40 ir 41 straipsniuose nurodytų darniųjų standartų arba bendrųjų specifikacijų naudojimo,

iii) rekomendacinių dokumentų, įskaitant rekomendacijas dėl 71 straipsnyje nurodytų administracinių baudų nustatymo, rengimo.

2 SKYRIUS

NACIONALINĖS KOMPETENTINGOS INSTITUCIJOS

59 straipsnis
Nacionalinių kompetentingų institucijų skyrimas

1. Kiekviena valstybė narė įsteigia arba paskiria nacionalines kompetentingas institucijas šio reglamento taikymui ir įgyvendinimui užtikrinti. Nacionalinių kompetentingų institucijų organizacinė struktūra turi būti tokia, kad būtų užtikrintas jų veiklos ir užduočių objektyvumas ir nešališkumas.

2. Kiekviena valstybė narė iš nacionalinių kompetentingų institucijų paskiria nacionalinę priežiūros instituciją. Nacionalinė priežiūros institucija veikia kaip notifikuojančioji institucija ir rinkos priežiūros institucija, nebent yra organizacinių ir administracinių priežasčių valstybei narei paskirti daugiau nei vieną instituciją.

3. Valstybės narės informuoja Komisiją apie paskirtą instituciją ar institucijas ir, jei taikytina, apie priežastis, kodėl paskirta daugiau nei viena institucija.

4. Valstybės narės užtikrina, kad nacionalinėms kompetentingoms institucijoms būtų suteikta pakankamai finansinių ir žmogiškųjų išteklių jų užduotims pagal šį reglamentą vykdyti. Visų pirma nacionalinės kompetentingos institucijos turi visada turėti pakankamai darbuotojų, kurių kompetencija ir patirtis apima išsamų dirbtinio intelekto technologijų, duomenų ir duomenų kompiuterijos, pagrindinių teisių, rizikos sveikatai ir saugai, taip pat esamų standartų bei teisinių reikalavimų išmanymą.

5. Valstybės narės kasmet praneša Komisijai apie nacionalinių kompetentingų institucijų finansinių ir žmogiškųjų išteklių būklę ir įvertina jų tinkamumą. Komisija perduoda šią informaciją Valdybai aptarti ir galimoms rekomendacijoms pateikti.

6. Komisija padeda nacionalinėms kompetentingoms institucijoms keistis patirtimi.

7. Nacionalinės kompetentingos institucijos gali teikti rekomendacijas ir patarimus dėl šio reglamento įgyvendinimo, be kita ko, smulkiesiems tiekėjams. Kai nacionalinės kompetentingos institucijos ketina dėl DI sistemos teikti rekomendacijų ir patarimų srityse, kurioms taikomi kiti Sąjungos teisės aktai, kai tinkama, konsultuojamasi su nacionalinėmis kompetentingomis institucijomis, kurios už tai atsakingos pagal tuos Sąjungos teisės aktus. Valstybės narės taip pat gali įsteigti vieną ryšių palaikymo centrą ryšiams su veiklos vykdytojais palaikyti.

8. Kai Sąjungos institucijos, agentūros ir įstaigos patenka į šio reglamento taikymo sritį, Europos duomenų apsaugos priežiūros pareigūnas veikia kaip kompetentinga jų priežiūros institucija.

VII ANTRAŠTINĖ DALIS

ATSKIRŲ DIDELĖS RIZIKOS DI SISTEMŲ ES DUOMENŲ BAZĖ

60 straipsnis
Atskirų didelės rizikos DI sistemų ES duomenų bazė

1. Komisija, bendradarbiaudama su valstybėmis narėmis, sukuria ir tvarko ES duomenų bazę, kurioje laikoma 2 dalyje nurodyta informacija, susijusi su 6 straipsnio 2 dalyje nurodytomis pagal 51 straipsnį įregistruotomis didelės rizikos DI sistemomis.
2. VIII priede nurodytus duomenis į ES duomenų bazę įrašo tiekėjai. Komisija jiems teikia techninę ir administracinę paramą.
3. ES duomenų bazėje esanti informacija yra prieinama visuomenei.
4. ES duomenų bazėje saugomi tik tokie asmens duomenys, kurie yra būtini informacijai pagal šį reglamentą rinkti ir tvarkyti. Ta informacija apima fizinių asmenų, atsakingų už sistemos registravimą ir turinčių teisinius įgaliojimus atstovauti tiekėjui, vardus, pavardes ir kontaktinius duomenis.
5. Komisija yra ES duomenų bazės valdytoja. Ji taip pat užtikrina, kad tiekėjams būtų teikiama tinkama techninė ir administracinė parama.

VIII ANTRAŠTINĖ DALIS

PRIEŽIŪRA PO PATEIKIMO RINKAI, DALIJIMASIS INFORMACIJA IR RINKOS PRIEŽIŪRA

1 SKYRIUS

PRIEŽIŪRA PO PATEIKIMO RINKAI

61 straipsnis
Tiekėjų vykdoma priežiūra po pateikimo rinkai ir didelės rizikos DI sistemų priežiūros po pateikimo rinkai planas

1. Tiekėjai nustato priežiūros po pateikimo rinkai sistemą ir ją dokumentuoja tokiu būdu, kuris yra proporcingas dirbtinio intelekto technologijų pobūdžiui ir didelės rizikos DI sistemos keliamai rizikai.
2. Pagal priežiūros po pateikimo rinkai sistemą aktyviai ir sistemingai renkami, dokumentuojami ir analizuojami atitinkami naudotojų pateikti arba iš kitų šaltinių surinkti duomenys apie didelės rizikos DI sistemų veikimo efektyvumą per visą jų gyvavimo laikotarpį; ji taip pat leidžia tiekėjui įvertinti, ar DI sistemos nuolat atitinka III antraštinės dalies 2 skyriuje nustatytus reikalavimus.
3. Priežiūros po pateikimo rinkai sistema grindžiama priežiūros po pateikimo rinkai planu. Priežiūros po pateikimo rinkai planas yra vienas iš IV priede nurodytų techninių dokumentų. Komisija priima įgyvendinimo aktą, kuriame nustatomos išsamios nuostatos dėl priežiūros po pateikimo rinkai plano šablono ir į planą įtrauktinų elementų sąrašo.

4. Didelės rizikos DI sistemų, kurioms taikomi II priede nurodyti teisės aktai, atveju, jeigu pagal tuos teisės aktus priežiūros po pateikimo rinkai sistema ir planas jau nustatyti, į tą sistemą ir planą atitinkamai įtraukiami 1, 2 ir 3 dalyse nurodyti elementai.

Pirma pastraipa taip pat taikoma III priedo 5 punkto b papunktyje nurodytoms didelės rizikos DI sistemoms, kurias rinkai pateikė arba pradėjo naudoti kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES.

2 SKYRIUS

DALIJIMASIS INFORMACIJA APIE INCIDENTUS IR VEIKIMO SUTRIKIMUS

62 straipsnis

Pranešimas apie didelius incidentus ir veikimo sutrikimus

1. Apie visus didelius incidentus ar didelės rizikos DI sistemų veikimo sutrikimus, kuriais pažeidžiami įpareigojimai pagal Sąjungos teisę, kuriais siekiama apsaugoti pagrindines teises, Sąjungos rinkai pateiktų didelės rizikos DI sistemų tiekėjai praneša valstybių narių, kuriose įvyko tas incidentas ar pažeidimas, rinkos priežiūros institucijoms.

   Pranešta turi būti iš karto tiekėjui nustačius priežastinį ryšį tarp DI sistemos ir incidento ar veikimo sutrikimo arba pagrįstą tokio ryšio tikimybę ir bet kuriuo atveju ne vėliau kaip per 15 dienų nuo tos dienos, kurią tiekėjas sužino apie didelį incidentą arba veikimo sutrikimą.

2. Gavusi pranešimą apie įpareigojimų pagal Sąjungos teisę, kuriais siekiama apsaugoti pagrindines teises, pažeidimą, rinkos priežiūros institucija informuoja 64 straipsnio 3 dalyje nurodytas nacionalines valdžios institucijas ar įstaigas. Siekdama palengvinti 1 dalyje nustatytų įpareigojimų laikymąsi Komisija parengia specialias gaires. Tos gairės pateikiamos ne vėliau kaip per 12 mėnesių nuo šio reglamento įsigaliojimo dienos.

3. III priedo 5 punkto b papunktyje nurodytų didelės rizikos DI sistemų, kurias rinkai pateikia arba pradeda naudoti tiekėjai, kurie yra kredito įstaigos, kurių veikla reglamentuojama Direktyva 2013/36/ES, ir didelės rizikos DI sistemų, kurios yra priemonių, kurioms taikomas Reglamentas (ES) 2017/745 ir Reglamentas (ES) 2017/746, saugos komponentai arba pačios yra tokios priemonės, atveju pranešama tik apie tuos didelius incidentus ar veikimo sutrikimus, kuriais pažeidžiami įpareigojimai pagal Sąjungos teisę, kuriais siekiama apsaugoti pagrindines teises.

3 SKYRIUS

VYKDYMO UŽTIKRINIMAS

63 straipsnis

Rinkos priežiūra ir Sąjungos rinkoje esančių DI sistemų kontrolė

1. DI sistemoms, kurios patenka į šio reglamento taikymo sritį, taikomas Reglamentas (ES) 2019/1020. Tačiau siekiant veiksmingai užtikrinti šio reglamento vykdymą laikoma, kad:

(a) nuorodos į ekonominės veiklos vykdytoją pagal Reglamentą (ES) 2019/1020 apima visus šio reglamento III antraštinės dalies 3 skyriuje nurodytus veiklos vykdytojus;

(b) nuorodos į gaminį pagal Reglamentą (ES) 2019/1020 apima visas DI sistemas, kurioms taikomas šis reglamentas.

2. Nacionalinė priežiūros institucija reguliariai praneša Komisijai atitinkamos rinkos priežiūros veiklos rezultatus. Nacionalinė priežiūros institucija nedelsdama praneša Komisijai ir atitinkamoms nacionalinėms konkurencijos institucijoms visą vykdant rinkos priežiūros veiklą nustatytą informaciją, kuri gali būti svarbi taikant Sąjungos konkurencijos taisykles reglamentuojančius teisės aktus.

3. Didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi II priedo A skirsnyje išvardyti teisės aktai, atveju įgyvendinant šį reglamentą rinkos priežiūros institucija yra pagal tuos teisės aktus paskirta institucija, atsakinga už rinkos priežiūros veiklą.

4. DI sistemų, kurias rinkai teikia, pradeda naudoti arba naudoja finansų įstaigos, kurių veiklą reglamentuoja Sąjungos teisės aktai dėl finansinių paslaugų, atveju įgyvendinant šį reglamentą rinkos priežiūros institucija yra atitinkama institucija, pagal tuos teisės aktus atsakinga už tų įstaigų finansinę priežiūrą.

5. Jei 1 punkto a papunktyje nurodytos DI sistemos naudojamos teisėsaugos tikslais (III priedo 6 ir 7 punktai), įgyvendindamos šį reglamentą valstybės narės rinkos priežiūros institucijomis paskiria kompetentingas duomenų apsaugos priežiūros institucijas pagal Direktyvą (ES) 2016/680 arba Reglamentą 2016/679 arba nacionalines kompetentingas institucijas, prižiūrinčias teisėsaugos, imigracijos ar prieglobsčio institucijų, pradedančių naudoti arba naudojančių tas sistemas, veiklą.

6. Jeigu Sąjungos institucijos, agentūros ir įstaigos patenka į šio reglamento taikymo sritį, Europos duomenų apsaugos priežiūros pareigūnas veikia kaip jų rinkos priežiūros institucija.

7. Valstybės narės sudaro palankias sąlygas koordinuoti pagal šį reglamentą paskirtų rinkos priežiūros institucijų ir kitų atitinkamų nacionalinių institucijų ar įstaigų, prižiūrinčių, kaip taikomi II priede išvardyti Sąjungos derinamieji teisės aktai ar kiti Sąjungos teisės aktai, kurie gali būti svarbūs III priede nurodytoms didelės rizikos DI sistemoms, veiklą.

64 straipsnis
Prieiga prie duomenų ir dokumentų

1. Savo veiklą vykdančioms rinkos priežiūros institucijoms suteikiama visapusiška prieiga prie tiekėjo naudojamų mokymo, validavimo ir bandymo duomenų rinkinių, be kita ko, naudojantis programų sąsajomis (API) arba kitomis tinkamomis techninėmis ar nuotolinę prieigą užtikrinančiomis priemonėmis.

2. Jeigu reikia įvertinti didelės rizikos DI sistemos atitiktį III antraštinės dalies 2 skyriuje nustatytiems reikalavimams, pateikus pagrįstą prašymą rinkos priežiūros institucijoms suteikiama prieiga prie DI sistemos pirminio kodo.

3. Nacionalinės valdžios institucijos arba įstaigos, prižiūrinčios, kaip laikomasi įpareigojimų pagal Sąjungos teisę, kuriais siekiama apsaugoti pagrindines teises, kai naudojamos III priede nurodytos didelės rizikos DI sistemos, arba užtikrinančios tų įpareigojimų laikymąsi, turi teisę prašyti visų pagal šį reglamentą parengtų ar

saugomų dokumentų ir gauti prie jų prieigą, kai ta prieiga yra būtina pareigoms pagal jų įgaliojimus vykdyti neperžengiant jų jurisdikcijos ribų. Atitinkama valdžios institucija ar įstaiga apie tokį prašymą informuoja atitinkamos valstybės narės rinkos priežiūros instituciją.

4. Per 3 mėnesius nuo šio reglamento įsigaliojimo dienos kiekviena valstybė narė nustato 3 dalyje nurodytas valdžios institucijas ar įstaigas ir jų sąrašą viešai paskelbia nacionalinės priežiūros institucijos svetainėje. Valstybės narės pateikia sąrašą Komisijai ir visoms kitoms valstybėms narėms ir nuolat jį atnaujina.

5. Jeigu 3 dalyje nurodytų dokumentų nepakanka, kad būtų galima nustatyti, ar buvo pažeistas įpareigojimas pagal Sąjungos teisę, kuriuo siekiama apsaugoti pagrindines teises, 3 dalyje nurodyta valdžios institucija arba įstaiga gali pateikti rinkos priežiūros institucijai motyvuotą prašymą organizuoti didelės rizikos DI sistemos bandymus techninėmis priemonėmis. Rinkos priežiūros institucija per pagrįstą laikotarpį nuo prašymo pateikimo dienos suorganizuoja bandymus glaudžiai bendradarbiaudama su prašančiąja valdžios institucija ar įstaiga.

6. Visa informacija ir dokumentai, kuriuos 3 dalyje nurodytos nacionalinės valdžios institucijos ar įstaigos gavo pagal šio straipsnio nuostatas, tvarkomi laikantis 70 straipsnyje nustatytų konfidencialumo įpareigojimų.

65 straipsnis

Nacionalinio lygmens riziką keliančioms DI sistemoms taikoma procedūra

1. Riziką kelianti DI sistema laikoma Reglamento (ES) 2019/1020 3 straipsnio 19 punkte apibrėžtu pavojų keliančiu gaminiu, jei ji kelia riziką asmenų sveikatai ar saugai arba pagrindinių teisių apsaugai.

2. Jeigu valstybės narės rinkos priežiūros institucija turi pakankamų priežasčių manyti, kad DI sistema kelia 1 dalyje nurodytą riziką, ji atlieka atitinkamos DI sistemos atitikties visiems šiame reglamente nustatytiems reikalavimams ir įpareigojimams vertinimą. Kai kyla rizika pagrindinių teisių apsaugai, rinkos priežiūros institucija taip pat informuoja atitinkamas 64 straipsnio 3 dalyje nurodytas nacionalines valdžios institucijas ar įstaigas. Atitinkami veiklos vykdytojai prireikus bendradarbiauja su 64 straipsnio 3 dalyje nurodytomis rinkos priežiūros institucijomis ir kitomis nacionalinėmis valdžios institucijomis ar įstaigomis.

   Jeigu atlikdama vertinimą rinkos priežiūros institucija nustato, kad DI sistema neatitinka šiame reglamente nustatytų reikalavimų ir įpareigojimų, ji nedelsdama reikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų reikiamų taisomųjų veiksmų, kad užtikrintų DI sistemos atitiktį, pašalintų DI sistemą iš rinkos arba ją atšauktų per pagrįstą laikotarpį, kurį ji nustato atsižvelgdama į nustatytos rizikos pobūdį.

   Rinkos priežiūros institucija apie tai informuoja atitinkamą notifikuotąją įstaigą. Antroje pastraipoje nurodytoms priemonėms taikomas Reglamento (ES) 2019/1020 18 straipsnis.

3. Jei rinkos priežiūros institucija mano, kad neatitikties esama ne tik jos nacionalinėje teritorijoje, ji informuoja Komisiją ir kitas valstybes nares apie vertinimo rezultatus ir veiksmus, kurių jos nurodymu turi imtis veiklos vykdytojas.

4. Veiklos vykdytojas užtikrina, kad visų tinkamų taisomųjų veiksmų būtų imtasi dėl visų susijusių DI sistemų, kurias jis patiekė rinkai visoje Sąjungoje.

5. Jeigu per 2 dalyje nurodytą laikotarpį su DI sistema susijusios veiklos vykdytojas nesiima tinkamų taisomųjų veiksmų, rinkos priežiūros institucija imasi visų tinkamų laikinųjų priemonių, kad būtų uždraustas arba apribotas DI sistemos tiekimas jos nacionalinei rinkai, gaminys būtų pašalintas iš rinkos arba atšauktas. Apie tokias priemones ta institucija nedelsdama informuoja Komisiją ir kitas valstybes nares.

6. Teikiant 5 dalyje nurodytą informaciją pateikiami visi turimi duomenys, visų pirma – duomenys, kurių reikia reikalavimų neatitinkančiai DI sistemai identifikuoti, DI sistemos kilmė, įtariamos neatitikties ir keliamos rizikos pobūdis, taikomų nacionalinių priemonių pobūdis ir trukmė, taip pat atitinkamo veiklos vykdytojo pateikti argumentai. Visų pirma rinkos priežiūros institucijos nurodo, ar neatitiktis sietina su viena ar daugiau iš šių priežasčių:

   (a) DI sistema neatitinka III antraštinės dalies 2 skyriuje nustatytų reikalavimų;

   (b) 40 ir 41 straipsniuose nurodyti darnieji standartai arba bendrosios specifikacijos, kuriais remiantis daryta atitikties prielaida, turi trūkumų.

7. Valstybių narių, išskyrus procedūrą inicijavusią valstybę narę, rinkos priežiūros institucijos nedelsdamos praneša Komisijai ir kitoms valstybėms narėms apie visas priemones, kurių ėmėsi, ir pateikia visą turimą papildomą informaciją, susijusią su atitinkamos DI sistemos neatitiktimi, ir, jei nesutinka su nacionaline priemone, apie kurią pranešta, savo prieštaravimus.

8. Jeigu per tris mėnesius nuo 5 dalyje nurodytos informacijos gavimo nei valstybė narė, nei Komisija nepareiškia prieštaravimo dėl laikinosios priemonės, kurios ėmėsi valstybė narė, ta priemonė laikoma pagrįsta. Tai nedaro poveikio atitinkamo veiklos vykdytojo procesinėms teisėms pagal Reglamento (ES) 2019/1020 18 straipsnį.

9. Visų valstybių narių rinkos priežiūros institucijos užtikrina, kad atitinkamam gaminiui nedelsiant būtų taikomos tinkamos ribojamosios priemonės, pvz., gaminys būtų pašalintas iš rinkos.

66 straipsnis
Sąjungos apsaugos procedūra

1. Jeigu per tris mėnesius nuo 65 straipsnio 5 dalyje nurodyto pranešimo gavimo kuri nors valstybė narė pareiškia prieštaravimų dėl priemonės, kurios ėmėsi kita valstybė narė, arba jeigu Komisija mano, kad priemonė prieštarauja Sąjungos teisei, Komisija nedelsdama pradeda konsultacijas su atitinkama valstybe nare ir veiklos vykdytoju ar vykdytojais ir tą nacionalinę priemonę įvertina. Remdamasi to vertinimo rezultatais, Komisija per devynis mėnesius nuo 65 straipsnio 5 dalyje nurodyto pranešimo dienos nusprendžia, ar nacionalinė priemonė yra pagrįsta, ir apie tokį sprendimą praneša atitinkamai valstybei narei.

2. Jeigu nacionalinė priemonė laikoma pagrįsta, visos valstybės narės imasi priemonių, būtinų užtikrinti, kad reikalavimų neatitinkanti DI sistema būtų pašalinta iš jų rinkos, ir atitinkamai informuoja Komisiją. Jeigu nacionalinė priemonė laikoma nepagrįsta, atitinkama valstybė narė tą priemonę pašalina.

3. Jei nacionalinė priemonė laikoma pagrįsta, o DI sistemos neatitiktis siejama su darniųjų standartų arba bendrųjų specifikacijų, nurodytų šio reglamento 40 ir 41 straipsniuose, trūkumais, Komisija taiko Reglamento (ES) Nr. 1025/2012 11 straipsnyje numatytą procedūrą.

67 straipsnis

Riziką keliančios reikalavimus atitinkančios DI sistemos

1. Jeigu atlikusi vertinimą pagal 65 straipsnį valstybės narės rinkos priežiūros institucija nustato, kad, nors DI sistema atitinka šio reglamento reikalavimus, ji kelia riziką žmonių sveikatai ar saugai, įpareigojimų pagal Sąjungos arba nacionalinę teisę, kuriais siekiama apsaugoti pagrindines teises, laikymuisi ar kitiems viešojo intereso apsaugos aspektams, ji reikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų tinkamų priemonių užtikrinti, kad rinkai pateikta arba pradėta naudoti atitinkama DI sistema nebekeltų tokis rizikos, pašalintų DI sistemą iš rinkos arba ją atšauktų per tokį pagrįstą laikotarpį, kurį ji nustato atsižvelgdama į rizikos pobūdį.

2. Tiekėjas arba kiti atitinkami veiklos vykdytojai užtikrina, kad taisomųjų veiksmų dėl visų susijusių DI sistemų, kurias jie patiekė rinkai visoje Sąjungoje, būtų imtasi per 1 dalyje nurodytos valstybės narės rinkos priežiūros institucijos nustatytą terminą.

3. Valstybė narė nedelsdama informuoja Komisiją ir kitas valstybes nares. Ta informacija apima visus turimus duomenis, visų pirma nurodomi atitinkamai DI sistemai identifikuoti būtini duomenys, DI sistemos kilmė ir tiekimo grandinė, keliamos rizikos pobūdis ir taikomų nacionalinių priemonių pobūdis ir trukmė.

4. Komisija nedelsdama pradeda konsultacijas su valstybėmis narėmis ir atitinkamu veiklos vykdytoju ir įvertina priimtas nacionalines priemones. Remdamasi to vertinimo rezultatais Komisija nusprendžia, ar priemonė pagrįsta, ar ne, ir prireikus pasiūlo tinkamų priemonių.

5. Komisija savo sprendimą skiria valstybėms narėms.

68 straipsnis

Oficiali neatitiktis

1. Jeigu valstybės narės rinkos priežiūros institucija nustato vieną iš toliau nurodytų faktų, ji reikalauja, kad atitinkamas tiekėjas pašalintų nustatytą neatitiktį:

   (a) atitikties ženklu ženklinta pažeidžiant 49 straipsnį;

   (b) nebuvo ženklinama atitikties ženklu;

   (c) neparengta ES atitikties deklaracija;

   (d) ES atitikties deklaracija parengta netinkamai;

   (e) nebuvo pažymėta atitikties vertinimo procedūroje dalyvaujančios notifikuotosios įstaigos identifikaciniu numeriu (jei taikoma).

2. Jeigu 1 dalyje nurodyta neatitiktis nepašalinama, atitinkama valstybė narė imasi visų tinkamų priemonių, kuriomis apribojamas ar uždraudžiamas didelės rizikos DI sistemos tiekimas rinkai arba užtikrinama, kad ji būtų atšaukta arba pašalinta iš rinkos.

IX ANTRAŠTINĖ DALIS

ELGESIO KODEKSAI

69 straipsnis
Elgesio kodeksai

1. Komisija ir valstybės narės skatina ir padeda rengti elgesio kodeksus, kuriais siekiama skatinti savanorišką III antraštinės dalies 2 skyriuje nustatytų reikalavimų taikymą DI sistemoms (išskyrus didelės rizikos DI sistemas), remiantis techninėmis specifikacijomis ir sprendimais, kurie yra tinkamos priemonės atitikčiai tokiems reikalavimams užtikrinti atsižvelgiant į numatytąją sistemų paskirtį.

2. Komisija ir Valdyba skatina ir padeda rengti elgesio kodeksus, kuriais siekiama skatinti savanorišką reikalavimų, susijusių, pavyzdžiui, su aplinkosauginiu tvarumu, neįgaliesiems skirta prieiga, suinteresuotųjų subjektų dalyvavimu projektuojant ir kuriant DI sistemas ir kūrimo grupių įvairove, taikymą DI sistemoms, remiantis aiškiais tikslais ir tų tikslų pasiekimui įvertinti skirtais pagrindiniais veiklos rodikliais.

3. Elgesio kodeksus gali rengti atskiri DI sistemų tiekėjai arba jiems atstovaujančios organizacijos, arba ir vieni, ir kiti, be kita ko, įtraukdami naudotojus, suinteresuotuosius subjektus ir jiems atstovaujančias organizacijas. Elgesio kodeksai gali būti taikomi vienai ar daugiau DI sistemų, atsižvelgiant į atitinkamų sistemų numatytosios paskirties panašumą.

4. Komisija ir Valdyba, skatindamos ir padėdamos rengti elgesio kodeksus, atsižvelgia į konkrečius smulkiųjų tiekėjų ir startuolių interesus ir poreikius.

X ANTRAŠTINĖ DALIS

KONFIDENCIALUMAS IR SANKCIJOS

70 straipsnis
Konfidencialumas

1. Šį reglamentą taikančios nacionalinės kompetentingos institucijos ir notifikuotosios įstaigos užtikrina informacijos ir duomenų, kuriuos jos gavo vykdydamos savo užduotis ir veiklą, konfidencialumą, kad būtų apsaugoti:

   (a) intelektinės nuosavybės teisės ir fizinio ar juridinio asmens konfidenciali verslo informacija ar komercinės paslaptys, įskaitant šaltinio kodą, išskyrus Direktyvos 2016/943 dėl neatskleistos praktinės patirties ir verslo informacijos (komercinių paslapčių) apsaugos nuo neteisėto gavimo, naudojimo ir atskleidimo 5 straipsnyje nurodytais atvejais;

   (b) veiksmingas šio reglamento įgyvendinimas, visų pirma susijęs su patikrinimais, tyrimais arba auditu; c) visuomenės ir nacionalinio saugumo interesai;

   (c) baudžiamojo ar administracinio proceso vientisumas.

2. Nedarant poveikio 1 daliai, informacija, kuria konfidencialiai tarpusavyje keičiasi nacionalinės kompetentingos institucijos ir nacionalinės kompetentingos institucijos ir Komisija, neatskleidžiama iš anksto nepasikonsultavus su ją pateikusia nacionaline

kompetentinga institucija ir naudotoju, kai III priedo 1, 6 ir 7 punktuose nurodytas didelės rizikos DI sistemas naudoja teisėsaugos, imigracijos ar prieglobsčio institucijos, jei toks atskleidimas keltų grėsmę visuomenės ir nacionalinio saugumo interesams.

Kai teisėsaugos, imigracijos ar prieglobsčio institucijos yra didelės rizikos DI sistemų, nurodytų III priedo 1, 6 ir 7 punktuose, tiekėjos, IV priede nurodyti techniniai dokumentai laikomi tų institucijų patalpose. Tos institucijos užtikrina, kad, pateikusios prašymą, atitinkamai 63 straipsnio 5 ir 6 dalyse nurodytos rinkos priežiūros institucijos galėtų nedelsdamos susipažinti su dokumentais arba gauti jų kopijas. Susipažinti su tais dokumentais ar jų kopijomis leidžiama tik rinkos priežiūros institucijos darbuotojams, turintiems atitinkamo lygio asmens patikimumo pažymėjimą.

3. 1 ir 2 dalimis nedaromas poveikis Komisijos, valstybių narių ir notifikuotųjų įstaigų teisėms ir pareigoms keistis informacija bei platinti įspėjimus, taip pat atitinkamų šalių pareigoms teikti informaciją pagal valstybių narių baudžiamąją teisę.

4. Komisija ir valstybės narės prireikus gali keistis konfidencialia informacija su trečiųjų valstybių, su kuriomis jos yra sudariusios dvišalius arba daugiašalius konfidencialumo susitarimus, kuriais užtikrinamas reikiamas konfidencialumo lygis, reguliavimo institucijomis.

71 straipsnis
Sankcijos

1. Laikydamosi šiame reglamente nustatytų sąlygų, valstybės narės nustato taisykles dėl sankcijų, įskaitant administracines baudas, taikytinų už šio reglamento pažeidimus, ir imasi visų būtinų priemonių užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Jomis visų pirma atsižvelgiama į smulkiųjų tiekėjų ir startuolių interesus ir jų ekonominį gyvybingumą.

2. Valstybės narės praneša apie tas taisykles ir priemones Komisijai ir nedelsdamos ją informuoja apie visus vėlesnius joms įtakos turinčius pakeitimus.

3. Administracinės baudos iki 30 000 000 EUR arba, jei pažeidėjas yra bendrovė, iki 6 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų) skiriamos už šiuos pažeidimus:

   (a) 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo nesilaikymą;

   (b) DI sistemos neatitiktį 10 straipsnyje nustatytiems reikalavimams.

4. Už DI sistemos neatitiktį bet kokiems šio reglamento reikalavimams ar įpareigojimams, išskyrus nustatytuosius 5 ir 10 straipsniuose, skiriamos administracinės baudos iki 20 000 000 EUR arba, jei pažeidėjas yra bendrovė, iki 4 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų).

5. Už neteisingos, neišsamios ar klaidinančios informacijos pateikimą notifikuotosioms įstaigoms ir nacionalinėms kompetentingoms institucijoms atsakant į jų prašymą taikomos administracinės baudos iki 10 000 000 EUR arba, jei pažeidėjas yra bendrovė, iki 2 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų).

6. Sprendžiant dėl administracinės baudos dydžio kiekvienu konkrečiu atveju deramai atsižvelgiama į visas reikšmingas konkrečios situacijos aplinkybes ir į šiuos dalykus:

   (a) pažeidimo pobūdį, sunkumą, trukmę ir jo pasekmes;

   (b) ar kitos rinkos priežiūros institucijos jau skyrė administracines baudas tam pačiam veiklos vykdytojui už tą patį pažeidimą;

   (c) pažeidimą padariusio veiklos vykdytojo dydį ir rinkos dalį.

7. Kiekviena valstybė narė nustato taisykles, reglamentuojančias, ar ir kokiu mastu administracinės baudos gali būti skiriamos toje valstybėje narėje įsisteigusioms valdžios institucijomis ir įstaigoms.

8. Priklausomai nuo valstybių narių teisinės sistemos, administracines baudas reglamentuojančios taisyklės gali būti taikomos taip, kad tose valstybėse narėse baudas atitinkamai skirtų kompetentingi nacionaliniai teismai ar kitos įstaigos. Tokių taisyklių taikymo poveikis tose valstybėse narėse turi būti lygiavertis.

72 straipsnis

Administracinės baudos Sąjungos institucijoms, agentūroms ir įstaigoms

1. Europos duomenų apsaugos priežiūros pareigūnas gali skirti administracines baudas Sąjungos institucijoms, agentūroms ir įstaigoms, kurioms taikomas šis reglamentas. Sprendžiant, ar skirti administracinę baudą ir koks turėtų būti jos dydis, kiekvienu konkrečiu atveju deramai atsižvelgiama į visas reikšmingas konkrečios situacijos aplinkybes ir į šiuos dalykus:

   (a) pažeidimo pobūdį, sunkumą, trukmę ir jo pasekmes;

   (b) bendradarbiavimą su Europos duomenų apsaugos priežiūros pareigūnu siekiant ištaisyti pažeidimą ir sumažinti galimą neigiamą pažeidimo poveikį, taip pat visų priemonių, kurias Europos duomenų apsaugos priežiūros pareigūnas anksčiau nurodė taikyti Sąjungos institucijai, agentūrai ar įstaigai dėl to paties dalyko, taikymą;

   (c) bet kokius anksčiau Sąjungos institucijos, agentūros ar įstaigos padarytus panašius pažeidimus.

2. Už šiuos pažeidimus skiriamos iki 500 000 EUR administracinės baudos:

   (a) 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo nesilaikymą;

   (b) DI sistemos neatitiktį 10 straipsnyje nustatytiems reikalavimams.

3. Už DI sistemos neatitiktį bet kokiems šio reglamento reikalavimams ar įpareigojimams, išskyrus nustatytuosius 5 ir 10 straipsniuose, skiriamos administracinės baudos iki 250 000 EUR.

4. Prieš priimdamas sprendimus pagal šį straipsnį, Europos duomenų apsaugos priežiūros pareigūnas suteikia Sąjungos institucijai, agentūrai ar įstaigai, dėl kurios jis pradėjo procesą, galimybę būti išklausytai su galimu pažeidimu susijusiais klausimais. Europos duomenų apsaugos priežiūros pareigūnas savo sprendimus grindžia tik tais elementais ir aplinkybėmis, dėl kurių atitinkamos šalys galėjo pateikti pastabas. Skundo pateikėjai, jei jų yra, turi būti įtraukti į procesą.

5. Proceso metu turi būti visapusiškai gerbiama šalių teisė į gynybą. Joms turi būti suteikta teisė susipažinti su Europos duomenų apsaugos priežiūros pareigūno byla,

atsižvelgiant į fizinių asmenų ar įmonių teisėtą interesą, kad būtų apsaugoti jų asmens duomenys ar verslo paslaptys.

6. Lėšos, surinktos paskyrus šiame straipsnyje numatytas baudas, laikomos Sąjungos bendrojo biudžeto pajamomis.

XI ANTRAŠTINĖ DALIS

DELEGUOTIEJI ĮGALIOJIMAI IR KOMITETO PROCEDŪRA

73 straipsnis
Įgaliojimų delegavimas

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. 4 straipsnyje, 7 straipsnio 1 dalyje, 11 straipsnio 3 dalyje, 43 straipsnio 5 ir 6 dalyse ir 48 straipsnio 5 dalyje nurodyti deleguotieji įgaliojimai Komisijai suteikiami neribotam laikotarpiui nuo [*šio reglamento įsigaliojimo diena*].

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 4 straipsnyje, 7 straipsnio 1 dalyje, 11 straipsnio 3 dalyje, 43 straipsnio 5 ir 6 dalyse ir 48 straipsnio 5 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Jis įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

4. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.

5. Pagal 4 straipsnį, 7 straipsnio 1 dalį, 11 straipsnio 3 dalį, 43 straipsnio 5 ir 6 dalis ir 48 straipsnio 5 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per tris mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas trimis mėnesiais.

74 straipsnis
Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

XII ANTRAŠTINĖ DALIS

BAIGIAMOSIOS NUOSTATOS

75 straipsnis
Reglamento (EB) Nr. 300/2008 pakeitimas

Reglamento (EB) Nr. 300/2008 4 straipsnio 3 dalis papildoma šia pastraipa:

„Priimant išsamias priemones, susijusias su dirbtinio intelekto sistemų, apibrėžtų Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, saugumo įrangos patvirtinimo ir naudojimo techninėmis specifikacijomis ir procedūromis, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

76 straipsnis
Reglamento (ES) Nr. 167/2013 pakeitimas

Reglamento (ES) Nr. 167/2013 17 straipsnio 5 dalis papildoma šia pastraipa:

„Priimant deleguotuosius aktus pagal pirmą pastraipą dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

77 straipsnis
Reglamento (ES) Nr. 168/2013 pakeitimas

Reglamento (ES) Nr. 168/2013 22 straipsnio 5 dalis papildoma šia pastraipa:

„Priimant deleguotuosius aktus pagal pirmą pastraipą dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

78 straipsnis
Direktyvos 2014/90/ES pakeitimas

Direktyvos 2014/90/ES 8 straipsnis papildomas šia dalimi:

„4. Vykdydama veiklą pagal 1 dalį ir priimdama technines specifikacijas ir bandymo standartus pagal 2 ir 3 dalis, susijusius su dirbtinio intelekto sistemomis, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, Komisija atsižvelgia į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

79 straipsnis
Direktyvos (ES) 2016/797 pakeitimas

Direktyvos (ES) 2016/797 5 straipsnis papildomas šia dalimi:

„12. Priimant deleguotuosius aktus pagal 1 dalį ir įgyvendinimo aktus pagal 11 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

80 straipsnis
Reglamento (ES) 2018/858 pakeitimas

Reglamento (ES) 2018/858 5 straipsnis papildomas šia dalimi:

„4. Priimant deleguotuosius aktus pagal 3 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

81 straipsnis
Reglamento (ES) 2018/1139 pakeitimas

Reglamentas (ES) 2018/1139 iš dalies keičiamas taip:

1. 17 straipsnis papildomas šia dalimi:

„3. Nedarant poveikio 2 daliai, priimant įgyvendinimo aktus pagal 1 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [*dėl dirbtinio intelekto*]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

2. 19 straipsnis papildomas šia dalimi:

„4. Priimant deleguotuosius aktus pagal 1 ir 2 dalis dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Reglamente (ES) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“

3. 43 straipsnis papildomas šia dalimi:

„4. Priimant įgyvendinimo aktus pagal 1 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Reglamente (ES) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“

4. 47 straipsnis papildomas šia dalimi:

„3. Priimant deleguotuosius aktus pagal 1 ir 2 dalis dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Reglamente (ES) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“

5. 57 straipsnis papildomas šia dalimi:

„Priimant tuos įgyvendinimo aktus dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Reglamente (ES) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“

6. 58 straipsnis papildomas šia dalimi:

„3. Priimant deleguotuosius aktus pagal 1 ir 2 dalis dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Reglamente (ES) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“

82 straipsnis
Reglamento (ES) 2019/2144 pakeitimas

Reglamento (ES) 2019/2144 11 straipsnis papildomas šia pastraipa:

„3. Priimant įgyvendinimo aktus pagal 2 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, apibrėžti Europos Parlamento ir Tarybos reglamente (ES) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

* Reglamentas (ES) YYY/XX [dėl dirbtinio intelekto] (OL ...).“

83 straipsnis
Rinkai jau pateiktos ar pradėtos naudoti DI sistemos

1. Šis reglamentas netaikomas DI sistemoms, kurios yra didelės apimties IT sistemų, nustatytų IX priede nurodytais teisės aktais ir pateiktų rinkai arba pradėtų naudoti iki *[12 mėnesių po 85 straipsnio 2 dalyje nurodytos šio reglamento taikymo pradžios dienos]*, komponentai, išskyrus atvejus, kai dėl tų teisės aktų pakeitimo ar dalinio keitimo iš esmės pasikeičia atitinkamos DI sistemos ar DI sistemų modelis arba numatytoji paskirtis.

   Atliekant kiekvienos IX priede nurodytais teisės aktais nustatytos didelės apimties IT sistemos vertinimą pagal tuos atitinkamus aktus, atsižvelgiama, kai taikytina, į šiame reglamente nustatytus reikalavimus.

2. Šis reglamentas taikomas didelės rizikos DI sistemoms (išskyrus nurodytąsias 1 dalyje), kurios buvo pateiktos rinkai arba pradėtos naudoti iki [*85 straipsnio 2 dalyje nurodyta šio reglamento taikymo pradžios diena*], tik tuo atveju, jei nuo tos dienos iš esmės pasikeičia tų sistemų modelis arba numatytoji paskirtis.

84 straipsnis
Vertinimas ir peržiūra

1. Komisija kartą per metus nuo šio reglamento įsigaliojimo įvertina poreikį iš dalies pakeisti III priede pateiktą sąrašą.

2. Ne vėliau kaip [*treji metai po 85 straipsnio 2 dalyje nurodytos šio reglamento taikymo pradžios dienos*] ir vėliau kas ketverius metus Komisija teikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitas. Ataskaitos skelbiamos viešai.

3. 2 dalyje nurodytose ataskaitose ypatingas dėmesys skiriamas šiems dalykams:

(a) nacionalinių kompetentingų institucijų finansinių ir žmogiškųjų išteklių būklei, kad jos galėtų veiksmingai vykdyti joms pagal šį reglamentą pavestas užduotis;

(b) sankcijų, visų pirma 71 straipsnio 1 dalyje nurodytų administracinių baudų, kurias valstybės narės taiko už šio reglamento nuostatų pažeidimus, būklei.

4. Iki [*treji metai po 85 straipsnio 2 dalyje nurodytos šio reglamento taikymo pradžios dienos*] ir vėliau kas ketverius metus Komisija įvertina elgesio kodeksų poveikį ir veiksmingumą skatinant III antraštinės dalies 2 skyriuje nustatytų reikalavimų ir galbūt papildomų reikalavimų taikymą DI sistemoms, išskyrus didelės rizikos DI sistemas.

5. Įgyvendinant 1–4 dalis Valdyba, valstybės narės ir nacionalinės kompetentingos institucijos Komisijos prašymu jai teikia informaciją.

6. Atlikdama 1–4 dalyse nurodytus vertinimus ir peržiūras, Komisija atsižvelgia į Valdybos, Europos Parlamento, Tarybos, taip pat kitų susijusių įstaigų ar šaltinių nuomones ir išvadas.

7. Prireikus Komisija pateikia tinkamus pasiūlymus iš dalies pakeisti šį reglamentą, visų pirma atsižvelgdama į technologinius pokyčius ir informacinės visuomenės pažangą.

85 straipsnis
Įsigaliojimas ir taikymas

1. Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

2. Šis reglamentas taikomas nuo [24 mėnesiai po šio reglamento įsigaliojimo].

3. Nukrypstant nuo 2 dalies:

(a) III antraštinės dalies 4 skyrius ir VI antraštinė dalis taikomi nuo [*trys mėnesiai po šio reglamento įsigaliojimo*];

(b) 71 straipsnis taikomas nuo [dvylika mėnesių po šio reglamento įsigaliojimo].

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

1.2. Atitinkama (-os) politikos sritis (-ys)

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

1.4.2. Konkretus (-ūs) tikslas (-ai)

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

1.4.4. Veiklos rezultatų rodikliai

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

1.5.3. Panašios patirties išvados

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

1.5.5 Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

1.7. Numatytas (-i) valdymo būdas (-ai)

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

2.2. Valdymo ir kontrolės sistema

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

3.2.2. Numatomas veiklos asignavimais finansuojamas išvedinys

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis pajamoms

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Europos Parlamento ir Tarybos reglamentas, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai

1.2. Atitinkama (-os) politikos sritis (-ys)

Ryšių tinklai, turinys ir technologijos;

Vidaus rinka, pramonė, verslumas ir MVĮ;

Poveikis biudžetui susijęs su naujais Komisijai paskirtais uždaviniais, įskaitant paramą ES DI valdybai;

Veikla: Europos skaitmeninės ateities formavimas.

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

X **nauju veiksmu**

☐ **nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai**[64]

☐ **esamo veiksmo galiojimo pratęsimu**

☐ **veiksmas, perorientuotas į naują veiksmą**

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

Bendras intervencijos tikslas – užtikrinti tinkamą bendrosios rinkos veikimą sukuriant sąlygas patikimam dirbtiniam intelektui kurti ir naudoti Sąjungoje.

1.4.2. Konkretus (-ūs) tikslas (-ai)

1 konkretus tikslas

Nustatyti būtent su DI sistemomis susijusius reikalavimus ir pareigas visiems vertės grandinės dalyviams, siekiant užtikrinti, kad rinkai pateikiamos ir naudojamos DI sistemos būtų saugios ir derėtų su galiojančiais pagrindines teises reglamentuojančiais aktais ir Sąjungos vertybėmis.

2 konkretus tikslas

Užtikrinti teisinį tikrumą, siekiant sudaryti palankesnes sąlygas investicijoms ir inovacijoms DI srityje aiškiai nurodant, kokių esminių reikalavimų, pareigų, taip pat atitikties ir reikalavimų laikymosi procedūrų būtina paisyti pateikiant DI sistemą Sąjungos rinkai arba ją naudojant.

3 konkretus tikslas

Gerinti valdymą ir veiksmingą dabartinių teisės aktų, kuriais reglamentuojamos pagrindinės teisės ir DI sistemoms taikytini saugos reikalavimai, vykdymo

[64] Kaip nurodyta Finansinio reglamento 54 straipsnio 2 dalies a arba b punkte.

užtikrinimą suteikiant naujus įgaliojimus, išteklius ir atitinkamoms institucijoms nustatant aiškias taisykles dėl atitikties vertinimo ir *ex post* stebėsenos procedūrų, taip pat dėl valdymo ir priežiūros užduočių nacionaliniu ir ES lygmenimis paskirstymo.

4 konkretus tikslas

Palengvinti bendrosios teisėtų, saugių ir patikimų DI prietaikų rinkos plėtrą ir užkirsti kelią rinkos susiskaidymui imantis ES veiksmų, siekiant nustatyti būtiniausius reikalavimus DI sistemoms, kurios turi būti pateikiamos Sąjungos rinkai ir joje naudojamos, laikantis galiojančių pagrindines teises ir saugumą reglamentuojančių aktų.

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

DI paslaugų teikėjams turėtų būti naudingas būtiniausių, tačiau aiškių reikalavimų rinkinys, nes tai padėtų sukurti teisinį tikrumą ir užtikrinti prieigą prie visos bendrosios rinkos.

DI naudotojams turėtų būti naudingas teisinis tikrumas, susijęs su tuo, kad jų perkamos didelės rizikos DI sistemos atitinka Europos įstatymus ir vertybes.

Vartotojams turėtų būti naudinga mažesnė jų saugumo ar pagrindinių teisių pažeidimo rizika.

1.4.4. Veiklos rezultatų rodikliai

Nurodyti pasiūlymo (iniciatyvos) įgyvendinimo stebėjimo rodiklius.

1 rodiklis

Didelių incidentų arba DI veikimo atvejų, laikomų dideliu incidentu arba pagrindinių teisių įpareigojimų pažeidimu, skaičius (kas pusmetį) pagal prietaikų sritis, išreikštas a) absoliučiais terminais, b) kaip įdiegtų prietaikų dalis ir c) kaip susijusių piliečių dalis.

2 rodiklis

a) Iš viso ES investicijų į DI (metinis rodiklis)

b) Iš viso investicijų į DI pagal valstybę narę (metinis rodiklis)

c) Įmonių, naudojančių DI, dalis (metinis rodiklis)

c) MVĮ, naudojančių DI, dalis (metinis rodiklis)

a ir b punktų dydžiai bus apskaičiuojami remiantis oficialiais šaltiniais ir lyginami su privačiai įverčiais

c ir d punktų dydžiai bus nustatomi renkant informaciją atliekant įprastas įmonių apklausas

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

Reglamentas turėtų būti visa apimtimi taikomas praėjus pusantrų metų nuo jo priėmimo. Tačiau valdymo struktūros elementai iki to laiko jau turi būti nustatyti. Visų pirma valstybės narės turi paskirtas esamas institucijas ir (arba) anksčiau sukūrė naujas institucijas, atliekančias teisės akte nustatytas užduotis, be to, reikėtų sukurti veikiančią ES DI valdybą. Iki taikymo pradžios Europos DI sistemų duomenų bazė turi visiškai veikti. Todėl kartu su patvirtinimo procesu būtina kurti duomenų bazę, kad ji būtų sukurta iki reglamento įsigaliojimo.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Gali būti, kad bus kuriamos skirtingos nacionalinės taisyklės, kurios stabdys gausų DI sistemų tiekimą ES ir nebus naudingos veiksmingai užtikrinant pagrindinių teisių ir Sąjungos vertybių įvairiose valstybėse narėse saugumą ir apsaugą. Bendri ES teisėkūros veiksmai DI srityje galėtų duoti postūmį vidaus rinkai ir turi didelį potencialą suteikti Europos pramonei konkurencinį pranašumą pasauliniu mastu ir masto ekonomiką, kurios pavieniui negali pasiekti atskiros valstybės narės.

1.5.3. Panašios patirties išvados

Elektroninės komercijos direktyvoje 2000/31/EB numatoma pagrindinė bendrosios rinkos veikimo ir skaitmeninių paslaugų priežiūros sistema, sukuriama bazinė bendrojo valstybių narių bendradarbiavimo mechanizmo struktūra, iš principo apimanti visus skaitmeninėms paslaugoms keliamus reikalavimus. Įvertinus direktyvą paaiškėjo keli šio bendradarbiavimo mechanizmo trūkumai, įskaitant tokius svarbius procedūrinius aspektus kaip tai, jog nebuvo nustatyti aiškūs valstybių narių reagavimo terminai ir apskritai nebūdavo reaguojama į partnerių prašymus. Ilgainiui tai padarė neigiamą poveikį valstybių narių pasitikėjimui sprendžiant problemas, susijusias su tarpvalstybinių skaitmeninių paslaugų teikėjais. Iš direktyvos vertinimo matyti, kad Europos lygmeniu reikia apibrėžti skirtingus taisyklių ir reikalavimų rinkinius. Dėl šios priežasties įgyvendinant konkrečias šiame reglamente nustatytas prievoles reikėtų konkretaus ES lygmens bendradarbiavimo mechanizmo su valdymo struktūra, kuria ES lygmeniu būtų užtikrinamas konkrečių atsakingų įstaigų veiklos koordinavimas.

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

Reglamente, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai, apibrėžiama nauja bendra DI sistemoms taikomų reikalavimų sistema, kuri yra gerokai platesnio užmojo, palyginti su dabartiniuose teisės aktuose nustatyta sistema. Todėl šiuo pasiūlymu reikia sukurti naują nacionalinio ir Europos lygmenų reglamentavimo ir koordinavimo funkciją.

Dėl galimos sinergijos su kitomis atitinkamomis priemonėmis pažymėtina, kad notifikuojančiųjų institucijų vaidmenį nacionaliniu lygmeniu gali atlikti nacionalinės institucijos, vykdančios panašias funkcijas pagal kitus ES reglamentus.

Be to, didindamas pasitikėjimą DI ir taip skatindamas investicijas į DI kūrimą ir priėmimą, pasiūlymas papildo Skaitmeninės Europos programą, pagal kurią DI sklaidos skatinimas yra vienas iš jos prioritetų.

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

Numatoma perskirstyti darbuotojus. Kitos išlaidos bus dengiamos iš Skaitmeninės Europos programos paketo, atsižvelgiant į tai, kad šio reglamento tikslu, t. y. užtikrinti patikimą DI, tiesiogiai prisidedama prie vieno iš pagrindinių Skaitmeninės Europos programos tikslų, t. y. paspartinti DI kūrimą ir diegimą Europoje.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☐ **trukmė ribota**

– ☐ galioja nuo MMMM [MM DD] iki MMMM [MM DD],

– ☐ įsipareigojimų asignavimų finansinis poveikis nuo MMMM iki MMMM, o mokėjimų asignavimų – nuo MMMM iki MMMM.

X **trukmė neribota**

– Įgyvendinimo pradinis laikotarpis – nuo vieni / dveji (bus nuspręsta) metai,

– vėliau – visuotinis taikymas.

1.7. Numatytas (-i) valdymo būdas (-ai)[65]

X **Tiesioginis valdymas**, vykdomas Komisijos:

– ☐ padalinių, įskaitant Sąjungos delegacijų darbuotojus;

– ☐ vykdomųjų įstaigų.

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

☐ **Netiesioginis valdymas**, biudžeto vykdymo užduotis pavedant:

– ☐ trečiosioms valstybėms arba jų paskirtoms įstaigoms;

– ☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

– ☐ EIB ir Europos investicijų fondui;

– ☐ įstaigoms, nurodytoms Finansinio reglamento 70 ir 71 straipsniuose;

– ☐ viešosios teisės subjektams;

– ☐ privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta teikti viešąsias paslaugas, jeigu jos pateikia pakankamas finansines garantijas;

– ☐ valstybės narės privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamas finansines garantijas;

– ☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

– *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

Pastabos

65 Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

Nurodyti dažnumą ir sąlygas.

Reglamentas bus peržiūrimas ir įvertinamas praėjus penkeriems metams nuo jo įsigaliojimo. Pagrindinius nustatytus faktus Komisija pateiks Europos Parlamentui, Tarybai bei Europos ekonomikos ir socialinių reikalų komitetui.

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

Reglamentu parengiama nauja politika dėl suderintų taisyklių dėl dirbtinio intelekto sistemų tiekimo vidaus rinkoje, kartu užtikrinant pagarbą saugumui ir pagrindinėms teisėms. Pagal šias naujas taisykles reikalaujama užtikrinti nuoseklaus tarpvalstybinio pareigų taikymo pagal šį reglamentą mechanizmą šiuo tikslu sudarant naują patariamąją grupę, koordinuojančią nacionalinių institucijų veiklą.

Siekiant vykdyti šias naujas užduotis, būtina užtikrinti, kad Komisijos tarnybos turėtų pakankamai išteklių. Remiantis skaičiavimais, naujojo reglamento vykdymo užtikrinimui reikės 10 etato ekvivalentų *à regime* (5 etato ekvivalentų Valdybos veiklai ir 5 etato ekvivalentų Europos duomenų apsaugos priežiūros pareigūnui, kuris veikia kaip DI sistemų Europos Sąjungos paskirta notifikuojančioji įstaiga).

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Siekiant užtikrinti, kad Valdybos nariai turėtų galimybę atlikti pagrįstas analizes remdamiesi faktiniais įrodymais, numatoma, kad Valdybą turėtų remti Komisijos administracinė struktūra, taip pat numatoma sukurti ekspertų grupę, kuri prireikus teiktų papildomas specialiąsias žinias.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

Dėl susitikimų išlaidų, atsižvelgiant į mažą kiekvieno sandorio vertę (pvz., į susitikimą siunčiamo delegato kelionės išlaidų grąžinimas), atrodo, kad standartinės kontrolės procedūros yra pakankamos. Dėl duomenų bazių kūrimo pažymėtina, kad CNECT GD, vykdydamas centralizuotų viešųjų pirkimų veiklą, sutarties skyrimui taiko nustatytą griežtą vidaus kontrolės sistemą.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

Papildomi asignavimai, reikalingi šiam reglamentui, bus padengiami esamomis Komisijai taikomomis sukčiavimo prevencijos priemonėmis.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA[66]	ELPA šalių[67]	šalių kandidačių[68]	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą
7	20 02 06 Administracinės išlaidos	NDA	NE	NE	NE	NE
1	02 04 03 DEP Dirbtinis intelektas	DA	TAIP	NE	NE	NE
1	02 01 30 01 Rėmimo išlaidos Skaitmeninės Europos programai	NDA	TAIP	NE	NE	NE

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimų išlaidoms santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– X Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos	1	

[66] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

[67] ELPA – Europos laisvosios prekybos asociacija.

[68] Valstybių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių kandidačių.

išlaidų kategorija		

GD: Ryšių tinklų, turinio ir technologijų (CNECT)				**2022** metai	**2023** metai	**2024** metai	**2025** metai	**2026** metai	**2027** metai[69]	**IŠ VISO**	
• Veiklos asignavimai											
Biudžeto eilutė[70] 02 04 03		Įsipareigojimai	(1a)		1,000						**1,000**
		Mokėjimai	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Biudžeto eilutė		Įsipareigojimai	(1b)								
		Mokėjimai	(2b)								
Administracinio pobūdžio asignavimai, finansuojami iš konkrečių programų paketo lėšų[71]											
Biudžeto eilutė 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
IŠ VISO asignavimų CNECT GD		Įsipareigojimai	= 1a + 1b + 3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Mokėjimai	= 2a + 2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

• IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)		1,000						**1,000**

69 Orientacinis ir priklauso nuo biudžeto prieinamumo.

70 Pagal oficialią biudžeto nomenklatūrą.

71 Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

	Mokėjimai	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
IŠ VISO asignavimų pagal daugiametės finansinės programos 1 IŠLAIDŲ KATEGORIJĄ	Įsipareigojimai	= 4 + 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Mokėjimai	= 5 + 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Jei pasiūlymas (iniciatyva) daro poveikį kelioms išlaidų kategorijoms, pakartokite pirmiau pateiktą dalį:

• IŠ VISO veiklos asignavimų (visose veiklos išlaidų kategorijose)	Įsipareigojimai	(4)								
	Mokėjimai	(5)								
• IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų (visose veiklos išlaidų kategorijose)		(6)								
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–6 IŠLAIDŲ KATEGORIJAS (Orientacinė suma)	Įsipareigojimai	= 4 + 6								
	Mokėjimai	= 5 + 6								

Daugiametės finansinės programos išlaidų kategorija	**7**	„Administracinės išlaidos“

Šią dalį pildyti naudojant administracinio pobūdžio biudžeto duomenų lentelę, kuri pirmiausia bus pateikta finansinės teisės akto pasiūlymo pažymos priede (Vidaus taisyklių V priedas) ir įkelta į DECIDE tarnybų tarpusavio konsultacijoms.

mln. EUR (tūkstantųjų tikslumu)

		2023 metai	**2024** metai	**2025** metai	**2026** metai	**2027** metai	**Po 2027**[72]	**IŠ VISO**
GD: Ryšių tinklų, turinio ir technologijų (CNECT)								
• Žmogiškieji ištekliai		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Kitos administracinės išlaidos		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
IŠ VISO CNECT GD	**Asignavimai**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Europos duomenų apsaugos priežiūros pareigūnas								
• Žmogiškieji ištekliai		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Kitos administracinės išlaidos								
IŠ VISO EDAPP	**Asignavimai**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
IŠ VISO asignavimų pagal daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ	(Iš viso įsipareigojimų = Iš viso mokėjimų)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

mln. EUR (tūkstantųjų tikslumu)

	2022 metai	**2023** metai	**2024** metai	**2025** metai	**2026** metai	**2027** metai		**IŠ VISO**

[72] Visi skaičiai šioje skiltyje yra apytiksliai ir priklauso nuo programų tęstinumo ir asignavimų skyrimo.

IŠ VISO asignavimų pagal daugiametės finansinės programos 1–7 IŠLAIDŲ KATEGORIJAS	Įsipareigojimai		2,770	1,770	1,770	1,770	1,770		**9,850**
	Mokėjimai		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Numatomas veiklos asignavimais finansuojamas išvedinys

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir išvedinius ⇩			**2022** metai		**2023** metai		**2024** metai		**2025** metai		**2026** metai		**2027** metai		Po **2027**[73]		**IŠ VISO**	
	IŠVEDINIAI																	
	Rūšis	Vidutinės sąnaudos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Nr.	Sąnau-dos	Bend-ras skai-čius	Iš viso sąnaudų
1 KONKRETUS TIKSLAS [74]…																		
Duomenų bazė					1	1,000	1		1		1		1		1	0,100	1	1,000
Susitikimai –					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Komunikacijos veikla					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
1 konkretaus tikslo tarpinė suma																		
2 KONKRETUS TIKSLAS ...																		
– Išvedinys																		
2 konkretaus tikslo tarpinė suma																		
IŠ VISO					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Visi skaičiai šioje skiltyje yra apytiksliai ir priklauso nuo programų tęstinumo ir asignavimų skyrimo

[74] Kaip apibūdinta 1.4.2 skirsnyje. „Konkretus (-ūs) tikslas (-ai) ...“.

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– X Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2022 metai	**2023** metai	**2024** metai	**2025** metai	**2026** metai	**2027** metai	**Kasmet po 2027**[75]	**IŠ VISO**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA								
Žmogiškieji ištekliai		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Kitos administracinės išlaidos		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ[76]								
Žmogiškieji ištekliai								
Kitos administracinio pobūdžio išlaidos		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinę sumą		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
IŠ VISO		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų veiksmui valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

[75] Visi skaičiai šioje skiltyje yra apytiksliai ir priklauso nuo programų tęstinumo ir asignavimų skyrimo.

[76] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

3.2.3.1. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– X Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą surašyti etatų vienetais

.		**2023** metai	**2024** metai	**2025** metai	**2026** metai	**2027** metai	**Po 2027**[77]	
•Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)								
20 01 02 01 (Komisijos būstinė ir atstovybės)		10	10	10	10	10	10	
20 01 02 03 (Delegacijos)								
01 01 01 01 (Netiesioginiai moksliniai tyrimai)								
01 01 01 11 (Tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
• Išorės darbuotojai (etatų vienetais): FTE)[78]								
20 02 01 (CA, SNE, INT finansuojami iš bendrojo biudžeto)								
20 02 03 (CA, LA, SNE, INT ir JPD atstovybėse)								
XX 01 xx **yy zz** [79]	- būstinėje							
	- delegacijose							
01 01 01 02 (CA, SNE, INT – netiesioginiai moksliniai tyrimai)								
01 01 01 12 (CA, SNE, INT – tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
IŠ VISO		**10**	**10**	**10**	**10**	**10**	**10**	

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Tikimasi, kad EDAPP suteiks pusę reikalingų išteklių.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	Kad būtų surengti iš viso 13–16 susitikimų, parengtos ataskaitos, tęsiamas politinis darbas, pvz., susijęs su būsimais didelės rizikos DI prietaikų sąrašo pakeitimais, ir palaikomi ryšiai su valstybių narių institucijomis, reikės keturių AD etato ekvivalentų ir 1 AST etato ekvivalento. Už ES institucijų sukurtas DI sistemas atsako Europos duomenų apsaugos priežiūros pareigūnas. Remiantis ankstesne patirtimi, galima numatyti, kad EDAPP pareigoms pagal teisės akto projektą įvykdyti prireiks 5 AD etato ekvivalentų.
Išorės darbuotojai	

[77] Visi skaičiai šioje skiltyje yra apytiksliai ir priklauso nuo programų tęstinumo ir asignavimų skyrimo.

[78] CA – sutartininkas („Contract Staff“), LA – vietos darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („agency staff“), JPD – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

[79] Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

Pasiūlyme (iniciatyvoje):

– X Galima visiškai finansuoti perskirstant asignavimą atitinkamoje daugiametės finansinės programos (DFP) išlaidų kategorijoje.

Perprogramavimas nereikalingas.

– ☐ Reikia panaudoti nepaskirstytą maržą pagal atitinkamą DFP išlaidų kategoriją ir (arba) specialias priemones, kaip apibrėžta DFP reglamente.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes bei sumas ir pasiūlytas naudoti priemones.

– ☐ Reikia persvarstyti DFP.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes ir sumas.

3.2.5. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

– X nenumatyta bendro su trečiosiomis šalimis finansavimo

– ☐ numatytas trečiųjų šalių bendras finansavimas apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

	N metai[80]	**N+1** metai	**N+2** metai	**N+3** metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			Iš viso
Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

[80] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pvz., 2021). Atitinkamai pakeiskite vėlesnius metus.

3.3. Numatomas poveikis pajamoms

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

  – ☐ kitoms pajamoms

  – ☐ kitoms pajamoms

  – nurodyti, jei pajamos priskirtos išlaidų eilutėms ☐

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[81]						
		N metai	**N+1** metai	**N+2** metai	**N+3** metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
……. straipsnis								

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-oms) daromas poveikis.

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).

[81] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 proc. surinkimo sąnaudų.