EUROPOS SĄJUNGA

EUROPOS PARLAMENTAS **TARYBA**

Briuselis, 2024 m. gegužės 14 d.
(OR. en)

2021/0106(COD) **PE-CONS 24/24**

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

TEISĖS AKTAI IR KITI DOKUMENTAI

Dalykas:	EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas)

EUROPOS PARLAMENTO IR TARYBOS
REGLAMENTAS (ES) 2024/…

… m. … … d.

kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir
iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013,
(ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir
direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828)
(Dirbtinio intelekto aktas)

(Tekstas svarbus EEE)

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[1],

atsižvelgdami į Europos Centrinio Banko nuomonę[2],

atsižvelgdami į Regionų komiteto nuomonę[3],

laikydamiesi įprastos teisėkūros procedūros[4],

---

1 OL C 517, 2021 12 22, p. 56.
2 OL C 115, 2022 3 11, p. 5.
3 OL C 97, 2022 2 28, p. 60.
4 2024 m. kovo 13 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir … m. … … d. Tarybos sprendimas.

kadangi:

(1) šio reglamento paskirtis – pagerinti vidaus rinkos veikimą nustatant vienodą teisinę sistemą, visų pirma skirtą dirbtinio intelekto sistemų (toliau – DI sistemos) kūrimui, pateikimui rinkai, pradėjimui naudoti ir naudojimui Sąjungoje paisant Sąjungos vertybių, skatinti į žmogų orientuoto ir patikimo dirbtinio intelekto (toliau – DI) įsisavinimą kartu užtikrinant aukšto lygio sveikatos, saugumo, pagrindinių teisių, įtvirtintų Europos Sąjungos pagrindinių teisių chartijoje (toliau – Chartija), apsaugą, įskaitant demokratijos, teisinės valstybės ir aplinkos apsaugą, saugoti nuo žalingo DI sistemų poveikio Sąjungoje ir remti inovacijas. Šiuo reglamentu užtikrinamas laisvas DI grindžiamų prekių ir paslaugų tarpvalstybinis judėjimas, taip užkertant kelią valstybėms narėms nustatyti apribojimus DI sistemų kūrimui, teikimui rinkai ir naudojimui, nebent tai aiškiai leidžiama pagal šį reglamentą;

(2) šis reglamentas turėtų būti taikomas vadovaujantis Chartijoje įtvirtintomis Sąjungos vertybėmis, palengvinti fizinių asmenų, įmonių, demokratijos, teisės viršenybės ir aplinkos apsaugą, kartu skatinti inovacijas ir užimtumą ir užtikrinti, kad Sąjunga taptų patikimo DI įsisavinimo lydere;

(3) DI sistemos gali būti lengvai įdiegiamos labai įvairiuose ekonomikos sektoriuose ir lengvai plisti visose visuomenės grupėse, taip pat tarpvalstybiniu mastu, ir jos gali lengvai cirkuliuoti visoje Sąjungoje. Tam tikros valstybės narės jau išnagrinėjo galimybę priimti nacionalines taisykles, siekdamos užtikrinti, kad DI būtų patikimas bei saugus ir kuriamas bei naudojamas laikantis su pagrindinėmis teisėmis susijusių pareigų. Skirtingos nacionalinės taisyklės gali lemti vidaus rinkos susiskaidymą ir gali sumažinti teisinį tikrumą DI sistemas kuriantiems, importuojantiems ar naudojantiems veiklos vykdytojams. Todėl, siekiant užtikrinti patikimą DI, visoje Sąjungoje reikėtų užtikrinti nuoseklią ir aukšto lygio apsaugą ir užkirsti kelią skirtumams, trukdantiems DI sistemoms ir susijusiems gaminiams ir paslaugoms laisvai cirkuliuoti vidaus rinkoje, taip pat jų inovacijoms, diegimui ir įsisavinimui vidaus rinkoje, nustatant vienodas pareigas veiklos vykdytojams ir garantuojant vienodą svarbių viešojo intereso tikslų 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, taikomais nuotoliniam biometriniam tapatybės nustatymui teisėsaugos tikslu, DI sistemų naudojimu fizinių asmenų rizikos vertinimams teisėsaugos tikslu ir biometrinio kategorizavimo DI sistemų naudojimu teisėsaugos tikslu, tikslinga, kad šio reglamento pagrindas tų konkrečių taisyklių atžvilgiu būtų SESV 16 straipsnis; Atsižvelgiant į tas konkrečias taisykles ir rėmimusi SESV 16 straipsniu, tikslinga konsultuotis su Europos duomenų apsaugos valdyba;

(4) DI – tai grupė greitai besivystančių technologijų, kurios duoda visokeriopą ekonominę, aplinkosauginę ir visuomeninę naudą įvairiose pramonės šakose ir socialinės veiklos srityse. Patobulinus predikciją, optimizavus operacijas ir išteklių paskirstymą, taip pat personalizavus asmenims ir organizacijoms prieinamus skaitmeninius sprendimus DI naudojimas įmonėms gali suteikti esminių konkurencinių pranašumų ir padėti siekti socialiniu požiūriu ir aplinkai naudingų rezultatų, pavyzdžiui, sveikatos priežiūros, žemės ūkio, maisto saugumo, švietimo ir mokymo, žiniasklaidos, sporto, kultūros, infrastruktūros valdymo, energetikos, transporto ir logistikos, viešųjų paslaugų, saugumo, teisingumo, išteklių ir energijos vartojimo efektyvumo, aplinkos stebėsenos, biologinės įvairovės ir ekosistemų išsaugojimo ir atkūrimo, klimato kaitos švelninimo ir prisitaikymo prie jos srityse;

(5) kartu, priklausomai nuo aplinkybių, susijusių su konkrečiu DI taikymu, naudojimu, ir technologinės plėtros lygmeniu, DI gali kelti riziką ir padaryti žalos viešiesiems interesams ir pagrindinėms teisėms, kurių apsauga užtikrinama Sąjungos teisėje. Tokia žala gali būti turtinė arba neturtinė, įskaitant fizinę, psichologinę, visuomeninę ar ekonominę žalą;

(6) atsižvelgiant į didžiulį poveikį, kurį DI gali daryti visuomenei, ir poreikį didinti pasitikėjimą, labai svarbu, kad DI ir jo reglamentavimo sistema būtų plėtojami vadovaujantis Sąjungos vertybėmis, įtvirtintomis Europos Sąjungos sutarties (toliau – ES sutartis) 2 straipsnyje, pagrindinėmis teisėmis ir laisvėmis, įtvirtintomis Sutartyse ir, pagal ES sutarties 6 straipsnį, Chartijoje. Būtina sąlyga – DI turėtų būti į žmogų orientuota technologija. Ji turėtų būti žmonėms skirta priemonė, kurios pagrindinis tikslas – didinti žmonių gerovę;

(7) siekiant užtikrinti nuoseklią ir aukšto lygio viešųjų interesų, susijusių su sveikata, saugumu ir pagrindinėmis teisėmis, apsaugą, reikėtų nustatyti bendrąsias taisykles, taikomas didelės rizikos DI sistemoms. Tos taisyklės turėtų atitikti Chartiją, būti nediskriminacinės ir atitikti Sąjungos tarptautinės prekybos įsipareigojimus. Jomis taip pat turėtų būti atsižvelgiama į Europos deklaraciją dėl skaitmeninio dešimtmečio skaitmeninių teisių ir principų ir į Aukšto lygio ekspertų grupės dirbtinio intelekto klausimams (toliau – AI HLEG) parengtas patikimo DI etikos gaires;

(8) todėl reikia Sąjungos teisinės sistemos, kuria būtų nustatytos suderintos DI taisyklės, siekiant vidaus rinkoje skatinti kurti, naudoti ir įsisavinti DI, ir kuria tuo pat metu būtų užtikrinta viešųjų interesų, pavyzdžiui, sveikatos ir saugos, aukšto lygio apsauga ir pagrindinių teisių, įskaitant demokratiją, teisinę valstybę ir aplinkosaugą, apsauga, kaip pripažįstama ir saugoma Sąjungos teisėje. Kad toks tikslas būtų pasiektas, reikėtų nustatyti taisykles, kuriomis reglamentuojamas tam tikrų DI sistemų pateikimas rinkai, pradėjimas naudoti ir naudojimas, taip užtikrinant sklandų vidaus rinkos veikimą ir sudarant sąlygas tam, kad laisvo prekių ir paslaugų judėjimo principas suteiktų toms sistemoms naudos. Tos taisyklės turėtų būti aiškios ir tvirtos, kad būtų apsaugotos pagrindinės teisės, jomis turėtų būti remiami nauji novatoriški sprendimai, sudaromos sąlygos sukurti Europos viešųjų ir privačiųjų subjektų, kuriančių Sąjungos vertybes atitinkančias DI sistemas, ekosistemą ir išnaudoti skaitmeninės transformacijos potencialą visuose Sąjungos regionuose. Šiuo reglamentu, kuriuo nustatomos tokios taisyklės, taip pat priemonės, kuriomis remiamos inovacijos, ypatingą dėmesį skiriant mažosioms ir vidutinėms įmonėms (toliau – MVĮ), įskaitant startuolius, remiamas tikslas skatinti europinį į žmogų orientuotą DI ir tikslas pirmauti pasaulyje kuriant saugų, patikimą ir etišką DI , kaip nurodė Europos Vadovų Taryba[5], ir užtikrinama etikos principų apsauga, atsižvelgiant į specialų Europos Parlamento prašymą[6];

---

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

6 2020 m. spalio 20 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos, 2020/2012(INL).

(9) didelės rizikos DI sistemų pateikimui rinkai, pradėjimui naudoti ir naudojimui taikytinos suderintos taisyklės turėtų būti nustatytos taip, kad derėtų su Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008[7], Europos Parlamento ir Tarybos sprendimu 768/2008/EB[8] ir Europos Parlamento ir Tarybos reglamentu (ES) 2019/1020[9] (t. y. naująja teisės aktų sistema). Šiame reglamente nustatytos suderintos taisyklės turėtų būti taikomos visuose sektoriuose ir, laikantis naujosios teisės aktų sistemos, neturėtų daryti poveikio esamiems Sąjungos teisės aktams, visų pirma dėl duomenų apsaugos, vartotojų apsaugos, pagrindinių teisių, užimtumo, darbuotojų apsaugos ir gaminių saugos, kuriuos šis reglamentas papildo. Todėl jokioms teisėms ir teisių gynimo priemonėms, pagal tokius Sąjungos teisės aktus numatytoms vartotojams ir kitiems asmenims, kuriems DI sistemos gali turėti neigiamą poveikį, be kita ko, kiek tai susiję su galimos žalos atlyginimu pagal Tarybos direktyvą 85/374/EEB[10], poveikis nedaromas ir jos visos yra visapusiškai taikomos.

---

7 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

8 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).

9 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 (OL L 169, 2019 6 25, p. 1).

10 1985 m. liepos 25 d. Tarybos direktyva 85/374/EEB dėl valstybių narių įstatymų ir kitų teisės aktų, reglamentuojančių atsakomybę už gaminius su trūkumais, derinimo (OL L 210, 1985 8 7, p. 29).

Be to, užimtumo ir darbuotojų apsaugos srityje šiuo reglamentu neturėtų būti daromas poveikis Sąjungos socialinės politikos teisei ir nacionalinei darbo teisei, atitinkančiai Sąjungos teisę, susijusią su įdarbinimu ir darbo sąlygomis, įskaitant profesinę saugą ir sveikatą ir darbdavių bei darbuotojų santykius. Šiuo reglamentu taip pat neturėtų būti daromas poveikis naudojimuisi valstybėse narėse ir Sąjungos lygmeniu pripažįstamomis pagrindinėmis teisėmis, įskaitant teisę ar laisvę streikuoti arba imtis kitų veiksmų, numatytų konkrečiose valstybių narių darbo santykių sistemose, taip pat derėtis dėl kolektyvinių susitarimų, juos sudaryti ir užtikrinti jų vykdymą ar imtis kolektyvinių veiksmų pagal nacionalinę teisę. Šiuo reglamentu neturėtų būti daroma poveikio nuostatoms, kuriomis siekiama pagerinti darbo skaitmeninėse platformose sąlygas, nustatytoms Europos Parlamento ir Tarybos direktyvoje dėl darbo skaitmeninėse platformose sąlygų gerinimo. Be to, šiuo reglamentu siekiama padidinti tokių esamų teisių ir teisių gynimo priemonių veiksmingumą nustatant konkrečius reikalavimus ir pareigas, be kita ko, susijusius su DI sistemų skaidrumu, techniniais dokumentais ir įrašų tvarkymu. Be to, įvairiems DI vertės grandinėje dalyvaujantiems veiklos vykdytojams pagal šį reglamentą nustatytos pareigos turėtų būti taikomos nedarant poveikio nacionalinei teisei, atitinkančiai Sąjungos teisę, kuria ribojamas tam tikrų DI sistemų naudojimas, kai tokia teisė nepatenka į šio reglamento taikymo sritį arba ja siekiama kitų teisėtų viešojo intereso tikslų nei tie, kurių siekiama šiuo reglamentu. Pavyzdžiui, šiuo reglamentu neturėtų būti daromas poveikis nacionalinei darbo teisei ir nepilnamečių (t. y. jaunesnių nei 18 metų asmenų) apsaugos teisei, atsižvelgiant į JT VTK bendrąją pastabą Nr. 25 (2021) dėl vaikų teisių, susijusiai su skaitmenine aplinka, jei ji nėra konkrečiai taikoma DI sistemoms ir ja siekiama kitų teisėtų viešojo intereso tikslų;

(10) pagrindinė teisė į asmens duomenų apsaugą visų pirma užtikrinama Europos Parlamento ir Tarybos reglamentais (ES) 2016/679[11] ir (ES) 2018/1725[12] ir Europos Parlamento ir Tarybos direktyva (ES) 2016/680[13]. Europos Parlamento ir Tarybos direktyva 2002/58/EB[14] dar papildomai saugomas privatus gyvenimas ir ryšių konfidencialumas, be kita ko, nustatant asmens ir ne asmens duomenų saugojimo galiniuose įrenginiuose ir prieigos prie jų sąlygos. Tais Sąjungos teisės aktais nustatomas tvaraus ir atsakingo duomenų tvarkymo pagrindas, įskaitant atvejus, kai duomenų rinkiniuose yra asmens ir ne asmens duomenų derinys. Šiuo reglamentu nesiekiama daryti poveikio esamų Sąjungos teisės aktų, kuriais reglamentuojamas asmens duomenų tvarkymas, taikymui, įskaitant nepriklausomų priežiūros institucijų, kompetentingų stebėti, kaip laikomasi tų priemonių, užduotis ir įgaliojimus.

---

11 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).

12 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).

13 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 (OL L 119, 2016 5 4, p. 89).

14 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

Juo taip pat nedaromas poveikis DI sistemų tiekėjų ir diegėjų, kaip duomenų valdytojų ar tvarkytojų, pareigoms, kylančioms iš Sąjungos arba nacionalinės teisės dėl asmens duomenų apsaugos, tiek, kiek DI sistemų projektavimas, kūrimas ar naudojimas apima asmens duomenų tvarkymą. Taip pat tikslinga paaiškinti, kad duomenų subjektai ir toliau naudojasi visomis teisėmis ir garantijomis, kurios jiems suteikiamos pagal tokią Sąjungos teisę, įskaitant teises, susijusias tik su automatizuotu individualių sprendimų priėmimu, įskaitant profiliavimą. Šiuo reglamentu nustatytos DI sistemų pateikimo rinkai, pradėjimo naudoti ir naudojimo suderintos taisyklės turėtų palengvinti veiksmingą įgyvendinimą ir sudaryti sąlygas naudotis duomenų subjektų teisėmis ir kitomis teisių gynimo priemonėmis, garantuojamomis pagal Sąjungos teisę dėl asmens duomenų ir kitų pagrindinių teisių apsaugos;

(11) šiuo reglamentu neturėtų būti daromas poveikis nuostatoms dėl tarpininkavimo paslaugų teikėjų atsakomybės, išdėstytoms Europos Parlamento ir Tarybos reglamente (ES) 2022/2065[15];

[15] 2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas) (OL L 277, 2022 10 27, p. 1).

(12) DI sistemos sąvoka šiame reglamente turėtų būti aiškiai apibrėžta ir glaudžiai suderinta su tarptautinių organizacijų, dirbančių DI srityje, veikla, siekiant užtikrinti teisinį tikrumą, sudaryti palankesnes sąlygas konvergencijai tarptautiniu lygmeniu ir plačiam pripažinimui, kartu suteikiant lankstumo prisitaikyti prie sparčių technologinių pokyčių šioje srityje. Be to, apibrėžtis turėtų būti grindžiama pagrindinėmis DI sistemų charakteristikomis, pagal kurias ji skiriasi nuo paprastesnių įprastų programinės įrangos sistemų ar programavimo metodų, ir neturėtų apimti sistemų, kurios grindžiamos tik fizinių asmenų nustatytomis taisyklėmis, skirtomis automatiškai vykdyti operacijas. Pagrindinė DI sistemų savybė yra jų gebėjimas daryti išvadas. Šis gebėjimas daryti išvadas yra procesas, kuriam vykstant gaunami išvediniai, pavyzdžiui, predikcijos, turinys, rekomendacijos ar sprendimai, kurie gali turėti įtakos fizinei ir virtualiai aplinkai, ir tai, kad DI sistemos geba išvesti modelius arba algoritmus (arba juos abu) iš įvedinių ar duomenų. Metodai, leidžiantys daryti išvadas kuriant DI sistemą, apima mašininio mokymosi metodus, pagal kuriuos iš duomenų mokomasi, kaip pasiekti tam tikrus tikslus, ir logika bei žiniomis grindžiamus metodus, kuriuos taikant daromos išvados iš užkoduotų žinių arba atliktinos užduoties simbolinio vaizdavimo. DI sistemos gebėjimas daryti išvadas apima daugiau nei bazinį duomenų apdorojimą ir sudaro sąlygas mokytis, argumentuoti ar modeliuoti. Sąvoka „mašina grindžiamas“ reiškia, kad DI sistemos veikia naudojant mašinas.

Nuoroda į aiškius ar numanomus tikslus pabrėžiama tai, kad DI sistemos gali veikti pagal aiškius nustatytus arba numanomus tikslus. Konkrečiomis aplinkybėmis DI sistemos tikslai gali skirtis nuo numatytos DI sistemos paskirties. Šio reglamento tikslais aplinka turėtų būti suprantama kaip aplinkybės, kuriomis veikia DI sistemos, o DI sistemos sugeneruoti išvediniai atspindi skirtingas DI sistemų atliekamas funkcijas ir apima predikcijas, turinį, rekomendacijas ar sprendimus. DI sistemos projektuojamos taip, kad veiktų įvairiais autonomijos lygmenimis, t. y. kad jų veiksmai būtų tam tikru laipsniu nepriklausomi nuo žmogaus įsitraukimo ir kad jos galėtų veikti be žmogaus įsikišimo. Gebėjimas prisitaikyti, kurį DI sistema galėtų pademonstruoti ją įdiegus, reiškia savarankiško mokymosi pajėgumus, leidžiančius sistemai keistis jos naudojimo metu. DI sistemos gali būti naudojamos atskirai arba kaip gaminio komponentas, nepaisant to, ar sistema yra fiziškai integruota (įterpta) į gaminį ar padeda atlikti gaminio funkciją, tačiau į jį neintegruota (neįterpta);

(13) šiame reglamente nurodyta sąvoka „diegėjas“ turėtų būti aiškinama kaip bet kuris fizinis arba juridinis asmuo, įskaitant valdžios instituciją, agentūrą ar kitą įstaigą, naudojantis DI sistemą pagal savo įgaliojimus, išskyrus atvejus, kai DI sistema naudojama asmeniniais neprofesinės veiklos tikslais. Priklausomai nuo DI sistemos rūšies, sistemos naudojimas gali daryti poveikį ne tik diegėjui, bet ir kitiems asmenims;

(14) šiame reglamente vartojama sąvoka „biometriniai duomenys“ turėtų būti aiškinama atsižvelgiant į biometrinių duomenų sąvoką, apibrėžtą Reglamento (ES) 2016/679 4 straipsnio 14 punkte, Reglamento (ES) 2018/1725 3 straipsnio 18 punkte ir Direktyvos (ES) 2016/680 3 straipsnio 13 punkte. Biometriniai duomenys gali padėti patvirtinti ar nustatyti fizinių asmenų tapatybę arba juos suskirstyti į kategorijas ir atpažinti fizinių asmenų emocijas;

(15) šiame reglamente nurodyta sąvoka „biometrinis tapatybės nustatymas“ turėtų būti apibrėžiama kaip automatinis žmogaus fizinių, fiziologinių ir elgsenos požymių, pvz., veido, akių judėjimo, kūno formos, balso, kalbėsenos, eisenos, laikysenos, pulso dažnumo, kraujo spaudimo, kvapo, klavišų paspaudimų, atpažinimas, siekiant nustatyti asmens tapatybę, palyginant to asmens biometrinius duomenis su informacinėje duomenų bazėje saugomais asmenų biometriniais duomenimis, neatsižvelgiant į tai, ar asmuo davė sutikimą, ar ne. Tai neapima DI sistemų, skirtų naudoti biometriniam tikrinimui, kuris apima autentifikavimą, kurių vienintelis tikslas – patvirtinti, kad konkretus fizinis asmuo yra tas asmuo, kuriuo jis prisistato, ir patvirtinti fizinio asmens tapatybę vieninteliu – prieigos prie paslaugos, prietaiso atrakinimo ar saugaus patekimo į patalpas – tikslu;

(16) šiame reglamente nurodyta sąvoka „biometrinis kategorizavimas“ turėtų būti apibrėžiama kaip fizinių asmenų priskyrimas konkrečioms kategorijoms remiantis jų biometriniais duomenimis. Tokios konkrečios kategorijos gali būti susijusios su tokiais aspektais kaip lytis, amžius, plaukų spalva, akių spalva, tatuiruotės, elgesio ar asmenybės bruožai, kalba, religija, priklausymas tautinei mažumai, seksualinė ar politinė orientacija. Tai neapima tų biometrinio kategorizavimo sistemų, kurios yra tik papildoma savybė, neatsiejamai susijusi su kita komercine paslauga, t. y. savybė, kuri dėl objektyvių techninių priežasčių negali būti naudojama be pagrindinės paslaugos, o tos savybės ar funkcijos integravimas nėra būdas išvengti šio reglamento taisyklių taikymo. Pavyzdžiui, internetinėse prekyvietėse naudojami filtrai, skirti suskirstyti į kategorijas pagal veido bruožus ar kūno savybes, galėtų reikšti tokią papildomą funkciją, nes jie gali būti naudojami tik teikiant pagrindinę paslaugą, kurią sudaro gaminio pardavimas, leidžiant vartotojui pačiam peržiūrėti, kaip atitinkamas gaminys ant jo atrodo, ir padėti vartotojui priimti sprendimą pirkti ar ne. Papildoma funkcija taip pat galėtų būti laikomi filtrai, naudojami teikiant internetines socialinių tinklų paslaugas, kategorizuojantys veido bruožus ar kūno savybes ir skirti tam, kad naudotojai galėtų pridėti ar pakeisti nuotraukas ar vaizdo įrašus, nes tokie filtrai negali būti naudojami be pagrindinės socialinių tinklų paslaugų teikiamos paslaugos – dalijimosi turiniu internete;

(17) šiame reglamente nurodyta nuotolinio biometrinio tapatybės nustatymo sistemos sąvoka turėtų būti apibrėžiama funkciniu požiūriu, kaip DI sistema, skirta fizinių asmenų tapatybei nustatyti, jiems aktyviai nedalyvaujant, paprastai nuotoliniu būdu, palyginant asmens biometrinius duomenis su informacinėje duomenų bazėje esančiais biometriniais duomenimis, nepriklausomai nuo naudojamos konkrečios technologijos, procesų arba biometrinių duomenų rūšies. Tokios nuotolinio biometrinio tapatybės nustatymo sistemos paprastai tam, kad vienu metu būtų galima pastebėti kelis asmenis arba suvokti jų elgesį, kad būtų gerokai lengviau nustatyti asmenų tapatybę jiems aktyviai nedalyvaujant. Tai neapima DI sistemų, skirtų naudoti biometriniam tikrinimui, kuris apima autentifikavimą, kurių vienintelis tikslas – patvirtinti, kad konkretus fizinis asmuo yra tas asmuo, kuriuo jis prisistato, ir patvirtinti fizinio asmens tapatybę vieninteliu – prieigos prie paslaugos, prietaiso atrakinimo ar saugaus patekimo į patalpas – tikslu. Ta išimtis grindžiama tuo, kad tokios sistemos, tikėtina, daro nedidelį poveikį fizinių asmenų pagrindinėms teisėms, palyginti su nuotolinio biometrinio tapatybės nustatymo sistemomis, kurios gali būti naudojamos daugelio asmenų biometriniams duomenims tvarkyti jiems aktyviai nedalyvaujant. Jeigu naudojamos tikralaikės sistemos, biometrinių duomenų rinkimas, lyginimas ir tapatybės nustatymas vyksta momentiškai, beveik momentiškai arba bet kuriuo atveju be didesnės delsos. Šiuo atžvilgiu neturėtų būti jokių galimybių apeiti šio reglamento taisykles dėl tikralaikio atitinkamų DI sistemų naudojimo numatant nedidelę delsą. Tikralaikės sistemos yra susijusios su medžiagos naudojimu tiesiogiai arba beveik tiesiogiai, pavyzdžiui, filmuotos medžiagos, sukurtos naudojant kamerą arba kitą panašią funkciją atliekantį prietaisą, naudojimu. Netikralaikių sistemų atveju, atvirkščiai, 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;

(18) šiame reglamente nurodyta sąvoka „emocijų atpažinimo sistema“ sąvoka turėtų būti apibrėžiama kaip DI sistema, kurios paskirtis – atpažinti arba nuspėti fizinių asmenų emocijas ar ketinimus remiantis jų biometriniais duomenimis. Ši sąvoka apima tokias emocijas ar intencijas kaip laimė, liūdesys, pyktis, nustebimas, bjaurėjimasis, sumišimas, susijaudinimas, gėda, panieka, pasitenkinimas ir linksmumas. Ji neapima fizinių būklių, pavyzdžiui, skausmo ar nuovargio, įskaitant sistemas, naudojamas profesionalių pilotų ar vairuotojų nuovargiui nustatyti, siekiant užkirsti kelią nelaimingiems atsitikimams. Tai taip pat neapima paprasčiausio aiškiai matomų išraiškų, gestų ar judesių nustatymo, išskyrus atvejus, kai tai naudojama emocijoms atpažinti ar nuspėti. Šios išraiškos gali būti paprastos veido išraiškos, pavyzdžiui, suraukti antakiai ar šypsena, arba gestai, pavyzdžiui, plaštakų, rankų ar galvos judesiai, arba asmens balso savybės, pavyzdžiui, pakeltas balsas ar šnibždėjimas;

(19) šiame reglamente sąvoka „viešai prieinama erdvė“ turėtų būti suprantama kaip reiškianti bet kokią fizinę erdvę, prieinamą nenustatytam skaičiui fizinių asmenų ir, neatsižvelgiant į tai, ar ta erdvė priklauso viešam ar privačiam subjektui, neatsižvelgiant į veiklą, kuriai vykdyti ta erdvė gali būti naudojama, – kaip antai, prekyba, pavyzdžiui, parduotuvės, restoranai, kavinės, paslaugos, pavyzdžiui, bankai, profesinė veikla, svetingumo paslaugos, sportas, pavyzdžiui, baseinai, sporto salės, stadionai, transportas, pavyzdžiui, autobusai, metro ir geležinkelio stotys, oro uostai, transporto priemonės, pramogos, pavyzdžiui, kino teatrai, teatrai, muziejai, koncertų ir konferencijų salės), arba laisvalaikio ar kitokia veikla, pavyzdžiui, viešieji keliai ir aikštės, parkai, miškai, žaidimų aikštelės. Erdvė taip pat turėtų būti priskiriama viešai prieinamai erdvei ir tuo atveju, jei, nepaisant galimų pajėgumų ar saugumo apribojimų, tam, kad į ją patektum, taikomos tam tikros iš anksto numatytos sąlygos, kurias gali įvykdyti nenustatytas skaičius asmenų, pvz., reikia įsigyti bilietą ar teisę naudotis transportu, iš anksto registruotis arba būti tam tikro amžiaus. Tačiau erdvė neturėtų būti laikoma viešai prieinama, jei į ją patekti gali tik konkretūs ir apibrėžti fiziniai asmenys pagal Sąjungos arba nacionalinę teisę, tiesiogiai susijusią su viešuoju ar visuomenės saugumu, arba įgaliojimus dėl atitinkamos erdvė turinčiam asmeniui aiškiai išreiškus savo valią. Vien faktinė patekimo galimybė, pavyzdžiui, atrakintos durys ar atviri vartai užtvaroje, nereiškia, kad vieta yra viešai prieinama, jei esama požymių ar aplinkybių, pavyzdžiui, ženklų, kuriais prieiga draudžiama arba ribojama, iš kurių galima spręsti, kad yra kitaip. Įmonių ir gamyklų patalpos, taip pat biurai ir darbo vietos, į kuriuos turėtų patekti tik atitinkami darbuotojai ir paslaugų teikėjai, – tai vietos, kurios nėra viešai prieinamos. Kalėjimai ar pasienio kontrolės zonos neturėtų būti laikomi viešai prieinamomis erdvėmis. Kai kurias kitas erdves gali sudaryti ir viešai prieinamos, ir viešai neprieinamos erdvės, pavyzdžiui, privataus gyvenamojo pastato koridorius, per kurį galima patekti į gydytojo kabinetą, arba oro uostas. Tai netaikoma internetinėms erdvėms, nes jos nėra fizinės erdvės. Tačiau tai, ar atitinkama erdvė yra viešai prieinama, turėtų būti nustatyta kiekvienu konkrečiu atveju atsižvelgiant į konkrečios nagrinėjamos situacijos ypatumus;

(20) siekiant gauti didžiausią DI sistemų teikiamą naudą, kartu apsaugant pagrindines teises, sveikatą ir saugą, ir sudaryti sąlygas demokratinei kontrolei, tiekėjai, diegėjai ir asmenys, kuriems daromas poveikis, turėtų būti raštingi DI srityje, kad žinotų reikiamas sąvokas ir galėtų priimti informacija pagrįstus sprendimus dėl DI sistemų. Tos sąvokos gali skirtis atsižvelgiant į atitinkamas aplinkybes ir gali apimti supratimą apie tinkamą techninių elementų taikymą DI sistemos kūrimo etape, priemones, taikytinas jos naudojimo metu, tinkamus DI sistemos išvedinių aiškinimo būdus, o asmenų, kuriems daromas poveikis, atveju – žinias, būtinas norint suprasti, kokį poveikį jiems darys sprendimai, priimti naudojantis DI. Taikant šį reglamentą, raštingumas DI srityje turėtų suteikti visiems atitinkamiems DI vertės grandinės subjektams įžvalgų, kurių reikia siekiant užtikrinti tinkamą šio reglamento laikymąsi ir vykdymo užtikrinimą. Be to, platus raštingumo DI srityje priemonių įgyvendinimas ir ėmimasis tinkamų tolesnių susijusių veiksmų galėtų padėti gerinti darbo sąlygas ir galiausiai palaikyti patikimo DI konsolidavimą ir inovacijų trajektoriją Sąjungoje. Europos dirbtinio intelekto valdyba (toliau – Valdyba) turėtų remti Komisiją, kad paskatintų raštingumo DI srityje priemones, visuomenės informuotumą ir supratimą apie DI sistemų naudojimo naudą, riziką, apsaugos priemones ir teises bei pareigas. Bendradarbiaudamos su atitinkamais suinteresuotaisiais subjektais, Komisija ir valstybės narės turėtų padėti rengti savanoriškus elgesio kodeksus, kuriais būtų didinamas su DI kūrimu, veikimu ir naudojimu susijusių asmenų raštingumas DI srityje;

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

(22) tam tikros DI sistemos, atsižvelgiant į jų skaitmeninį pobūdį, turėtų patekti į šio reglamento taikymo sritį net jei jos neteikiamos rinkai, nepradedamos naudoti ir nenaudojamos Sąjungoje. Taip, pavyzdžiui, yra tuo atveju, kai Sąjungoje įsisteigęs veiklos vykdytojas sudaro sutartis su trečiojoje valstybėje įsisteigusiu veiklos vykdytoju dėl tam tikrų paslaugų, susijusių su veikla, kurią turi atlikti DI sistema, laikoma didelę riziką keliančia sistema . Šiomis aplinkybėmis veiklos vykdytojo trečiojoje valstybėje 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, nebuvo pradėta naudoti ir nenaudota Sąjungoje, išvedinį, gautą tvarkant tuos duomenis. Siekiant užkirsti kelią šio reglamento reikalavimų apėjimui ir užtikrinti veiksmingą Sąjungoje esančių fizinių asmenų apsaugą, šis reglamentas turėtų būti taikomas ir trečiojoje valstybėje įsisteigusiems DI sistemų tiekėjams ir diegėjams (tiek, kiek šių sistemų sugeneruotus išvedinius ketinama naudoti Sąjungoje).

Vis dėlto, siekiant atsižvelgti į dabartines taisykles ir specialius būsimo 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 Sąjungos arba nacionaliniu lygmeniu sudarytus bendradarbiavimo arba tarptautinius susitarimus teisėsaugos ir teisminio bendradarbiavimo su Sąjunga arba valstybėmis narėmis tikslais, jei atitinkama trečioji valstybė arba tarptautinės organizacijos užtikrina tinkamas su asmenų pagrindinių teisių ir laisvių apsauga susijusias apsaugos priemones. Kai aktualu, tai gali apimti subjektų, kuriems trečiosios valstybės pavedė atlikti konkrečias užduotis remiant tokį teisėsaugos ir teisminį bendradarbiavimą, veiklą. Toks bendradarbiavimo pagrindas arba susitarimai yra nustatyti dvišaliu pagrindu tarp valstybių narių ir trečiųjų valstybių arba tarp Europos Sąjungos, Europolo, kitų Sąjungos agentūrų ir trečiųjų valstybių bei tarptautinių organizacijų. Institucijos, pagal šį reglamentą kompetentingos vykdyti teisėsaugos ir teisminių institucijų priežiūrą, turėtų įvertinti, ar į tą bendradarbiavimo pagrindą ar tarptautinius susitarimus yra įtrauktos tinkamos su asmenų pagrindinių teisių ir laisvių apsauga susijusios apsaugos priemonės. Gavėjos nacionalinės institucijos ir Sąjungos institucijos, įstaigos, organai ir agentūros, kurie Sąjungoje naudojasi tokiais išvediniais, lieka atsakingi už tai, kad jų naudojimasis atitiktų Sąjungos teisę. Kai tie tarptautiniai susitarimai peržiūrimi arba ateityje sudaromi nauji susitarimai, susitariančiosios šalys turėtų dėti visas pastangas, kad tie susitarimai būtų suderinti su šio reglamento reikalavimais;

(23) šis reglamentas taip pat turėtų būti taikomas Sąjungos institucijoms, įstaigoms, organams ir agentūroms, kai jie veikia kaip DI sistemos tiekėjai arba diegėjai;

(24) jei ir tokiu mastu, kokiu DI sistemos pateikiamos rinkai, pradedamos naudoti arba naudojamos, tokios sistemos, su pakeitimais kariniais, gynybos ar nacionalinio saugumo tikslais arba be jų, neturėtų patekti į šio reglamento taikymo sritį, neatsižvelgiant į tai, kokios rūšies subjektas vykdo tą veiklą, pavyzdžiui, ar jis yra viešasis ar privatus subjektas. Kalbant apie karinius ir gynybos tikslus, tokia išimtis pagrįsta tiek atsižvelgiant į ES sutarties 4 straipsnio 2 dalį, tiek į valstybių narių ir bendros Sąjungos gynybos politikos, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius, ypatumus, kuriems taikoma tarptautinė viešoji teisė, todėl tai yra tinkamesnė teisinė sistema DI sistemoms reguliuoti, kai naudojama mirtina jėga, ir kitoms DI sistemoms reguliuoti, kai vykdoma karinė ir gynybos veikla. Kiek tai susiję su nacionalinio saugumo tikslais, išimtis pagrįsta tiek atsižvelgiant į tai, kad pagal ES sutarties 4 straipsnio 2 dalį už nacionalinį saugumą atsakingos išlieka išimtinai valstybės narės, tiek į specifinį nacionalinio saugumo veiklos pobūdį bei veiklos poreikius ir tai veiklai taikomas konkrečias nacionalines taisykles. Vis dėlto, jei DI sistema, sukurta, pateikta rinkai, pradėta naudoti ar naudojama kariniais, gynybos ar nacionalinio saugumo tikslais, yra laikinai arba nuolat naudojama kitais tikslais pavyzdžiui, civiliniais ar humanitariniais tikslais, teisėsaugos ar visuomenės saugumo tikslais, tokia sistema patektų į šio reglamento taikymo sritį. Tokiu atveju subjektas, kuris DI sistemą naudoja ne kariniais, gynybos ar nacionalinio saugumo tikslais, turėtų užtikrinti, kad DI sistema atitiktų šį reglamentą, nebent ji jau atitinka šį reglamentą. Į šio reglamento taikymo sritį patenka DI sistemos, pateiktos rinkai arba pradėtos naudoti tikslu, kuriam netaikomas šis reglamentas, t. y. kariniu, gynybos ar nacionalinio saugumo tikslu, ir vienu ar daugiau tikslų, kuriems netaikomas šis reglamentas, pavyzdžiui, civilinių arba teisėsaugos tikslų, o tų sistemų tiekėjai turėtų užtikrinti, kad sistemos atitiktų šį reglamentą. Tais atvejais tai, kad DI sistema gali patekti į šio reglamento taikymo sritį, neturėtų daryti poveikio nacionalinio saugumo, gynybos ir karinę veiklą vykdančių subjektų (neatsižvelgiant į jų rūšį) galimybei nacionalinio saugumo, kariniais ir gynybos tikslais naudoti DI sistemas, kurių naudojimui šis reglamentas netaikomas. DI sistema, pateikta rinkai civiliniais ar teisėsaugos tikslais, kuri su pakeitimais arba be jų naudojama kariniais, gynybos ar nacionalinio saugumo tikslais, neturėtų patekti į šio reglamento taikymo sritį, neatsižvelgiant į tokią veiklą vykdančio subjekto rūšį;

(25) šiuo reglamentu turėtų būti remiamos inovacijos, turėtų būti gerbiama mokslo laisvė ir neturėtų būti pakenkta mokslinių tyrimų ir plėtros veiklai. Todėl į jo taikymo sritį reikia neįtraukti DI sistemų ir modelių, specialiai sukurtų ir pradėtų naudoti vien tik mokslinių tyrimų ir plėtros tikslu. Be to, būtina užtikrinti, kad šis reglamentas kitaip nedarytų poveikio su DI sistemomis arba modeliais susijusiai mokslinių tyrimų ir plėtros veiklai prieš juos pateikiant rinkai arba pradedant naudoti. Į gaminius orientuotų mokslinių tyrimų, bandymų ir plėtros veiklai, susijusiai su DI sistemomis arba modeliais, šio reglamento nuostatos taip pat neturėtų būti taikomos prieš tas sistemas ir modelius pradedant naudoti arba pateikiant rinkai. Tas netaikymas nedaro poveikio pareigai laikytis šio reglamento, kai DI sistema, patenkanti į šio reglamento taikymo sritį, kaip tokios mokslinių tyrimų ir plėtros veiklos rezultatas pateikiama rinkai arba pradedama naudoti, ir nuostatų dėl apribotų DI bandomųjų reglamentavimo aplinkų ir bandymų realiomis sąlygomis taikymui. Be to, nedarant poveikio netaikymui DI sistemoms, specialiai sukurtoms ir pradėtoms naudoti tik mokslinių tyrimų ir plėtros tikslu, šio reglamento nuostatos ir toliau turėtų būti taikomos bet kuriai kitai DI sistemai, kuri gali būti naudojama bet kokiai mokslinių tyrimų ir plėtros veiklai vykdyti. Bet kuriuo atveju bet kokia mokslinių tyrimų ir plėtros veikla turėtų būti vykdoma laikantis pripažintų moksliniams tyrimams taikomų etikos ir profesinių standartų ir turėtų būti vykdoma laikantis taikytinos Sąjungos teisės;

(26) siekiant nustatyti proporcingą ir veiksmingą DI sistemoms taikomų taisyklių rinkinį, reikėtų vadovautis aiškiai apibrėžtu rizika grindžiamu požiūriu. Laikantis to požiūrio tokių taisyklių rūšį ir turinį reikėtų pritaikyti prie rizikos, kurią gali sukelti DI sistemos, intensyvumo ir masto. Todėl būtina uždrausti tam tikrą nepriimtiną su DI susijusią praktiką, nustatyti didelės rizikos DI sistemoms taikomus reikalavimus, o atitinkamiems veiklos vykdytojams – pareigas, taip pat nustatyti skaidrumo pareigas tam tikroms DI sistemoms;

(27) nors rizika grindžiamas požiūris yra proporcingų ir veiksmingų privalomų taisyklių pagrindas, svarbu priminti 2019 m. Patikimo DI etikos gaires, kurias parengė Komisijos paskirta nepriklausoma AI HLEG. Tose gairėse AI HLEG parengė septynis neprivalomus DI etikos principus, kuriais siekiama padėti užtikrinti, kad DI būtų patikimas ir atitiktų etikos normas. Septyni principai apima žmogiškąjį veiksnį ir žmogaus atliekamą priežiūrą, techninį patvarumą ir saugumą, privatumą ir duomenų valdymą, skaidrumą, įvairovę, nediskriminavimą ir teisingumą, visuomenės ir aplinkos gerovę, ir atskaitomybę. Nedarant poveikio teisiškai privalomiems šio reglamento ir bet kurios kitos taikytinos Sąjungos teisės reikalavimams, tomis gairėmis prisidedama prie nuoseklaus, patikimo ir į žmogų orientuoto DI projektavimo, laikantis Chartijos ir vertybių, kuriomis grindžiama Sąjunga. Pagal AI HLEG gaires žmogiškasis veiksnys ir žmogaus atliekama priežiūra reiškia, kad DI sistemos kuriamos ir naudojamos kaip priemonė, kuri tarnauja žmonėms, kuria gerbiamas žmogaus orumas ir asmens autonomiškumas ir kuri veikia taip, kad ją galėtų kontroliuoti ir prižiūrėti žmonės.

Techninis patvarumas ir saugumas reiškia, kad DI sistemos kuriamos ir naudojamos taip, kad būtų užtikrintas patvarumas kilus problemoms ir atsparumas mėginimams pakeisti DI sistemos naudojimą ar veikimo efektyvumą, kad trečiosios šalys galėtų ją neteisėtai naudoti, ir kad būtų kuo labiau sumažinta nenumatyta žala. Privatumas ir duomenų valdymas reiškia, kad DI sistemos kuriamos ir naudojamos laikantis privatumo ir duomenų apsaugos taisyklių, kartu tvarkant aukštus kokybės ir vientisumo standartus atitinkančius duomenis. Skaidrumas reiškia, kad DI sistemos kuriamos ir naudojamos taip, kad būtų sudarytos sąlygos tinkamam atsekamumui ir paaiškinamumui, kartu informuojant žmones apie tai, kad jie bendrauja ar sąveikauja su DI sistema, taip pat tinkamai informuojant diegėjus apie šios DI sistemos pajėgumus ir ribotumus, o asmenis, kuriems daromas poveikis – apie jų teises. Įvairovė, nediskriminavimas ir teisingumas reiškia, kad DI sistemos kuriamos ir naudojamos taip, kad šiame procese dalyvautų įvairūs subjektai, ir kad būtų skatinama vienoda prieiga, lyčių lygybė ir kultūrų įvairovė, kartu išvengiant pagal Sąjungos ar nacionalinę teisę draudžiamo diskriminacinio poveikio ir nepagrįsto šališkumo. Visuomenės ir aplinkos gerovė reiškia, kad DI sistemos kuriamos ir naudojamos tvariu ir palankiu aplinkai būdu ir taip, kad jos būtų naudingos visiems žmonėms, kartu stebint ir vertinant ilgalaikį poveikį asmenims, visuomenei ir demokratijai. Tų principų taikymas, kai įmanoma, turėtų būti perkeltas į DI modelių projektavimą ir naudojimą. Bet kuriuo atveju jais turėtų būti remiamasi rengiant elgesio kodeksus pagal šį reglamentą. Visi suinteresuotieji subjektai, įskaitant pramonę, akademinę bendruomenę, pilietinę visuomenę ir standartizacijos organizacijas, raginami rengiant savanorišką geriausią praktiką ir standartus atitinkamai atsižvelgti į etikos principus;

(28) be daugybės naudingų DI panaudojimo būdų, juo taip pat gali būti piktnaudžiaujama ir ji gali suteikti naujoviškų ir galingų manipuliavimo, išnaudojimo ir socialinės kontrolės praktikos įrankių. Tokia praktika yra ypač žalinga, ja lengva piktnaudžiauti ir ji turėtų būti draudžiama, nes prieštarauja Sąjungos vertybėms, susijusioms su pagarba žmogaus orumui, laisve, lygybe, demokratija ir teisine valstybe ir su Chartijoje įtvirtintomis pagrindinėmis teisėmis, be kita ko, teisėmis į nediskriminavimą, duomenų apsaugą bei privatumą ir vaiko teisėmis;

(29) DI grindžiami manipuliavimo metodai gali būti naudojami siekiant įtikinti asmenis atlikti nepageidaujamus veiksmus arba juos apgauti, skatinant juos priimti sprendimus taip, kad būtų trukdoma ir kenkiama jų autonomiškumui, sprendimų priėmimui ir laisvam pasirinkimui. Tam tikrų DI sistemų pateikimas rinkai, pradėjimas naudoti arba naudojimas siekiant iš esmės iškreipti arba iškreipiant žmogaus elgesį, galbūt sukeliant didelę žalą, visų pirma darančią pakankamai didelį neigiamą poveikį fizinei, psichologinei sveikatai ar finansiniams interesams, yra ypač pavojingas ir todėl turėtų būti draudžiamas. Tokiose DI sistemose naudojami pasąmonę veikiantys komponentai, pavyzdžiui, garso, paveikslėlių, judamo vaizdo stimuliacijos, kurių žmonės negali suvokti, nes tos stimuliacijos priemonės yra žmogui nesuvokiamos, arba kiti manipuliavimo ar apgaulės metodai, kuriais trukdoma arba kenkiama asmens autonomiškumui, sprendimų priėmimui ar laisvam pasirinkimui tokiais būdais, kad žmonės sąmoningai nesuvokia tų priemonių, jei jas ir suvokia, vis tiek yra apgaunami arba negali jų kontroliuoti ar joms pasipriešinti. Tą galėtų palengvinti, pavyzdžiui, mašinos ir smegenų sąsajos arba virtualioji realybė, nes jos leidžia geriau kontroliuoti, kokios stimuliacijos pateikiamos žmonėms, tiek, kiek jos gali iš esmės iškreipti jų elgesį labai žalingu būdu. Be to, DI sistemos taip pat gali kitaip išnaudoti asmens arba konkrečios asmenų grupės pažeidžiamumą dėl jų amžiaus, negalios, kaip tai suprantama Europos Parlamento ir Tarybos direktyvoje (ES) 2019/882[16], arba konkrečios socialinės ar ekonominės padėties, dėl kurios tuos asmenis yra lengviau išnaudoti, pavyzdžiui, ypač skurdžiai gyvenančius asmenis, etnines ar religines mažumas.

---

16 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/882 dėl gaminių ir paslaugų prieinamumo reikalavimų (OL L 151, 2019 6 7, p. 70).

Tokios DI sistemos gali būti pateiktos rinkai, pradėtos naudoti arba naudojamos siekiant iš esmės iškreipti arba iškreipiant asmens elgesį tokiu būdu, kuris sukelia arba pagrįstai manoma, kad gali sukelti didelę žalą tam ar kitam asmeniui arba asmenų grupėms, įskaitant žalą, kuri laikui bėgant gali didėti, ir todėl turėtų būti draudžiamos. Gali būti neįmanoma daryti prielaidos, kad ketinama iškreipti elgesį, kai iškreipimą lemia su DI sistema nesusiję veiksniai, kurių tiekėjas ar diegėjas negali kontroliuoti, t. y. veiksniai, kurių DI sistemos tiekėjas ar diegėjas negali pagrįstai numatyti ir dėl to negali sušvelninti jų poveikio. Bet kuriuo atveju nebūtina, kad tiekėjas ar diegėjas ketintų sukelti didelę žalą, jeigu tokia žala vis tiek atsiranda dėl manipuliavimo ar išnaudojimo pasitelkiant DI grindžiamas praktiką. Tokios DI praktikos draudimai papildo Europos Parlamento ir Tarybos direktyvos 2005/29/EB[17] nuostatas, visų pirma tai, kad nesąžininga komercinė praktika, daranti ekonominę ar finansinę žalą vartotojams, yra draudžiama bet kokiomis aplinkybėmis, nepaisant to, ar ji vykdoma naudojant DI sistemas ar kitaip. Šiame reglamente nustatyti manipuliavimo ir išnaudojimo praktikos draudimai neturėtų daryti poveikio teisėtai praktikai, susijusiai su medicininiu gydymu, pavyzdžiui, psichologiniu psichikos ligos gydymu ar fizine reabilitacija, kai tokia praktika vykdoma laikantis taikytinos teisės ir medicinos standartų, pavyzdžiui, gavus aiškų asmenų arba jų teisinių atstovų sutikimą. Be to, įprasta ir teisėta komercinė praktika, pavyzdžiui, reklamos srityje, kuri atitinka taikytiną teisę, neturėtų būti savaime laikoma DI grindžiama žalinga manipuliavimo praktika;

---

[17] 2005 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva 2005/29/EB dėl nesąžiningos įmonių komercinės veiklos vartotojų atžvilgiu vidaus rinkoje ir iš dalies keičianti Tarybos direktyvą 84/450/EEB, Europos Parlamento ir Tarybos direktyvas 97/7/EB, 98/27/EB bei 2002/65/EB ir Europos Parlamento ir Tarybos reglamentą (EB) Nr. 2006/2004 („Nesąžiningos komercinės veiklos direktyva“) (OL L 149, 2005 6 11, p. 22).

(30) turėtų būti draudžiamos biometrinio kategorizavimo sistemos, grindžiamos fizinių asmenų biometriniais duomenimis, pavyzdžiui, asmens veidu ar pirštų atspaudu, siekiant nuspręsti dėl ar padaryti išvadas dėl asmens politinių pažiūrų, narystės profesinėse sąjungose, religinių ar filosofinių įsitikinimų, rasės, lytinio gyvenimo ar seksualinės orientacijos. Tas draudimas neturėtų būti taikomas pagal Sąjungos ar nacionalinę teisę gautų biometrinių duomenų rinkinių teisėtam ženklinimui, filtravimui ar kategorizavimui pagal biometrinius duomenis, pavyzdžiui, paveikslėlių rūšiavimui pagal plaukų arba akių spalvą, kurie, pavyzdžiui, gali būti naudojami teisėsaugos srityje;

(31) viešų arba privačių subjektų naudojimasis DI sistemomis, kurių paskirtis yra vykdyti fizinių asmenų socialinį reitingavimą, gali duoti diskriminuojančių rezultatų, o tam tikros grupės gali patirti atskirtį. Taip gali būti pažeista teisė į orumą ir nediskriminavimą ir lygybės bei teisingumo vertybės. Tokios DI sistemos vertina arba klasifikuoja fizinius asmenis arba jų grupes remdamosi daugybe duomenų taškų, susijusių su jų socialiniu elgesiu įvairiomis aplinkybėmis arba žinomomis, numanomomis ar nuspėjamais asmeniniais arba asmenybės bruožais tam tikrais laikotarpiais. Tokių DI sistemų sukurtas socialinio reitingavimo rezultatas gali lemti žalingą arba nepalankų elgesį su fiziniais asmenimis arba ištisomis jų grupėmis ir tai gali būti daroma socialinėmis aplinkybėmis, kurios nėra susijusios su aplinkybėmis, kuriomis duomenys buvo iš pradžių sugeneruoti arba surinkti, arba žalingą elgesį, kuris yra neproporcingas arba nepagrįstas atsižvelgiant į jų socialinio elgesio rimtumą. Todėl DI sistemos, taikančios tokią nepriimtiną reitingavimo praktiką ir lemiančios tokius žalingus ar nepalankius rezultatus, turėtų būti draudžiamos. Tas draudimas neturėtų daryti poveikio teisėtai fizinių asmenų vertinimo praktikai, vykdomai konkrečiu tikslu laikantis Sąjungos ir nacionalinės teisės;

(32) DI sistemų naudojimas dėl tikralaikio nuotolinio biometrinio fizinių asmenų tapatybės nustatymo viešai prieinamose erdvėse teisėsaugos tikslu itin riboja atitinkamų asmenų teises ir laisves, nes tai gali daryti poveikį didelės gyventojų dalies privačiam gyvenimui, sukelti nuolatinį sekimo jausmą ir netiesiogiai atgrasyti nuo naudojimosi susirinkimų teise ir kitomis pagrindinėmis teisėmis. DI sistemų, skirtų nuotoliniam fizinių asmenų biometriniam tapatybės nustatymui, techniniai netikslumai gali lemti šališkus rezultatus ir daryti diskriminacinį poveikį. Tokie galimi šališki rezultatai ir diskriminacinis poveikis yra ypač svarbūs amžiaus, etninės kilmės, rasės, lyties arba negalios atžvilgiu. Be to, poveikio betarpiškumas ir ribotos galimybės atlikti tolesnes patikras ar taisymus, susijusius su tokiomis tikruoju laiku veikiančiomis sistemomis, kelia didesnę riziką atitinkamų asmenų, kurių atžvilgiu vykdoma teisėsaugos veikla arba kuriems ji daro poveikį, teisėms ir laisvėms;

(33) todėl šių sistemų naudojimas teisėsaugos tikslu turėtų būti draudžiamas, išskyrus išsamiai išvardytas ir tiksliai apibrėžtas situacijas, kai sistemas naudoti tikrai būtina siekiant apginti esminį viešąjį interesą, kurio svarba nusveria riziką. Šios situacijos apima tam tikrų nusikaltimo aukų, įskaitant dingusius asmenis, paiešką, tam tikras grėsmes fizinių asmenų gyvybei arba fiziniam saugumui arba teroristinio išpuolio grėsmes ir šio reglamento priede išvardytų nusikalstamų veikų vykdytojų arba įtariamųjų buvimo vietos arba tapatybės nustatymą, jei už tas nusikalstamas veikas atitinkamoje valstybėje narėje pagal tos valstybės narės teisę baudžiama laisvės atėmimo bausme arba priimant sprendimą dėl įkalinimo ne trumpiau nei ketveriems metams, ir kaip jos apibrėžtos tos valstybės narės teisėje. Tokia nacionalinėje teisėje nustatyta laisvės atėmimo bausmės arba sprendimo dėl įkalinimo riba padeda užtikrinti, jog tam, kad būtų galima pateisinti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimą, nusikalstama veika turi būti pakankamai rimta. Be to, šio reglamento priede pateiktas nusikalstamų veikų sąrašas yra grindžiamas 32 nusikalstamomis veikomis, išvardytomis Tarybos pamatiniame sprendime 2002/584/TVR[18], atsižvelgiant į tai, kad kai kurios iš tų veikų praktiniu požiūriu gali būti svarbesnės palyginti su kitomis, taigi tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas gali būti būtinas ir proporcingas (labai įvairiu mastu) norint praktiškai nustatyti įvairių išvardytų nusikalstamų veikų vykdytojo arba įtariamojo buvimo vietą arba tapatybę, kartu atsižvelgiant į tikėtinus žalos arba galimų neigiamų pasekmių rimtumo, tikėtinumo ir masto skirtumus.

[18] 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).

Neišvengiama grėsmė fizinių asmenų gyvybei arba fiziniam saugumui taip pat galėtų kilti dėl didelio ypatingos svarbos infrastruktūros, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2022/2557[19] 2 straipsnio 4 punkte, sutrikimo, kai tokios ypatingos svarbos infrastruktūros sutrikimas arba sunaikinimas sukeltų neišvengiamą grėsmę asmens gyvybei arba fiziniam saugumui, be kita ko, dėl didelės žalos būtiniausių prekių tiekimui gyventojams arba valstybės pagrindinės funkcijos vykdymui. Be to, šiuo reglamentu turėtų būti išsaugota galimybė teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijoms atlikti tapatybės patikrinimus dalyvaujant atitinkamam asmeniui, laikantis Sąjungos ir nacionalinėje teisėje tokiems patikrinimams nustatytų sąlygų. Visų pirma teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijos turėtų turėti galimybę naudotis informacinėmis sistemomis pagal Sąjungos arba nacionalinę teisę, kad nustatytų asmenų, kurie tapatybės patikrinimo metu atsisako leisti nustatyti jų tapatybę arba negali nurodyti ar įrodyti savo tapatybės, tapatybę, nereikalaujant pagal šį reglamentą gauti išankstinį leidimą. Tai galėtų būti, pavyzdžiui, asmuo, dalyvavęs vykdant nusikaltimą, nenorintis arba negalintis dėl nelaimingo atsitikimo ar sveikatos būklės atskleisti savo tapatybės teisėsaugos institucijoms;

---

[19] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (OL L 333, 2022 12 27, p. 164).

(34) siekiant užtikrinti, kad tos sistemos būtų naudojamos atsakingai ir proporcingai, taip pat svarbu nustatyti, kad kiekvienoje iš šių išsamiai nurodytų ir tiksliai apibrėžtų situacijų būtų atsižvelgiama į tam tikrus aspektus, visų pirma susijusius su situacijos, dėl kurios 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 sistemos viešai prieinamose erdvėse teisėsaugos tikslu turėtų būti diegiamos tik tam, kad būtų patvirtinta konkrečiai tiriamo asmens tapatybė, ir turėtų neviršyti to, kas tikrai būtina, kiek tai susiję su laikotarpiu, taip pat geografine ir subjektine taikymo sritimi, atsižvelgiant visų pirma į įrodymus arba požymius, susijusius su grėsmėmis, aukomis arba nusikalstamos veikos vykdytoju. Tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą viešai prieinamose erdvėse turėtų būti leidžiama naudoti tik tuo atveju, jei atitinkama teisėsaugos institucija yra atlikusi poveikio pagrindinėms teisėms vertinimą ir, jei šiame reglamente nenumatyta kitaip, yra užregistravusi sistemą duomenų bazėje, kaip nustatyta šiame reglamente. Kiekvienoje iš pirmiau nurodytų situacijų kiekvieno panaudojimo atveju turėtų būti pasirenkama tinkama informacinė asmenų duomenų bazė;

(35) kiekvieną kartą viešai prieinamose erdvėse teisėsaugos tikslu naudojant tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą reikėtų gauti aiškų ir konkretų valstybės narės teisminės institucijos arba nepriklausomos administracinės institucijos, kurios sprendimas yra privalomas, leidimą. Toks leidimas iš esmės turėtų būti gautas prieš pradedant naudoti DI sistemą tam, kad būtų nustatyta asmens ar asmenų tapatybė. Turėtų būti leidžiama netaikyti tos taisyklės tinkamai pagrįstose neatidėliotinose situacijose, t. y. situacijose, kuriose poreikis naudoti atitinkamas sistemas yra toks, kad faktiškai ir objektyviai neįmanoma gauti leidimo prieš pradedant naudoti DI sistemą. Tokiose neatidėliotinose situacijose DI sistemos naudojimas turėtų apsiriboti tik tuo, kas absoliučiai minimaliai būtina, ir turėtų būti taikomos tinkamos apsaugos priemonės ir sąlygos, kaip apibrėžta nacionalinėje teisėje ir kaip konkrečiai nurodė pati teisėsaugos institucija, atsižvelgdama į kiekvieną individualų neatidėliotino naudojimo atvejį. Be to, tokiose situacijose teisėsaugos institucija turėtų paprašyti tokio leidimo, kartu nurodydama priežastis, dėl kurių negalėjo leidimo paprašyti anksčiau, nepagrįstai nedelsdama ir ne vėliau kaip per 24 valandas. Jei tokį leidimą atsisakoma išduoti, su tuo leidimu susietų tikralaikio biometrinio tapatybės nustatymo sistemų naudojimas turėtų būti tuojau pat nutrauktas ir visi su tokiu naudojimu susiję duomenys turėtų būti pašalinti ir ištrinti. Tokie duomenys apima įvesties duomenis, kuriuos DI sistema tiesiogiai gauna naudojant tokią sistemą, taip pat su tuo leidimu susieto naudojimo rezultatus ir išvedinius. Jie neturėtų apimti pagal kitą Sąjungos arba nacionalinės teisės aktą teisėtai gautos įvesties. Bet kuriuo atveju, remiantis vien nuotolinio biometrinio tapatybės nustatymo sistemos išvediniu neturėtų būti priimtas joks sprendimas, kuris sukeltų asmeniui nepalankų teisinį poveikį;

(36) kad atitinkama rinkos priežiūros institucija ir nacionalinė duomenų apsaugos institucija galėtų atlikti savo užduotis pagal šiame reglamente ir nacionalinėse taisyklėse nustatytus reikalavimus, joms turėtų būti pranešama apie kiekvieną tikralaikio biometrinio tapatybės nustatymo sistemos naudojimą. Rinkos priežiūros institucijos ir nacionalinės duomenų apsaugos institucijos, kurios buvo notifikuotos, turėtų pateikti Komisijai metinę tikralaikio biometrinio tapatybės nustatymo sistemų naudojimo ataskaitą;

(37) be to, laikantis šiame reglamente nustatytos išsamios sistemos, tinkama numatyti, kad toks naudojimas valstybės narės teritorijoje pagal šį reglamentą turėtų būti įmanomas tik tais atvejais ir tik tiek, kiek atitinkama valstybė narė yra nusprendusi 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 kuriais tikslais, kuriais būtų galima pagrįsti pagal šį reglamentą nustatytą leistiną naudojimą. Apie tokias nacionalines taisykles Komisijai turėtų būti pranešta per 30 dienų nuo jų priėmimo;

(38) viešai prieinamose erdvėse teisėsaugos tikslu naudojant DI sistemas dėl tikralaikio nuotolinio biometrinio fizinių asmenų tapatybės nustatymo neišvengiamai tvarkomi biometriniai duomenys. Šio reglamento taisyklės, kuriomis, išskyrus tam tikras išimtis, draudžiamas toks naudojimas, grindžiamos 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 taikymo ribų kompetentingos institucijos, veikdamos teisėsaugos tikslu, negalėtų naudoti tokių sistemų ir tvarkyti su tuo susijusių tokių duomenų, remdamosi Direktyvos (ES) 2016/680 10 straipsnyje išvardytais pagrindais. Atsižvelgiant į tai šiuo reglamentu nesiekiama nustatyti asmens duomenų tvarkymo pagal Direktyvos (ES) 2016/680 8 straipsnį teisinio pagrindo. Tačiau tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešai prieinamose erdvėse kitais nei teisėsaugos tikslu, įskaitant atvejus, kai tai daro kompetentingos institucijos, neturėtų patekti į konkrečios sistemos, susijusios su tokiu naudojimu teisėsaugos tikslu, kuri nustatyta šiame reglamente, taikymo sritį. Todėl tokiam naudojimui kitais nei teisėsaugos tikslais neturėtų būti reikalaujama leidimo pagal šį reglamentą ir taikomas išsamias nacionalinės teisės taisykles, pagal kurias gali būti įgyvendinamas tas leidimas;

(39) bet koks biometrinių duomenų ir kitų asmens duomenų, susijusių su DI sistemų naudojimu biometrinio tapatybės nustatymo tikslais, naudojimas, išskyrus atvejus, kai viešai prieinamose erdvėse teisėsaugos tikslu naudojamos tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos, kaip nustatyta šiame reglamente, turėtų ir toliau derėti su visais reikalavimais, taikomais pagal Direktyvos (ES) 2016/680 10 straipsnį. Kitais nei teisėsaugos tikslais pagal Reglamento (ES) 2016/679 9 straipsnio 1 dalį ir Reglamento (ES) 2018/1725 10 straipsnio 1 dalį draudžiama tvarkyti biometrinius duomenis, kuriems taikomos tuose straipsniuose numatytos ribotos išimtys. Taikant Reglamento (ES) 2016/679 9 straipsnio 1 dalį, nuotolinio biometrinio tapatybės nustatymo naudojimui kitais nei teisėsaugos tikslais jau buvo taikomi nacionalinių duomenų apsaugos institucijų sprendimai dėl draudimo;

(40) 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 pirmos pastraipos g punkte, tiek, kiek jis taikomas biometrinio kategorizavimo sistemų naudojimui vykdant veiklą policijos bendradarbiavimo ir teisminio bendradarbiavimo baudžiamosiose bylose srityje, 5 straipsnio 1 dalies pirmos pastraipos d punkte, tiek, kiek jis taikomas DI sistemų naudojimui, kuriam taikoma ta nuostata, 5 straipsnio 1 dalies pirmos pastraipos h punkte, 5 straipsnio 2–6 dalyse ir 26 straipsnio 10 dalyje 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;

(41) 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 pirmos pastraipos g punkte, tiek, kiek jis taikomas biometrinio kategorizavimo sistemų naudojimui vykdant veiklą policijos bendradarbiavimo ir teisminio bendradarbiavimo baudžiamosiose bylose srityje, 5 straipsnio 1 dalies pirmos pastraipos d punkte, tiek, kiek jis taikomas DI sistemų naudojimui, kuriam taikoma ta nuostata, 5 straipsnio 1 dalies pirmos pastraipos h punkte, 5 straipsnio 2–6 dalyse ir 26 straipsnio 10 dalyje 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;

(42) laikantis nekaltumo prezumpcijos, fiziniai asmenys Sąjungoje visada turėtų būti vertinami pagal jų faktinį elgesį. Fiziniai asmenys niekada neturėtų būti vertinami pagal DI nuspėtą elgesį remiantis vien jų profiliavimu, asmenybės savybėmis ar bruožais, pavyzdžiui, pilietybe, gimimo vieta, gyvenamąja vieta, vaikų skaičiumi, skolos dydžiu ar automobilio modeliu, nesant pagrįsto įtarimo, kad tas asmuo dalyvauja nusikalstamoje veikloje, remiantis objektyviais patikrinamais faktais ir be žmogaus atliekamo vertinimo. Todėl turėtų būti draudžiama atlikti rizikos vertinimus, susijusius su fiziniais asmenimis, siekiant įvertinti tikimybę, kad jie gali padaryti nusikaltimą, arba nuspėti, kad bus padaryta faktinė ar potenciali nusikalstama veika, remiantis vien jų profiliavimu arba asmenybės savybių ir bruožų vertinimu. Bet kuriuo atveju tas draudimas nėra susijęs su rizikos analitika, kuri nėra grindžiama asmenų profiliavimu ar asmenų asmenybės savybėmis ir bruožais, pavyzdžiui, DI sistemomis, kuriose rizikos analitika naudojama įmonių finansinio sukčiavimo tikimybei įvertinti remiantis įtartinais sandoriais arba rizikos analitika, skirta numatyti tikimybę, kad muitinės gali nustatyti narkotikų ar neteisėtų prekių buvimo vietą, pavyzdžiui, remiantis žinomais neteisėtos prekybos maršrutais;

(43) turėtų būti draudžiama pateikti rinkai, pradėti naudoti tuo konkrečiu tikslu arba naudoti DI sistemas, kuriomis kuriamos arba plečiamos veido atpažinimo duomenų bazės, netikslingai renkant veido atvaizdus iš interneto arba apsauginės vaizdo stebėjimo sistemos (AVSS) įrašų, nes ta praktika prisideda prie masinio sekimo jausmo ir gali lemti šiurkščius pagrindinių teisių, įskaitant teisę į privatumą, pažeidimus;

(44) didelį susirūpinimą kelia DI sistemų, kuriomis siekiama nustatyti emocijas arba daryti dėl jų išvadas, mokslinis pagrindas, visų pirma dėl to, kad emocijų raiška įvairiose kultūrose ir situacijose, taip pat net ir vieno asmens atveju, labai skiriasi. Vienas iš pagrindinių tokių sistemų trūkumų yra ribotas patikimumas, specifiškumo stoka ir ribotos galimybės apibendrinti. Todėl DI sistemos, pagal kurias nustatomos fizinių asmenų emocijos ar ketinimai arba daromos dėl jų išvados remiantis jų biometriniais duomenimis, gali lemti diskriminuojančius rezultatus ir gali riboti atitinkamų asmenų teises ir laisves. Atsižvelgiant į galios disbalansą darbo arba švietimo srityje ir į tai, kad šios sistemos yra ribojančio pobūdžio, tokios sistemos galėtų lemti žalingą arba nepalankų elgesį su tam tikrais fiziniais asmenimis arba ištisomis jų grupėmis. Todėl turėtų būti draudžiama pateikti rinkai, pradėti naudoti arba naudoti DI sistemas, skirtas naudoti siekiant nustatyti asmenų emocinę būklę situacijose, susijusiose su darbo vieta ir švietimu. Tas draudimas neturėtų būti taikomas DI sistemoms, kurios pateikiamos rinkai tik dėl medicininių ar saugumo priežasčių, pavyzdžiui, sistemoms, skirtoms naudoti terapijoje;

(45) šiuo reglamentu neturėtų būti daromas poveikis praktikai, kurią draudžia Sąjungos teisė, įskaitant duomenų apsaugos teisės aktus, nediskriminavimo teisės aktus, vartotojų apsaugos teisės aktus ir konkurencijos teisės aktus;

(46) didelės rizikos DI sistemos Sąjungos rinkai turėtų būti pateikiamos, pradedamos naudoti arba naudojamos tik jeigu jos atitinka tam tikrus privalomus reikalavimus. Šiais reikalavimais turėtų būti užtikrinama, kad Sąjungoje prieinamos didelės rizikos DI sistemos arba sistemos, kurių išvedinys kitaip naudojamas Sąjungoje, nekeltų nepriimtinos rizikos svarbiems Sąjungos interesams, kurie pripažįstami ir saugomi pagal Sąjungos teisę. Remiantis naująja teisės aktų sistema, kaip paaiškinta Komisijos pranešime „2022 m. Mėlynasis vadovas dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo“[20], bendra taisyklė yra ta, kad vienam gaminiui gali būti taikoma daugiau nei vienas teisės aktas iš Sąjungos derinamųjų teisės aktų, pavyzdžiui, Europos Parlamento ir Tarybos reglamentai (ES) 2017/745[21] ir (ES) 2017/746[22] arba Europos Parlamento ir Tarybos direktyva 2006/42/EB[23], nes pateikti rinkai arba pradėti naudoti galima tik tada, kai gaminys atitinka visus taikytinus Sąjungos derinamuosius teisės aktus. Siekiant užtikrinti suderinamumą ir išvengti nereikalingos administracinės naštos ar išlaidų, gaminio, kuriame yra viena ar daugiau didelės rizikos DI sistemų, kurioms taikomi šio reglamento ir šio reglamento priede išvardytų Sąjungos derinamųjų teisės aktų reikalavimai, tiekėjai turėtų būti lankstūs, kiek tai susiję su veiklos sprendimais dėl to, kaip optimaliai užtikrinti gaminio, kuriame yra viena ar daugiau DI sistemų, atitiktį visiems taikytiniems Sąjungos derinamųjų teisės aktų reikalavimams. 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 turėtų būti kiek įmanoma sumažintas galimas tarptautinės prekybos suvaržymas;

---

[20] OL C 247, 2022 6 29, p. 1.

[21] 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).

[22] 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).

[23] 2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyva 2006/42/EB dėl mašinų, iš dalies keičianti Direktyvą 95/16/EB (OL L 157, 2006 6 9, p. 24).

(47) DI sistemos galėtų daryti neigiamą poveikį asmenų sveikatai ir saugai, visų pirma tais atvejais, kai tokios sistemos veikia kaip gaminių saugos 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 saugos rizikai, kurią gali sukelti visas gaminys dėl savo skaitmeninių komponentų, įskaitant DI sistemas, ir tokia rizika būtų tinkamai mažinama. 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;

(48) DI sistemos keliamo neigiamo poveikio mastas pagal Chartiją saugomoms pagrindinėms teisėms yra ypač aktualus tuomet, kai DI sistema priskiriama didelės rizikos sistemoms. 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, teisė į nediskriminavimą, teisė į švietimą, vartotojų apsauga, darbuotojų teisės, asmenų su negalia teisės, lyčių lygybė, intelektinės nuosavybės teisės, teisė į veiksmingą teisių gynimą ir teisingą bylos nagrinėjimą, teisė į gynybą ir nekaltumo prezumpcija ir teisė į gerą administravimą. Be šių teisių, svarbu akcentuoti tai, kad vaikai turi specialias teises, įtvirtintas Chartijos 24 straipsnyje ir Jungtinių Tautų vaiko teisių konvencijoje ir išplėtotas JT VTK bendrojoje pastaboje Nr. 25 dėl skaitmeninės aplinkos; pagal abu šiuos dokumentus reikia atsižvelgti į vaikų pažeidžiamumą ir suteikti jiems tokią apsaugą ir priežiūrą, kuri yra būtina jų gerovei užtikrinti. Vertinant žalos, kurią gali sukelti DI sistema, įskaitant žalą asmenų sveikatai ir saugai, rimtumą taip pat reikėtų atsižvelgti į pagrindinę teisę į aukšto lygio aplinkos apsaugą, kuri yra įtvirtinta Chartijoje ir įgyvendinta Sąjungos politikoje;

(49) dėl didelės rizikos DI sistemų, kurios yra gaminių arba sistemų saugos komponentai, arba pačios yra gaminiai arba sistemos, patenkantys į Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008[24], Europos Parlamento ir Tarybos reglamento (ES) Nr. 167/2013[25], Europos Parlamento ir Tarybos reglamento (ES) Nr. 168/2013[26], Europos Parlamento ir Tarybos direktyvos 2014/90/ES[27], Europos Parlamento ir Tarybos direktyvos (ES) 2016/797[28],

---

[24] 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).

[25] 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).

[26] 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).

[27] 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).

[28] 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).

Europos Parlamento ir Tarybos reglamento (ES) 2018/858[29] taikymo sritis, Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139[30] ir Europos Parlamento ir Tarybos reglamentas (ES) 2019/2144[31], yra tikslinga iš dalies pakeisti šiuos aktus, siekiant užtikrinti, kad Komisija, remdamasi kiekvieno sektoriaus techniniais ir reglamentavimo ypatumais ir nesikišdama į esamus valdymo, atitikties vertinimo ir vykdymo užtikrinimo mechanizmus ir jais nustatytus įgaliojimus, atsižvelgtų į šiame reglamente nustatytus privalomus reikalavimus didelės rizikos DI sistemoms, kai remdamasi šiais išvardytais aktais ji priima susijusius deleguotuosius ar įgyvendinimo aktus;

---

[29] 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).

[30] 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).

[31] 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).

(50) dėl DI sistemų, kurios yra gaminių saugos komponentai arba kurios pačios yra gaminiai, patenkantys į tam tikrų Sąjungos derinamųjų teisės aktų, išvardytų šio reglamento priede, taikymo sritį, pagal šį reglamentą yra tikslinga jas priskirti didelės rizikos sistemoms, jeigu atitinkamam gaminiui taikoma atitikties vertinimo procedūra, kurią pagal tą atitinkamą Sąjungos derinamąjį teisės aktą atlieka trečiosios šalies atitikties vertinimo įstaiga. Tokie gaminiai visų pirma yra mašinos, žaislai, liftai, įranga ir apsaugos sistemos, skirtos naudoti potencialiai sprogioje aplinkoje, radijo įranga, slėginiai įrenginiai, pramoginių laivų įrenginiai, lynų kelio įrenginiai, dujinį kurą deginantys prietaisai, medicininiai prietaisai, *in vitro* diagnostiniai medicinos prietaisai, automobiliai ir aviacija;

(51) DI sistemos priskyrimas didelės rizikos sistemoms pagal šį reglamentą nebūtinai turėtų reikšti, kad gaminys, kurio saugos komponentas yra DI sistema, arba pati DI sistema kaip gaminys, yra laikomas didelės rizikos pagal atitinkamame Sąjungos derinamajame teisės akte nustatytus kriterijus, kurie taikomi gaminiui. Tai visų pirma pasakytina apie reglamentus (ES) 2017/745 ir (ES) 2017/746, kuriuose numatyta galimybė trečiajai šaliai atlikti vidutinės rizikos ir didelės rizikos gaminių atitikties vertinimą;

(52) atskiras DI sistemas, konkrečiai, 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 didelę žalos asmenų sveikatai ir saugumui arba pagrindinėms teisėms riziką, atsižvelgiant į galimos žalos dydį ir jos pasireiškimo tikimybę, ir į tai, kad šios sistemos naudojamos įvairiose šiame reglamente iš anksto konkrečiai apibrėžtose srityse. Tų sistemų identifikavimas grindžiamas ta pačia metodika ir kriterijais, kurie yra numatyti ir bet kuriems būsimiems didelės rizikos DI sistemų sąrašo pakeitimams, kuriuos Komisija turėtų būti įgaliota priimti deleguotaisiais aktais, kad būtų atsižvelgta į spartų technologinės plėtros tempą ir galimus DI sistemų naudojimo pokyčius;

(53) taip pat svarbu paaiškinti, kad gali būti konkrečių atvejų, kai DI sistemos, naudojamos šiame reglamente iš anksto konkrečiai apibrėžtose srityse, nekelia reikšmingos žalos rizikos pagal tas sritis saugomiems teisiniams interesams, nes jos nedaro reikšmingos įtakos sprendimų priėmimui arba reikšmingos žalos tiems interesams. Šio reglamento tikslais DI sistema, kuri nedaro reikšmingos įtakos sprendimų priėmimo proceso rezultatams, turėtų būti suprantama kaip DI sistema, kuri nedaro reikšmingo poveikio žmogaus ar automatizuotai priimamų sprendimų esmei, taigi, ir rezultatams. DI sistema, kuri nedaro reikšmingos įtakos sprendimų priėmimo proceso rezultatams, galėtų būti sistema, naudojama situacijose, kai tenkinama viena ar daugiau iš toliau nurodytų sąlygų. Pirmoji tokia sąlyga turėtų būti ta, kad DI sistema būtų skirta atlikti siaurą procedūrinę užduotį, pavyzdžiui, nestruktūrizuotus duomenis paversti struktūrizuotais ar gaunamus dokumentus klasifikuoti pagal kategorijas, arba turėtų būti naudojama tam, kad tarp daugybės taikomųjų programų nustatytų identiškas programas. Tos užduotys yra tokio siauro ir riboto pobūdžio, kad kelia tik nedidelę riziką, kuri nepadidėja naudojant DI sistemą aplinkybėmis, kurios šio reglamento priede pateikiamame sąraše išvardytos kaip didelės rizikos naudojimas. Antroji sąlyga turėtų būti ta, kad DI sistemos atliekama užduotis turėtų pagerinti veiklos, kurią anksčiau atlikdavo žmogus ir kuri gali būti svarbi šio reglamento priede pateikiamame sąraše išvardytų kaip didelės rizikos naudojimo atvejų tikslais, rezultatus. Atsižvelgiant į tuos ypatumus, DI sistema tik šiek tiek papildo žmogaus veiklą, todėl ir jos keliama rizika atitinkamai yra mažesnė. Ta sąlyga, pavyzdžiui, būtų taikoma DI sistemoms, skirtoms patobulinti dokumentų, kuriuos anksčiau rengdavo žmogus, kalbą, pavyzdžiui, profesinį toną ar akademinį kalbos stilių, arba suderinti tekstą su tam tikro prekės ženklo skleidžiama žinia. Trečioji sąlyga turėtų būti ta, kad DI sistema turėtų būti skirta nustatyti sprendimų priėmimo modelius arba nukrypimus nuo ankstesnių sprendimų priėmimo modelių.

Rizika sumažėtų dėl to, kad DI sistema būtų naudojama po to, kai žmogus jau būtų atlikęs įvertinimą, kurio ji negalėtų pakeisti ar paveikti be tinkamos žmogaus atliekamos peržiūros. Tokios DI sistemos yra, pavyzdžiui, tos, kurios, atsižvelgiant į tam tikrą mokytojo vertinimo modelį, gali būti naudojamos *ex post* patikrinti, ar mokytojas galėjo nukrypti nuo vertinimo modelio, kad nustatytų galimus neatitikimus ar anomalijas. Ketvirta sąlyga turėtų būti ta, kad DI sistema būtų skirta atlikti užduotį, kuri būtų tik parengiamoji prieš atliekant vertinimą, svarbų šio reglamento priede išvardytų DI sistemų tikslais, todėl galimas sistemos išvedinių poveikis būtų labai mažas kalbant apie riziką vertinimui, kurį reikia atlikti. Ši sąlyga, be kita ko, apima išmaniuosius bylų tvarkymo sprendimus, apimančius įvairias funkcijas – nuo indeksavimo, paieškos, teksto ir kalbos apdorojimo arba duomenų susiejimo su kitais duomenų šaltiniais, arba DI sistemas, naudojamas pirminiams dokumentams versti. Bet kuriuo atveju DI sistemos, šio reglamento priede pateikiamame sąraše išvardytos kaip didelės rizikos naudojimo atvejai, turėtų būti laikomos keliančiomis reikšmingą žalos sveikatai, saugai ar pagrindinėms teisėms riziką, jei jos apima profiliavimą, kaip tai suprantama Reglamento (ES) 2016/679 4 straipsnio 4 punkte arba Direktyvos (ES) 2016/680 3 straipsnio 4 punkte, arba Reglamento (ES) 2018/1725 3 straipsnio 5 punkte. Siekiant užtikrinti atsekamumą ir skaidrumą, tiekėjas, manantis, kad DI sistema nėra didelės rizikos DI sistema, remdamasis pirmiau nurodytomis sąlygomis, turėtų parengti vertinimo dokumentus prieš pateikdamas tą sistemą rinkai arba prieš pradedant ją naudoti ir nacionalinėms kompetentingoms institucijoms paprašius turėtų joms pateikti tuos dokumentus. Toks tiekėjas turėtų būti įpareigotas užregistruoti DI sistemą pagal šį reglamentą sukurtoje ES duomenų bazėje. Siekdama pateikti papildomų gairių dėl sąlygų, kuriomis šio reglamento priede išvardytos DI sistemos išimties tvarka laikomos nedidelės rizikos DI sistemomis, praktinio įgyvendinimo, Komisija, pasikonsultavusi su Valdyba, turėtų pateikti gaires, kuriose būtų nurodyta to praktinio įgyvendinimo tvarka, papildytas išsamiu praktinių didelės rizikos DI sistemų naudojimo atvejų ir nedidelės rizikos DI sistemų naudojimo atvejų pavyzdžių sąrašu;

(54) kadangi biometriniai duomenys yra speciali asmens duomenų kategorija, tikslinga tam tikrus ypatingos svarbos biometrinių sistemų naudojimo atvejus klasifikuoti kaip didelės rizikos, jei jas leidžiama naudoti pagal atitinkamą Sąjungos ir nacionalinę teisę. DI sistemų, skirtų nuotoliniam fizinių asmenų biometriniam tapatybės nustatymui, techniniai netikslumai gali lemti šališkus rezultatus ir daryti diskriminacinį poveikį. Tokių šališkų rezultatų ir diskriminacinio poveikio rizika yra ypač aktuali kalbant apie amžių, etninę kilmę, rasę, lytį arba negalią. Todėl nuotolinio biometrinio tapatybės nustatymo sistemos, atsižvelgiant į jų keliamą riziką, turėtų būti klasifikuojamos kaip didelės rizikos sistemos. Į tokią klasifikaciją nepatenka DI sistemos, skirtos naudoti biometriniam sutikrinimui, įskaitant autentiškumo patvirtinimą, kurių vienintelis tikslas – patvirtinti, kad konkretus fizinis asmuo yra tas asmuo, kuriuo jis prisistato, ir patvirtinti fizinio asmens tapatybę vieninteliu – prieigos prie paslaugos, prietaiso atrakinimo ar saugaus patekimo į patalpas – tikslu. Be to, DI sistemos, skirtos naudoti biometriniam kategorizavimui pagal neskelbtinus požymius ar ypatumus, saugomus pagal Reglamento (ES) 2016/679 9 straipsnio 1 dalį, remiantis biometriniais duomenimis, jei jos nėra draudžiamos pagal šį reglamentą, ir emocijų atpažinimo sistemos, kurios nėra draudžiamos pagal šį reglamentą, turėtų būti klasifikuojamos kaip didelės rizikos sistemos. Biometrinės sistemos, skirtos naudoti tik kibernetinio saugumo užtikrinimo ir asmens duomenų apsaugos priemonių tikslais, neturėtų būti laikomos didelės rizikos DI sistemomis;

(55) 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 Direktyvos (ES) 2022/2557 priedo 8 punkte nurodytą ypatingos svarbos skaitmeninę infrastruktūrą, kelių transportą ir vandens, dujų, šilumos ir elektros energijos tiekimą, nes joms sugedus arba sutrikus jų veikimui gali kilti rizika daugelio žmonių gyvybei ir sveikatai ir didelių įprastos socialinės ir ekonominės veiklos sutrikimų. Ypatingos svarbos infrastruktūros, įskaitant ypatingos svarbos skaitmeninę infrastruktūrą, saugos komponentai yra sistemos, kurios yra naudojamos siekiant tiesiogiai apsaugoti ypatingos svarbos infrastruktūros fizinį vientisumą arba asmenų sveikatą bei saugą ir turtą, tačiau nėra būtinos, kad sistema veiktų. Dėl tokių komponentų gedimo arba trikties gali kilti tiesioginis pavojus ypatingos svarbos infrastruktūros fiziniam vientisumui, taigi ir žmonių sveikatai bei saugai ir turtui. Komponentai, skirti naudoti tik kibernetinio saugumo tikslais, neturėtų būti laikomi saugos komponentais. Tokios ypatingos svarbos infrastruktūros saugos komponentų pavyzdžiai gali būti vandens slėgio stebėsenos sistemos arba priešgaisrinės signalizacijos sistemos debesijos kompiuterijos centruose;

(56) DI sistemų diegimas švietimo srityje yra svarbus norint skatinti kokybišką skaitmeninį švietimą ir mokymą ir sudaryti sąlygas visiems besimokantiems asmenims ir mokytojams įgyti būtinų skaitmeninių įgūdžių ir kompetencijų, įskaitant gebėjimą naudotis žiniasklaidos priemonėmis ir kritinį mąstymą, ir jais dalytis, kad jie galėtų aktyviai dalyvauti ekonomikoje, visuomenėje ir demokratiniuose procesuose. Tačiau DI sistemos, švietimo ar profesinio mokymo srityje naudojamos visų pirma suteikiant prieigą arba priimant ar skiriant asmenis į švietimo ir profesinio mokymo įstaigas arba programas visais lygmenimis, vertinant asmenų mokymosi rezultatus, vertinant, koks švietimo lygmuo tinkamas asmeniui ir darant esminę įtaką švietimo ir mokymo, kurį asmenys gaus ar galės gauti, lygiui arba stebint ir nustatant draudžiamą mokinių elgesį testų metu, turėtų būti priskiriamos didelės rizikos DI sistemoms, nes jos gali nulemti asmens švietimo ir profesinio kelio kryptį, taigi, ir gali daryti poveikį jo gebėjimui užsitikrinti pragyvenimo šaltinį. Tokios sistemos, jeigu jos netinkamai suprojektuojamos ir naudojamos, gali būti itin intervencinės ir pažeisti teisę į švietimą ir mokymą, taip pat teisę nebūti diskriminuojamam ir atkartoti įprastinius diskriminavimo modelius, pavyzdžiui, liečiančius moteris, tam tikro amžiaus grupes, asmenis su negalia arba tam tikros rasinės ar etninės kilmės arba seksualinės orientacijos asmenis;

(57) DI sistemos, naudojamos užimtumo, darbuotojų valdymo ir galimybės dirbti savarankiškai, visų pirma asmenų įdarbinimo ir atrankos, sprendimų, darančių poveikį sutartinių darbo santykių sąlygoms, priėmimo, sutartinių darbo santykių skatinimo arba nutraukimo, užduočių skyrimo remiantis individualiu elgesiu, asmenybės bruožais ar savybėmis ir asmenų stebėsena ar vertinimu sutartiniuose darbo santykiuose srityse, taip pat turėtų būti klasifikuojamos kaip didelės rizikos sistemos, nes tos sistemos gali daryti apčiuopiamą poveikį tų asmenų būsimoms karjeros galimybėms, jų pragyvenimo šaltiniams ir darbuotojų teisėms. Atitinkamuose sutartiniuose darbo santykiuose turėtų prasmingai dalyvauti darbuotojai ir per platformas paslaugas teikiantys asmenys, kaip nurodyta 2021 m. Komisijos darbo programoje. Darbuotojų įdarbinimo metu ir juos vertinant, paaukštinant arba išlaikant asmenis sutartiniuose darbo santykiuose, tokios sistemos gali atkartoti įprastinius diskriminavimo modelius, pavyzdžiui, liečiančius moteris, tam tikro amžiaus grupes, asmenis su negalia arba tam tikros rasinės ar etninės kilmės arba seksualinės orientacijos asmenis. DI sistemos, naudojamos tokių asmenų veiklos rezultatams ir elgesiui stebėti, taip pat gali pažeisti jų pagrindines teises į duomenų apsaugą ir privatumą;

(58) kita sritis, kurioje DI sistemų naudojimui reikia skirti ypatingą dėmesį, yra galimybė gauti tam tikras esmines privačiąsias ir viešąsias paslaugas ir išmokas, būtinas žmonėms tam, kad jie galėtų visapusiškai dalyvauti visuomenėje arba pagerinti savo pragyvenimo lygį, ir galimybė jomis pasinaudoti. Visų pirma fiziniai asmenys, valdžios institucijų prašantys arba iš jų gaunantys esmines viešosios paramos išmokas ir paslaugas, t. y. sveikatos priežiūros paslaugas, socialinės apsaugos išmokas, socialines paslaugas, užtikrinančias apsaugą motinystės, ligos, nelaimingų atsitikimų darbe, priklausomybės ar senatvės atvejais, taip pat darbo, socialinės paramos ir paramos būstui netekimo atvejais, paprastai priklauso nuo šių išmokų ir paslaugų ir yra pažeidžiami atsakingų institucijų atžvilgiu. Jeigu DI sistemos, naudojamos nustatyti, ar institucija turėtų skirti, atsisakyti skirti tokias išmokas ir paslaugas, jas sumažinti, panaikinti arba susigrąžinti, įskaitant tai, ar naudos gavėjai teisėtai turi teisę gauti tokias išmokas ar paslaugas, tos sistemos gali turėti reikšmingą poveikį asmenų pragyvenimo šaltiniui ir gali pažeisti jų pagrindines teises, pavyzdžiui, teisę į socialinę apsaugą, nediskriminavimą, žmogaus orumą arba veiksmingą teisių gynimą, ir todėl turėtų būti klasifikuojamos kaip didelės rizikos sistemos. Vis dėlto šis reglamentas neturėtų trukdyti kurti ir naudoti naujoviškus viešojo administravimo metodus, kuriuos įgyvendinant būtų naudinga plačiau naudotis reikalavimus atitinkančiomis ir saugiomis DI sistemomis, jeigu jos nekelia didelės rizikos juridiniams ir fiziniams asmenims.

Be to, 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 tais tikslais naudojamų DI sistemų gali būti diskriminuojami asmenys arba grupės ir gali būti atkartojami įprastiniai diskriminavimo modeliai, pavyzdžiui, dėl rasinės ar etninės kilmės, lyties, negalios, amžiaus ar seksualinės orientacijos, arba gali būti sukuriamos naujos diskriminacinio poveikio formos. Tačiau Sąjungos teisėje numatytos DI sistemos, kuriomis siekiama nustatyti sukčiavimą teikiant finansines paslaugas ir prudenciniais tikslais apskaičiuoti kredito įstaigų ir draudimo įmonių kapitalo reikalavimus, pagal šį reglamentą neturėtų būti laikomos didelės rizikos sistemomis. Be to, DI sistemos, skirtos naudoti su fiziniais asmenimis susijusiai rizikai vertinti ir kainodarai sveikatos ir gyvybės draudimo tikslais, taip pat gali daryti reikšmingą poveikį asmenų pragyvenimo šaltiniams ir, jei jos nėra tinkamai suprojektuotos, sukurtos ir naudojamos, gali pažeisti jų pagrindines teises ir sukelti rimtų pasekmių žmonių gyvybei ir sveikatai, įskaitant finansinę atskirtį ir diskriminaciją. Galiausiai DI sistemos, naudojamos fizinių asmenų skubios pagalbos skambučiams vertinti ir klasifikuoti arba teikiant arba nustatant prioritetines skubias pirmosios pagalbos paslaugas, įskaitant policijos, ugniagesių ir medicinos pagalbos paslaugas, taip pat teikiamos pagal neatidėliotinos medicinos pagalbos reikalingų pacientų skirstymo sistemas, taip pat turėtų būti klasifikuojamos kaip didelės rizikos sistemos, nes jos sprendimus priima ypač kritinėse situacijose, susijusiose su asmenų gyvybe ir sveikata bei jų turtu;

(59) atsižvelgiant į teisėsaugos institucijų vaidmenį ir atsakomybę, jų veiksmams, kuriuos vykdant tam tikru būdu naudojamos DI sistemos, būdingas didelis galios disbalansas ir jie gali lemti fizinio asmens sekimą, areštą arba jo laisvės apribojimą, taip pat daryti kitokį neigiamą poveikį Chartijoje garantuojamoms pagrindinėms teisėms. Visų pirma, jeigu DI sistema mokoma naudojant nekokybiškus duomenis, neatitinka jai keliamų pakankamų veikimo efektyvumo, tikslumo ar patikimumo reikalavimų arba nėra tinkamai suprojektuota ir išbandyta prieš pateikiant ją rinkai arba kitaip pradedant naudoti, ji gali atrinkti asmenis diskriminuojančiu arba kitokiu neteisingu arba nesąžiningu būdu. Be to, jei DI sistemos nėra pakankamai skaidrios, suprantamos ir dokumentuojamos, gali būti trukdoma užtikrinti svarbias procesines pagrindines teises, pavyzdžiui, teisę į veiksmingą teisių gynimo priemonę ir teisingą bylos nagrinėjimą, taip pat teisę į gynybą ir nekaltumo prezumpciją. Todėl yra tinkama klasifikuoti kaip didelės rizikos įvairias DI sistemas (jei jas leidžiama naudoti pagal atitinkamus Sąjungos ir nacionalinės teisės aktus), 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.

Atsižvelgiant į veiklos pobūdį ir su ja susijusią riziką, tos didelės rizikos DI sistemos visų pirma turėtų apimti DI sistemas, skirtas teisėsaugos institucijoms (arba jų vardu) arba teisėsaugos institucijoms padedančioms Sąjungos įstaigoms, organams ar agentūroms naudoti tam, kad būtų galima įvertinti riziką fiziniam asmeniui tapti nusikalstamų veikų auka (pavyzdžiui, poligrafus ir panašias priemones), tam, kad būtų galima įvertinti įrodymų patikimumą atliekant nusikalstamų veikų tyrimą ar vykdant baudžiamąjį persekiojimą už jas ir, jei tai nedraudžiama pagal šį reglamentą, tam, kad būtų galima įvertinti fizinio asmens nusikalstamumo ar pakartotinio nusikalstamumo riziką remiantis ne tik fizinių asmenų profiliavimu ar asmenybės savybių ir bruožų įvertinimu arba ankstesniu fizinių asmenų ar grupių nusikalstamu elgesiu, ir profiliavimui nustatant, tiriant nusikalstamas veikas arba vykdant baudžiamąjį persekiojimą už jas . DI sistemos, skirtos konkrečiai naudoti mokesčių inspekcijų ir muitinių administracinėse bylose, taip pat administracines užduotis atliekančių finansinės žvalgybos padalinių informacijos analizei pagal Sąjungos kovos su pinigų plovimu teisės aktus, neturėtų būti klasifikuojamos kaip didelės rizikos DI sistemos, teisėsaugos institucijų naudojamos nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo tikslais. Teisėsaugos ir kitos atitinkamos valdžios institucijos neturėtų naudoti DI priemonių taip, kad tai taptų nelygybės ar atskirties veiksniu. Nereikėtų ignoruoti DI priemonių naudojimo poveikio įtariamųjų teisėms į gynybą, visų pirma to, kad sunku gauti prasmingos informacijos apie tų sistemų veikimą ir dėl to atsirandančių sunkumų ginčijant jų rezultatus teisme, ypač fiziniams asmenims, kurių atžvilgiu atliekamas tyrimas;

(60) migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos daro poveikį žmonėms, kurie dažnai yra 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, visų pirma jų laisvo judėjimo teisei, teisei nebūti diskriminuojamiems, teisei į privataus gyvenimo ir asmens duomenų apsaugą, teisei į tarptautinę apsaugą ir gerą administravimą. Todėl tikslinga kaip didelės rizikos sistemas klasifikuoti DI sistemas (jei jų naudojimas leidžiamas pagal atitinkamus Sąjungos ir nacionalinės teisės aktus, skirtus kompetentingoms valdžios institucijoms (arba jų vardu) arba Sąjungos institucijoms, įstaigoms, organams ar agentūroms, kuriems tenka migracijos, prieglobsčio ir sienų kontrolės valdymo sričių užduotys (pavyzdžiui, poligrafus ir panašias priemones), naudoti tam, kad būtų galima įvertinti tam tikrą fizinių asmenų, atvykstančių į valstybės narės teritoriją arba prašančių vizos ar prieglobsčio, keliamą riziką, kad kompetentingoms valdžios institucijoms būtų padedama nagrinėti prieglobsčio, vizos ir leidimo gyventi prašymus ir susijusius skundus, įskaitant susijusius įrodymų patikimumo vertinimus, siekiant tikslo nustatyti, ar tam tikro statuso prašantys fiziniai asmenys atitinka reikalavimus, fizinių asmenų aptikimo, atpažinimo arba identifikavimo migracijos, prieglobsčio ir sienų kontrolės valdymo kontekste (išskyrus kelionės dokumentų tikrinimą) tikslu.

Migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos, kurioms taikomas šis reglamentas, turėtų atitikti atitinkamus procedūrinius reikalavimus, nustatytus Europos Parlamento ir Tarybos reglamente (EB) Nr. 810/2009[32], Europos Parlamento ir Tarybos direktyvoje 2013/32/ES[33] ir kituose susijusiuose Sąjungos teisės aktuose. Valstybės narės ar Sąjungos institucijos, įstaigos, organai ar agentūros jokiomis aplinkybėmis neturėtų naudoti DI sistemų migracijos, prieglobsčio ir sienų kontrolės valdymo srityse kaip priemonių tam, kad apeitų savo tarptautinius įsipareigojimus pagal 1951 m. liepos 28 d. Ženevoje priimtą JT konvenciją dėl pabėgėlių statuso su pakeitimais, padarytais 1967 m. sausio 31 d. protokolu. Tos sistemos taip pat neturėtų būti naudojamos siekiant kokiu nors būdu pažeisti negrąžinimo principą arba neleisti asmenims atvykti į Sąjungos teritoriją saugiais ir veiksmingais teisėtais būdais, įskaitant teisę į tarptautinę apsaugą;

---

32 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).

33 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).

(61) 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, skirtas naudoti teisminėms institucijoms arba jų vardu, siekiant padėti teisminėms institucijoms ieškoti faktų ir aiškinti faktus ir teisę ir taikyti įstatymus konkretiems faktų rinkiniams. DI sistemos, skirtos naudoti alternatyvaus ginčų sprendimo įstaigose minėtais tikslais, taip pat turėtų būti laikomos didelės rizikos sistemomis, kai alternatyvaus ginčų sprendimo proceso rezultatai sukelia teisinį poveikį šalims. DI priemonių naudojimas gali sustiprinti teisėjų gebėjimą priimti sprendimus ar teismų nepriklausomumą, bet neturėtų jų pakeisti – galutinį sprendimą privalo priimti žmogus. Tačiau DI sistemų klasifikavimas kaip didelės rizikos sistemų neturėtų būti taikomas DI sistemoms, skirtoms grynai papildomai administracinei veiklai, kuri nedaro poveikio faktiniam teisingumo vykdymui individualiais atvejais, pavyzdžiui, teismo sprendimų, dokumentų arba duomenų anoniminimui arba pseudoniminimui, darbuotojų tarpusavio ryšiams arba administracinėms užduotims ;

(62) nedarant poveikio Europos Parlamento ir Tarybos reglamente (ES) 2024/…[34+] numatytoms taisyklėms ir siekiant šalinti nederamo išorinio kišimosi į Chartijos 39 straipsnyje įtvirtintą balsavimo teisę ir neigiamo poveikio demokratijai ir teisinei valstybei riziką, DI sistemos, skirtos naudoti siekiant daryti įtaką rinkimų ar referendumų rezultatams arba fizinių asmenų balsavimo elgsenai balsuojant rinkimuose ar referendumuose, turėtų būti klasifikuojamos kaip didelės rizikos DI sistemos, išskyrus DI sistemas, kurių išvediniai fiziniams asmenims nedaro tiesioginio poveikio, pavyzdžiui, priemones, naudojamas politinėms kampanijoms organizuoti, optimizuoti ir struktūrizuoti administraciniu ir logistiniu požiūriu;

(63) tai, kad DI sistema pagal šį reglamentą klasifikuojama kaip didelės rizikos DI sistema, neturėtų reikšti, kad tos sistemos naudojimas 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, skirtų fizinių asmenų emocinei būklei nustatyti, naudojimo. Bet kuris toks naudojimas turėtų būti tęsiamas tik laikantis iš Chartijos ir taikomų Sąjungos antrinės teisės aktų ir nacionalinės teisės kylančių taikytinų reikalavimų. Šis reglamentas neturėtų būti suprantamas taip, kad juo nustatomas teisinis asmens duomenų, kai aktualu, įskaitant specialias asmens duomenų kategorijas, tvarkymo pagrindas, nebent šiame reglamente konkrečiai numatyta kitaip;

---

[34] … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/… dėl politinės reklamos skaidrumo ir atrankiojo adresavimo (OL L, …, ELI: …).

[+] OL: prašom tekste įrašyti dokumente PE 90/23 (2021/0381(COD)) pateikiamo reglamento numerį ir užpildyti atitinkamą išnašą.

(64) siekiant sumažinti pateikiamų rinkai arba pradėtų naudoti didelės rizikos DI sistemų keliamą riziką ir užtikrinti aukšto lygio patikimumą, didelės rizikos DI sistemoms reikėtų taikyti tam tikrus privalomus reikalavimus, atsižvelgiant į numatytąją sistemos naudojimo paskirtį ir DI sistemos naudojimo kontekstą ir laikantis rizikos valdymo sistemos, kurią turi nustatyti tiekėjas. Kad būtų pasiekti šio reglamento tikslai, priemonėmis, kurias tiekėjai priima siekdami laikytis privalomų šio reglamento reikalavimų, turėtų būti atsižvelgiama į visuotinai pripažintus pažangiausius DI srities metodus, jos turėtų būti proporcingos ir veiksmingos. Remiantis naująja teisės aktų sistema, kaip paaiškinta Komisijos pranešime „2022 m. Mėlynasis vadovas dėl gaminius reglamentuojančių ES taisyklių įgyvendinimo“, bendra taisyklė yra ta, kad vienam gaminiui gali būti taikomas daugiau nei vienas Sąjungos derinamasis teisės aktas, nes pateikti rinkai arba pradėti naudoti galima tik tada, kai gaminys atitinka visus taikytinus Sąjungos derinamuosius teisės aktus. DI sistemų, kurioms taikomi šio reglamento reikalavimai, keliami pavojai yra susiję su kitais aspektais nei tie, kuriuos apima esami Sąjungos derinamieji teisės aktai, todėl šio reglamento reikalavimai papildytų esamą Sąjungos derinamųjų teisės aktų sistemą. Pavyzdžiui, mašinos ar medicinos priemonių gaminiai, kuriuose įdiegta DI sistema, gali kelti riziką, kurios neapima atitinkamuose Sąjungos derinamuosiuose teisės aktuose nustatyti esminiai sveikatos ir saugos reikalavimai, nes tais sektorių teisės aktais nereglamentuojama DI sistemoms būdinga rizika.

Todėl vienu metu turi būti taikomi įvairūs teisėkūros procedūra priimami aktai ir jie turi papildyti vienas kitą. Siekiant užtikrinti suderinamumą ir išvengti nereikalingos administracinės naštos ir nereikalingų išlaidų, gaminio, kuriame yra viena ar daugiau didelės rizikos DI sistemų, kurioms taikomi šio reglamento ir Sąjungos derinamųjų teisės aktų, grindžiamų naująja teisės aktų sistema ir išvardytų šio reglamento priede, reikalavimai, tiekėjai turėtų būti lankstūs, kiek tai susiję su veiklos sprendimais dėl to, kaip optimaliai užtikrinti gaminio, kuriame yra viena ar daugiau DI sistemų, atitiktį visiems taikytiniems tų Sąjungos derinamųjų teisės aktų reikalavimams. Tas lankstumas galėtų reikšti, pavyzdžiui, tiekėjo sprendimą dalį reikalingų bandymų ir ataskaitų teikimo procesų, informacijos ir dokumentų, kurių reikalaujama pagal šį reglamentą, įtraukti į jau esamus dokumentus ir procedūras, kurių reikalaujama pagal esamus Sąjungos derinamuosius teisės aktus, grindžiamus naująja teisės aktų sistema ir išvardytus šio reglamento priede. Tai jokiu būdu neturėtų pakenkti tiekėjo pareigai laikytis visų taikytinų reikalavimų;

(65) rizikos valdymo sistemą turėtų sudaryti suplanuotas ir per visą didelės rizikos DI sistemos gyvavimo ciklą vykstantis nuolatinis kartotinis procesas. Tuo procesu turėtų būti siekiama nustatyti ir sumažinti atitinkamą DI sistemų riziką sveikatai, saugai ir pagrindinėms teisėms. Rizikos valdymo sistema turėtų būti reguliariai peržiūrima ir atnaujinama, kad būtų užtikrintas jos nuolatinis veiksmingumas, taip pat visų svarbių sprendimų ir veiksmų, kurių imamasi pagal šį reglamentą, pagrindimas ir dokumentavimas. Šiuo procesu turėtų būti užtikrinama, kad tiekėjas nustatytų riziką ar neigiamą poveikį ir įgyvendintų žinomos ir pagrįstai numatomos DI sistemų rizikos sveikatai, saugai ir pagrindinėms teisėms mažinimo priemones, atsižvelgdamas į jų numatytąją paskirtį ir pagrįstai numatomą netinkamą naudojimą, įskaitant galimą riziką, kylančią dėl DI sistemos ir aplinkos, kurioje ji veikia, sąveikos. Rizikos valdymo sistemoje turėtų būti patvirtintos tinkamiausios rizikos valdymo priemonės, atsižvelgiant į naujausius technikos laimėjimus DI srityje. Nustatydamas tinkamiausias rizikos valdymo priemones, tiekėjas turėtų dokumentuoti ir paaiškinti savo pasirinkimus ir, kai aktualu, įtraukti ekspertus ir išorės suinteresuotuosius subjektus. Nustatydamas pagrįstai numatomą netinkamą didelės rizikos DI sistemų naudojimą, tiekėjas turėtų apimti naudojimą DI sistemų, kurios, nors tiesiogiai ir nepatenka į numatytąją paskirtį ir nėra numatytos naudojimo instrukcijoje, vis dėlto pagrįstai tikėtinai gali būti netinkamai naudojamos dėl lengvai nuspėjamo žmogaus elgesio konkrečios DI sistemos konkrečių ypatumų ir naudojimo kontekste. Visos žinomos ar numatomos aplinkybės, susijusios 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, turėtų būti įtrauktos į tiekėjo pateikiamas naudojimo instrukcijas. Taip siekiama užtikrinti, kad diegėjas žinotų apie jas ir į jas atsižvelgtų naudodamas didelės rizikos DI sistemą. Neturėtų būti reikalaujama, kad tiekėjas, nustatydamas ir įgyvendindamas rizikos mažinimo priemones, susijusias su numatomu netinkamu naudojimu pagal šį reglamentą, siekdamas kovoti su numatomu netinkamo naudojimu didelės rizikos DI sistemai taikytų konkrečias papildomas mokymo priemones. Tačiau tiekėjai raginami apsvarstyti galimybę tokias papildomas mokymo priemones taikyti tam, kad prireikus atitinkamai būtų sumažintas pagrįstai numatomas netinkamas naudojimas;

(66) didelės rizikos DI sistemoms turėtų būti taikomi reikalavimai dėl rizikos valdymo, naudojamų duomenų rinkinių kokybės ir aktualumo, techninių dokumentų ir įrašų saugojimo, skaidrumo ir informacijos teikimo diegėjams, žmogaus vykdomos priežiūros, patikimumo, tikslumo ir kibernetinio saugumo. Tie reikalavimai yra būtini siekiant veiksmingai sumažinti riziką sveikatai, saugai ir pagrindinėms teisėms. Jeigu nėra pagrįstai prieinamų jokių kitų mažiau prekybą ribojančių priemonių, tie reikalavimai nėra nepagrįsti prekybos apribojimai;

(67) kokybiški duomenys ir prieiga prie kokybiškų duomenų atlieka esminį vaidmenį nustatant daugelio DI sistemų struktūrą ir užtikrinant efektyvų jų veikimą, ypač tais atvejais, kai naudojami su modelių mokymu susiję metodai, siekiant užtikrinti, kad didelės rizikos DI sistema veiktų kaip numatyta, saugiai ir netaptų pagal Sąjungos teisę draudžiamos diskriminacijos šaltiniu. Norint parengti kokybiškus mokymo, validavimo ir bandymo duomenų rinkinius, reikia įdiegti tinkamą duomenų valdymo ir tvarkymo praktiką. Mokymo, validavimo ir bandymo duomenų rinkiniai, įskaitant etiketes, turėtų būti aktualūs, pakankamai reprezentatyvūs ir, kiek įmanoma, be klaidų ir išsamūs, atsižvelgiant į numatytąją sistemos paskirtį. Siekiant sudaryti palankesnes sąlygas laikytis Sąjungos duomenų apsaugos teisės aktų, pavyzdžiui, Reglamento (ES) 2016/679, duomenų valdymo ir tvarkymo praktika asmens duomenų atveju turėtų būti tokia, kad būtų užtikrinamas skaidrumas, susijęs su pradiniu duomenų rinkimo tikslu. Duomenų rinkiniai taip pat turėtų turėti tinkamas statistines savybes, be kita ko, kiek tai susiję su asmenimis ar asmenų grupėmis, kurių atžvilgiu ketinama naudoti didelės rizikos DI sistemą, ypatingą dėmesį skiriant galimo šališkumo duomenų rinkiniuose, kuris gali daryti poveikį asmenų sveikatai ir saugai, neigiamą poveikį pagrindinėms teisėms arba lemti pagal Sąjungos teisę draudžiamą diskriminaciją, mažinimui, ypač tais atvejais, kai duomenų išvediniai daro įtaką būsimoms operacijoms (grįžtamojo ryšio grandinės). Pavyzdžiui, šališkumas gali būti būdingas pagrindiniams duomenų rinkiniams, ypač kai naudojami ankstesni duomenys, arba jis gali atsirasti diegiant sistemas realiomis sąlygomis.

DI sistemų teikiamiems rezultatams įtakos galėtų turėti toks būdingas šališkumas, kuris yra linkęs palaipsniui didėti ir taip įtvirtinti ir sustiprinti esamą diskriminaciją, ypač tam tikroms pažeidžiamoms grupėms, įskaitant rasines ar etnines grupes, priklausančių asmenų diskriminaciją. Reikalavimas, kad duomenų rinkiniai būtų kiek įmanoma išsamesni ir juose nebūtų klaidų, neturėtų daryti poveikio privatumo užtikrinimo priemonių naudojimui kuriant ir bandant DI sistemas. Visų pirma, kiek to reikia atsižvelgiant į numatytąją paskirtį, duomenų rinkiniai turėtų būti grindžiami požymiais, ypatumais ar elementais, būdingais konkrečiai geografinei, kontekstinei, elgsenos ar funkcinei aplinkai, kurioje DI sistema yra skirta naudoti. Su duomenų valdymu susijusių reikalavimų galima laikytis kreipiantis į trečiąsias šalis, kurios teikia sertifikuotas atitikties užtikrinimo paslaugas, įskaitant duomenų valdymo, duomenų rinkinių vientisumo ir duomenų mokymo, validavimo ir bandymo praktikos tikrinimą, jei užtikrinamas šiame reglamente nustatytų duomenų reikalavimų laikymasis;

(68) kad galėtų kurti ir vertinti didelės rizikos DI sistemas, tam tikri subjektai, pavyzdžiui, tiekėjai, notifikuotosios įstaigos ir kiti susiję subjektai, pavyzdžiui, Europos skaitmeninių inovacijų centrai, bandymų įstaigos ir tyrėjai, turėtų turėti galimybę gauti ir naudoti kokybiškus duomenų rinkinius su šiuo reglamentu susijusių subjektų veiklos srityse. Komisijos sukurtos Europos bendros duomenų erdvės ir dalijimosi duomenimis tarp įmonių ir vyriausybės viešojo intereso labui palengvinimas bus labai svarbūs teikiant 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 DI 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;

(69) teisė į privatumą ir asmens duomenų apsaugą turi būti užtikrinta per visą DI sistemos gyvavimo ciklą. Šiuo atžvilgiu, tvarkant asmens duomenis yra taikytini Sąjungos duomenų apsaugos teisės aktuose nustatyti duomenų kiekio mažinimo ir pritaikytosios bei standartizuotosios duomenų apsaugos principai. Priemonės, kurių tiekėjai imasi siekdami užtikrinti, kad būtų laikomasi tų principų, gali apimti ne tik anoniminimą ir šifravimą, bet ir technologijų, leidžiančių algoritmus įtraukti į duomenis ir mokyti DI sistemas tarp šalių neperduodant arba nekopijuojant pačių neapdorotų ar struktūrizuotų duomenų, naudojimą, nedarant poveikio šiame reglamente numatytiems duomenų valdymo reikalavimams;

(70) siekiant apsaugoti kitų asmenų teises nuo diskriminacijos, kuri gali atsirasti dėl šališkumo DI sistemose, tiekėjai išimties tvarka tiek, kiek tai tikrai būtina siekiant užtikrinti šališkumo, susijusio su didelės rizikos DI sistemomis, nustatymą ir ištaisymą, taikydami tinkamas fizinių asmenų pagrindinių teisių ir laisvių apsaugos priemones ir visas šiame reglamente nustatytas taikytinas sąlygas, taip pat reglamentuose (ES) 2016/679 ir (ES) 2018/1725 ir Direktyvoje (ES) 2016/680 nustatytas sąlygas, turėtų galėti tvarkyti ir specialių kategorijų asmens duomenis, jei tai yra susiję su svarbiu viešuoju interesu, kaip tai suprantama Reglamento (ES) 2016/679 9 straipsnio 2 dalies g punkte ir Reglamento (ES) 2018/1725 10 straipsnio 2 dalies g punkte;

(71) suprantamos informacijos apie tai, kaip buvo sukurtos didelės rizikos DI sistemos ir kaip jos veikia per visą jų naudojimo trukmę, turėjimas yra labai svarbus siekiant sudaryti sąlygas tų sistemų atsekamumui, patikrinti, kaip laikomasi šio reglamento reikalavimų, taip pat stebėti jų operacijas ir vykdyti priežiūrą po pateikimo rinkai. Šiuo tikslu reikia saugoti įrašus ir užtikrinti techninių dokumentų, kuriuose pateikiama informacija, būtina DI sistemos atitikčiai atitinkamiems reikalavimams įvertinti ir priežiūrai po pateikimo rinkai palengvinti, prieinamumą. Tokią informaciją turėtų sudaryti bendrieji sistemos ypatumai, pajėgumai ir ribotumai, algoritmai, duomenys, mokymai, bandymai ir naudojami validavimo procesai, taip pat dokumentai apie atitinkamą rizikos valdymo sistemą, ji turėtų būti pateikiama aiškia ir suprantama forma. Techniniai dokumentai turėtų būti nuolat tinkamai atnaujinami per visą DI sistemos naudojimo trukmę. Be to, didelės rizikos DI sistemos turėtų būti tokios, kad per visą sistemos naudojimo trukmę būtų techniškai įmanoma automatiškai žurnaluose registruoti įvykius.

(72) siekiant spręsti susirūpinimą keliančius klausimus, susijusius su tam tikrų DI sistemų neskaidrumu ir sudėtingumu, ir padėti diegėjams vykdyti savo pareigas pagal šį reglamentą, turėtų būti reikalaujama, kad didelės rizikos DI sistemų skaidrumas būtų užtikrintas prieš pateikiant jas rinkai arba pradedant jas naudoti. Didelės rizikos DI sistemos turėtų būti projektuojamos taip, kad diegėjai galėtų suprasti, kaip DI sistema veikia, įvertinti jos funkcionalumą ir suvokti jos privalumus ir ribotumus. Prie didelės rizikos DI sistemų turėtų būti pridedama atitinkama informacija, pateikiama kaip naudojimo instrukcija. Tokia informacija turėtų apimti DI sistemos veikimo efektyvumo ypatumus, pajėgumus ir ribotumus. Jie apimtų informaciją apie galimas žinomas ir numatomas aplinkybes, susijusias su didelės rizikos DI sistemos naudojimu, įskaitant diegėjo veiksmus, kurie gali turėti įtakos sistemos elgsenai ir veikimo efektyvumui ir dėl kurių DI sistema gali kelti riziką sveikatai, saugumui ir pagrindinėms teisėms, apie pakeitimus, kuriuos tiekėjas iš anksto nustatė ir įvertino atitikties tikslais, ir apie atitinkamas žmogaus atliekamos priežiūros priemones, įskaitant priemones, diegėjams leidžiančias lengviau interpretuoti DI sistemos išvedinius. Skaidrumas, įskaitant pridedamas naudojimo instrukcijas, turėtų padėti diegėjams naudotis sistema ir priimti informacija pagrįstus sprendimus. Diegėjai turėtų, *inter alia*, turėti geresnes galimybes tinkamai pasirinkti sistemą, kurią jie ketina naudoti, atsižvelgdami į jiems taikytinas pareigas, būti informuoti apie numatomus ir draudžiamus naudojimo būdus ir tinkamai naudoti DI sistemą. Kad į naudojimo instrukcijas įtraukta informacija būtų aiškesnė ir prieinamesnė, kai tikslinga, turėtų būti pateikiami aiškinamieji pavyzdžiai, pavyzdžiui, apie DI sistemos ribotumus ir numatomus bei draudžiamus naudojimo būdus. Tiekėjai turėtų užtikrinti, kad visuose dokumentuose, įskaitant naudojimo instrukcijas, būtų pateikiama prasminga, išsami, prieinama ir suprantama informacija, atsižvelgiant į tikslinių diegėjų poreikius ir numatomas žinias. Naudojimo instrukcijos turėtų būti pateikiamos tiksliniams diegėjams lengvai suprantama kalba, kurią nustato atitinkama valstybė narė;

(73) didelės rizikos DI sistemos turėtų būti projektuojamos ir kuriamos taip, kad fiziniai asmenys galėtų prižiūrėti jų veikimą, užtikrinti, kad jos būtų naudojamos taip, kaipo numatyta, ir kad jų poveikis būtų kontroliuojamas per visą sistemos gyvavimo ciklą. Tuo tikslu sistemos tiekėjas prieš pateikdamas sistemą rinkai arba prieš pradedant ją naudoti turėtų nustatyti atitinkamas žmogaus atliekamos priežiūros priemones. Visų pirma, kai tikslinga, tokiomis priemonėmis turėtų būti garantuojama, kad sistemai būtų taikomi integruoti veikimo apribojimai, kurių pati sistema negalėtų nepaisyti ir kuriuos galėtų kontroliuoti žmogus, ir kad fiziniai asmenys, kuriems pavesta atlikti priežiūrą, turėtų būtiną kompetenciją, kvalifikaciją ir įgaliojimus atlikti tą funkciją. Be to, labai svarbu atitinkamai užtikrinti, kad į didelės rizikos DI sistemas būtų įtraukiami mechanizmai, skirti fiziniam asmeniui, kuriam pavesta žmogaus atliekama priežiūra, orientuoti ir informuoti, kad jis galėtų priimti informacija grindžiamus sprendimus dėl to, ar, kada ir kaip įsikišti, kad būtų išvengta neigiamų pasekmių ar rizikos, arba sustabdyti sistemos veikimą, jei ji neveikia taip, kaip numatyta. Atsižvelgiant į tai, kad neteisingos atitikties tam tikrose biometrinio tapatybės nustatymo sistemose atveju asmenims kyla reikšmingų pasekmių, tikslinga numatyti griežtesnį žmogaus atliekamos tų sistemų priežiūros reikalavimą, kad diegėjas imtis veiksmų ar priimti sprendimą remdamasis sistemos atliktu tapatybės nustatymu galėtų tik tada, kai tai atskirai patikrina ir patvirtina bent du fiziniai asmenys. Tie asmenys galėtų būti iš vieno ar daugiau subjektų ir vienas iš jų turėtų būti sistemą valdantis arba naudojantis asmuo. Šis reikalavimas neturėtų sukelti nereikalingos naštos ar delsos, ir galėtų pakakti, kad atskiri skirtingų asmenų patikrinimai būtų automatiškai registruojami sistemos generuojamuose žurnaluose. Atsižvelgiant į teisėsaugos, migracijos, sienų kontrolės ir prieglobsčio sričių ypatumus, šis reikalavimas neturėtų būti taikomas, jei pagal Sąjungos ar nacionalinę teisę to reikalavimo taikymas yra neproporcingas;

(74) didelės rizikos DI sistemos turėtų veikti nuosekliai per visą savo gyvavimo ciklą ir atitikti tinkamą tikslumo, patvarumo ir kibernetinio saugumo lygį, atsižvelgiant į jų numatytąją paskirtį ir vadovaujantis visuotinai pripažintais pažangiausiais metodais. Komisija, atitinkamos organizacijos ir suinteresuotieji subjektai raginami tinkamai atsižvelgti į DI sistemų keliamos rizikos ir neigiamo poveikio mažinimą. Tikėtinas veikimo efektyvumo metrikos lygmuo turėtų būti nurodomas pridedamose naudojimo instrukcijose. Tiekėjai raginami perduoti tokią informaciją diegėjams aiškiu ir lengvai suprantamu būdu ir taip, kad nekiltų nesusipratimų ar nebūtų klaidinančių pareiškimų. Sąjungos teisės aktais dėl teisinės metrologijos, įskaitant Europos Parlamento ir Tarybos direktyvas 2014/31/ES[35] ir 2014/32/ES[36], siekiama užtikrinti matavimų tikslumą ir padėti užtikrinti komercinių sandorių skaidrumą ir sąžiningumą. Atsižvelgdama į tai, Komisija, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais ir organizacijomis, pavyzdžiui, metrologijos ir lyginamosios analizės institucijomis, turėtų atitinkamai skatinti rengti DI sistemų lyginamuosius parametrus ir matavimo metodikas. Tai darydama Komisija turėtų atsižvelgti į tarptautinius partnerius, dirbančius metrologijos ir atitinkamų su DI susijusių matavimo rodiklių srityje, ir su jais bendradarbiauti;

---

35 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/31/ES dėl valstybių narių įstatymų, susijusių su neautomatinių svarstyklių tiekimu rinkai, suderinimo (OL L 96, 2014 3 29, p. 107).

36 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/32/ES dėl valstybių narių įstatymų, susijusių su matavimo priemonių tiekimu rinkai, suderinimo (OL L 96, 2014 3 29, p. 149).

(75) techninis patvarumas yra pagrindinis didelės rizikos DI sistemoms keliamas reikalavimas. Jos turėtų būti atsparios žalingam ar kitokiam nepageidaujamam elgesiui, kurį gali lemti sistemų ar aplinkos, kurioje tos sistemos veikia, ribotumai (pvz., klaidos, gedimai, nenuoseklumas, netikėtos situacijos). Todėl reikėtų imtis techninių ir organizacinių priemonių, kad būtų užtikrintas didelės rizikos DI sistemų patvarumas, pavyzdžiui, projektuojant ir kuriant tinkamus techninius sprendimus, kad būtų užkirstas kelias žalingam ar kitokiam nepageidaujamam elgesiui arba kad toks elgesys būtų kuo labiau neutralizuojamas. Tie techniniai sprendimai gali apimti, pavyzdžiui, mechanizmus, leidžiančius sistemai saugiai nutraukti savo veikimą (atsparumo gedimams planai) esant tam tikroms anomalijoms arba kai veikimas vyksta už tam tikrų iš anksto nustatytų ribų. Nesugebėjimas apsisaugoti nuo šios rizikos galėtų sukelti pasekmių saugumui arba daryti neigiamą poveikį pagrindinėms teisėms, pavyzdžiui, dėl klaidingų sprendimų arba neteisingų ar šališkų DI sistemos sugeneruotų išvedinių;

(76) kibernetinis saugumas atlieka esminį vaidmenį užtikrinant, kad DI sistemos būtų atsparios bandymams pakeisti jų naudojimą, elgseną, veikimo efektyvumą arba pažeisti jų saugumo funkcijas, kai trečiosios šalys imasi kenkėjiškų veiksmų sistemos pažeidžiamumui išnaudoti. Kibernetiniai išpuoliai prieš DI sistemas gali turėti įtakos konkretiems DI ištekliams, pavyzdžiui, mokymo duomenų rinkiniams (pvz., duomenų užkrėtimas) arba išmokytiems modeliams (pvz., priešiški trukdžiai arba priklausymo inferencija), 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, pavyzdžiui, saugumo kontrolės, taip pat tinkamai atsižvelgdami į pagrindinę IRT infrastruktūrą;

(77) nedarant poveikio šiame reglamente nustatytiems reikalavimams dėl patvarumo ir tikslumo, į Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams taikymo sritį patenkančių didelės rizikos DI sistemų atitiktis to reglamento kibernetinio saugumo reikalavimams pagal tą reglamentą gali būti įrodoma patenkinant tame reglamente išdėstytus esminius kibernetinio saugumo reikalavimus. Jei didelės rizikos DI sistemos tenkina esminius Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams reikalavimus, jos turėtų būti laikomos atitinkančiomis šiame reglamente išdėstytus kibernetinio saugumo reikalavimus, jei tų reikalavimų laikymasis nurodytas pagal reglamentą išduodamoje ES atitikties deklaracijoje ar jos dalyse. Tuo tikslu atliekant kibernetinio saugumo rizikos, susijusios su skaitmeninių elementų turinčiu produktu, pagal šį reglamentą priskiriamu prie didelės rizikos DI sistemų, vertinimą pagal Europos Parlamento ir Tarybos reglamentą dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams urėtų būti atsižvelgiama į riziką DI sistemos kibernetiniam atsparumui, kiek tai susiję su leidimo neturinčių trečiųjų šalių bandymais pakeisti jos naudojimo paskirtį, elgseną ar veikimo efektyvumą, įskaitant DI būdingą pažeidžiamumą, pavyzdžiui, duomenų užkrėtimą arba priešiškus trukdžius, taip pat, kai aktualu, riziką pagrindinėms teisėms, kaip reikalaujama pagal šį reglamentą;

(78) šiame reglamente numatyta atitikties vertinimo procedūra turėtų būti taikoma vertinant skaitmeninių elementų turinčio produkto, kuriam taikomas Europos Parlamento ir Tarybos reglamentas dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams ir kuris pagal šį reglamentą priskiriamas prie didelės rizikos DI sistemų, esminius kibernetinio saugumo reikalavimus. Tačiau dėl šios taisyklės neturėtų sumažėti būtinas skaitmeninių elementų turinčių ypatingos svarbos produktų, kuriems taikomas Europos Parlamento ir Tarybos reglamentas dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, saugumo užtikrinimo lygis. Todėl, nukrypstant nuo šios taisyklės, didelės rizikos DI sistemoms, kurioms taikomas šis reglamentas ir kurios pagal Europos Parlamento ir Tarybos reglamentą dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams taip pat laikomos svarbiais ir skaitmeninių elementų turinčiais ypatingos svarbos produktais ir kurioms taikoma šio reglamento priede nurodyta vidaus kontrole grindžiama atitikties vertinimo procedūra, taikomos Europos Parlamento ir Tarybos reglamento (ES) 2024/…[+] dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams atitikties vertinimo nuostatos, kiek tai susiję su esminiais to reglamento kibernetinio saugumo reikalavimais. Šiuo atveju visų kitų aspektų, kuriems taikomas šis reglamentas, atžvilgiu turėtų būti taikomos atitinkamos šio reglamento priede išdėstytos nuostatos dėl vidaus kontrole grindžiamo atitikties vertinimo. Remdamasi ENISA žiniomis ir patirtimi, kiek tai susiję su kibernetinio saugumo politika ir užduotimis, ENISA pavestomis pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[37], Komisija turėtų bendradarbiauti su ENISA kibernetinio saugumo klausimais, susijusiais su DI sistemomis;

---

[37] 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. 15).

(79) tikslinga nustatyti, kad konkretus fizinis arba juridinis asmuo, kuris apibrėžiamas kaip tiekėjas, prisiimtų atsakomybę už didelės rizikos DI sistemos pateikimą rinkai arba pradėjimą naudoti, neatsižvelgiant į tai, ar tas fizinis arba juridinis asmuo yra sistemą suprojektavęs ar sukūręs asmuo;

(80) Sąjunga ir valstybės narės, kaip Jungtinių Tautų neįgaliųjų teisių konvenciją pasirašiusios šalys, yra teisiškai įpareigotos saugoti asmenis su negalia nuo diskriminacijos ir skatinti jų lygybę, užtikrinti asmenims su neįgalia lygiai su kitais asmenimis informacijos ir ryšių technologijų ir sistemų prieinamumą ir užtikrinti pagarbą asmenų su negalia privatumui. Atsižvelgiant į tai, kad DI sistemos tampa vis svarbesnės ir yra naudojamos vis daugiau, taikant universalumo principus visoms naujoms technologijoms ir paslaugoms turėtų būti užtikrintas visapusiškas ir vienodas prieinamumas visiems, kuriuos gali paveikti DI technologijos arba kurie jomis naudojasi, įskaitant asmenis su negalia, visapusiškai atsižvelgiant į jų prigimtinį orumą ir įvairovę. Todėl labai svarbu, kad tiekėjai užtikrintų visapusišką atitiktį prieinamumo reikalavimams, įskaitant Europos Parlamento ir Tarybos direktyvą (ES) 2016/2102[38] ir Direktyvą (ES) 2019/882. Tiekėjai turėtų užtikrinti, kad šių reikalavimų būtų laikomasi viso ciklo metu. Todėl būtinos priemonės turėtų būti kuo labiau integruotos jau projektuojant didelės rizikos DI sistemą;

---

[38] 2016 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/2102 dėl viešojo sektoriaus institucijų interneto svetainių ir mobiliųjų programų prieinamumo (OL L 327, 2016 12 2, p. 1).

(81) tiekėjas turėtų nustatyti patikimą kokybės valdymo sistemą, užtikrinti, kad būtų įgyvendinta reikalaujama atitikties vertinimo procedūra, parengti atitinkamą dokumentaciją ir nustatyti patikimą priežiūros po pateikimo rinkai sistemą. Didelės rizikos DI sistemų, dėl kurių pagal atitinkamą sektoriaus Sąjungos teisės aktą taikomos su kokybės valdymo sistemomis susijusios pareigos, tiekėjai turėtų turėti galimybę šiame reglamente numatytos kokybės valdymo sistemos elementus įtraukti į esamą kokybės valdymo sistemą, numatytą tame kitame sektoriaus Sąjungos teisės akte. Būsimoje standartizacijos veikloje arba Komisijos priimamose gairėse taip pat turėtų būti atsižvelgiama į šio reglamento ir esamų sektoriaus Sąjungos teisės aktų papildomumą. 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 dalis;

(82) siekiant sudaryti sąlygas šio reglamento vykdymo užtikrinimui ir sukurti vienodas sąlygas veiklos vykdytojams, taip pat atsižvelgiant į įvairias skaitmeninių gaminių tiekimo formas, svarbu užtikrinti, kad Sąjungoje įsisteigęs asmuo visomis aplinkybėmis galėtų institucijoms pateikti visą būtiną informaciją apie DI sistemos atitiktį. Todėl prieš pateikdami savo DI sistemas Sąjungoje, trečiosiose valstybėse įsisteigę tiekėjai rašytiniu įgaliojimu turėtų paskirti Sąjungoje įsisteigusį įgaliotąjį atstovą. Šis įgaliotasis atstovas atlieka pagrindinį vaidmenį užtikrinant didelės rizikos DI sistemų, kurias tie ne Sąjungoje įsisteigę tiekėjai jau pateikė rinkai arba kurios jau pradėtos naudoti Sąjungoje, atitiktį ir yra tų tiekėjų Sąjungoje įsisteigęs kontaktinis asmuo;

(83) atsižvelgiant į DI sistemų vertės grandinės pobūdį ir sudėtingumą ir laikantis naujosios teisės aktų sistemos, labai svarbu užtikrinti teisinį tikrumą ir sudaryti palankesnes sąlygas laikytis šio reglamento. Todėl būtina paaiškinti atitinkamų veiklos vykdytojų toje vertės grandinėje, pavyzdžiui, importuotojų ir platintojų, kurie gali prisidėti prie DI sistemų plėtojimo, vaidmenį ir konkrečias pareigas. Tam tikrais atvejais tie veiklos vykdytojai galėtų vienu metu atlikti daugiau nei vieną funkciją ir todėl turėtų bendrai vykdyti visas atitinkamas pareigas, susijusias su tomis funkcijomis. Pavyzdžiui, veiklos vykdytojas tuo pačiu metu galėtų veikti kaip platintojas ir kaip importuotojas;

(84) siekiant užtikrinti teisinį tikrumą, būtina paaiškinti, kad tam tikromis konkrečiomis sąlygomis bet kuris platintojas, importuotojas, diegėjas ar kita trečioji šalis turėtų būti laikomas didelės rizikos DI sistemos tiekėju ir todėl turėtų prisiimti visas atitinkamas pareigas. Taip būtų tuo atveju, jei ta šalis savo pavadinimą arba prekės ženklą suteiktų jau pateiktai rinkai arba pradėtai naudoti didelės rizikos DI sistemai, nedarant poveikio sutartiniams susitarimams, kuriuose nustatyta, kad pareigos paskirstomos kitaip. Taip būtų ir tuo atveju, jeigu ta šalis iš esmės pakeičia didelės rizikos DI sistemą, kuri jau pateikta rinkai arba pradėta naudoti, taip, kad ji lieka didelės rizikos DI sistema pagal šį reglamentą, arba jeigu ji pakeičia DI sistemos, įskaitant bendrosios paskirties DI sistemą, kuri nebuvo priskiriama didelės rizikos sistemoms ir jau buvo pateikta rinkai arba pradėta naudoti, numatytąją paskirtį taip, kad DI sistema tampa didelės rizikos DI sistema pagal šį reglamentą. Tos nuostatos turėtų būti taikomos nedarant poveikio konkretesnėms nuostatoms, nustatytoms tam tikruose Sąjungos derinamuosiuose teisės aktuose remiantis naująja teisės aktų sistema, su kuriais šis reglamentas turėtų būti taikomas kartu. Pavyzdžiui, Reglamento (ES) 2017/745 16 straipsnio 2 dalis, kuria nustatoma, kad tam tikri pakeitimai neturėtų būti laikomi priemonės pakeitimais, galinčiais turėti įtakos jo atitikčiai taikytiniems reikalavimams, turėtų būti toliau taikoma didelės rizikos DI sistemoms, kurios yra medicinos priemonės, kaip tai suprantama tame reglamente;

(85) bendrosios paskirties DI sistemos pačios gali būti naudojamos kaip didelės rizikos DI sistemos arba gali būti kitų didelės rizikos DI sistemų komponentai. Taigi, dėl ypatingo tų sistemų pobūdžio ir siekiant užtikrinti teisingą pasidalijimą atsakomybe DI vertės grandinėje, tokių bendrosios paskirties sistemų tiekėjai, nepriklausomai nuo to, ar kiti tiekėjai gali naudoti jas kaip didelės rizikos DI sistemas ar jos gali būti naudojamos kaip didelės rizikos DI sistemų komponentai ir jei šiame reglamente nenurodyta kitaip, turėtų glaudžiai bendradarbiauti su atitinkamų didelės rizikos DI sistemų tiekėjais, kad pastarieji galėtų vykdyti atitinkamas pareigas pagal šį reglamentą, ir su pagal šį reglamentą nustatytomis kompetentingomis institucijomis;

(86) jeigu šiame reglamente nustatytomis sąlygomis tiekėjas, kuris iš pradžių pateikė DI sistemą rinkai arba pradėjo ją naudoti, šio reglamento tikslais nebeturėtų toliau būti laikomas tiekėju, ir jeigu tas tiekėjas aiškiai neatmetė galimybės DI sistemą pakeisti didelės rizikos DI sistema, šis buvęs tiekėjas vis tiek turėtų glaudžiai bendradarbiauti ir teikti būtiną informaciją, taip pat suteikti pagrįstai tikėtiną techninę prieigą ir kitą pagalbą, kurių reikia norint įvykdyti šiame reglamente nustatytas pareigas, visų pirma kiek tai susiję su didelės rizikos DI sistemų atitikties vertinimo reikalavimų laikymusi;

(87) be to, jeigu didelės rizikos DI sistema, kuri yra gaminio, kuriam taikomi Sąjungos derinamieji teisės aktai remiantis naująja teisės aktų sistema, saugos komponentas, rinkai nepateikiama arba nepradedama naudoti atskirai nuo gaminio, gaminio gamintojas, apibrėžtas tuose teisės aktuose, turėtų laikytis šiame reglamente tiekėjui nustatytų pareigų, ir visų pirma turėtų užtikrinti, kad galutiniame gaminyje įterpta DI sistema atitiktų šio reglamento reikalavimus;

(88) DI vertės grandinėje daugybė šalių dažnai tiekia DI sistemas ir priemones ir teikia DI paslaugas, taip pat tiekia komponentus ar procesus, kuriuos tiekėjas įtraukia į DI sistemą įvairiais tikslais, be kita ko, kiek tai susiję su modelių mokymu, modelių mokymu iš naujo, modelių bandymu ir vertinimu, integravimu į programinę įrangą ar kitais modelių kūrimo aspektais. Toms šalims vertės grandinėje tenka svarbus vaidmuo didelės rizikos DI sistemos, į kurią yra integruotos jų DI sistemos, priemonės, paslaugos, komponentai ar procesai, tiekėjo atžvilgiu ir jos turėtų rašytiniu susitarimu šiam tiekėjui teikti būtiną informaciją, pajėgumus, techninę prieigą ir kitą pagalbą, grindžiamą visuotinai pripažintais pažangiausiais metodais, kad tiekėjas galėtų visapusiškai vykdyti šiame reglamente nustatytas pareigas, nepakenkdamas savo intelektinės nuosavybės teisėms ar komercinėms paslaptims;

(89) trečiosios šalys, viešam naudojimui tiekiančios priemones, teikiančios paslaugas, tiekiančios procesus ar DI komponentus, išskyrus bendrosios paskirties DI modelius, neturėtų būti įpareigotos laikytis reikalavimų, susijusių su atsakomybe visoje DI vertės grandinėje, visų pirma tiekėjo, kuris juos naudojo arba integravo, atžvilgiu, kai tos priemonės, paslaugos, procesai ar DI komponentai padaromi prieinamais pagal nemokamą ir atvirojo kodo licenciją. Tačiau nemokamų ir atvirojo kodo priemonių, paslaugų, procesų ar DI komponentų, išskyrus bendrosios paskirties DI modelius, kūrėjai turėtų būti skatinami įsivesti plačiai taikomą dokumentavimo praktiką, pvz., modelių korteles ir duomenų lapus – tokiu būdu būtų sparčiau dalijamasi informacija DI vertės grandinėje ir sudaromos sąlygos skatinti patikimas DI sistemas Sąjungoje;

(90) tam, kad palengvintų bendradarbiavimą vertės grandinėje, Komisija galėtų parengti ir rekomenduoti neprivalomas pavyzdines sutarčių tarp didelės rizikos DI sistemų tiekėjų ir trečiųjų šalių, tiekiančių priemones, teikiančių paslaugas, tiekiančių komponentus ar procesus, kurie naudojami didelės rizikos DI sistemoms arba yra į jas integruoti, sąlygas. Rengdama neprivalomas pavyzdines sutarčių sąlygas, Komisija taip pat turėtų atsižvelgti į galimus sutartinius reikalavimus, taikomus konkretiems sektoriams ar verslo atvejams;

(91) atsižvelgiant į DI sistemų pobūdį ir riziką saugumui ir pagrindinėms teisėms, kurios gali būti susijusios su jų naudojimu, be kita ko, kiek tai susiję su poreikiu užtikrinti tinkamą DI sistemos veikimo efektyvumo realiomis sąlygomis stebėseną, yra tikslinga diegėjams nustatyti konkrečias pareigas. Diegėjai visų pirma turėtų imtis tinkamų techninių ir organizacinių priemonių tam, jog užtikrintų, kad didelės rizikos DI sistemas jie naudotų laikydamiesi naudojimosi instrukcijų, be to, turėtų būti numatytos tam tikros kitos pareigos, susijusios atitinkamai su DI sistemų veikimo stebėsena ir įrašų tvarkymu. Be to, diegėjai turėtų užtikrinti, kad asmenys, paskirti įgyvendinti naudojimo instrukcijas ir atlikti žmogaus vykdomą priežiūrą, kaip nustatyta šiame reglamente, turėtų reikiamą kompetenciją, visų pirma turėti tinkamo lygio raštingumą DI srityje, būti baigus mokymus ir turėti įgaliojimus, kad galėtų tinkamai vykdyti tas užduotis. Tos pareigos neturėtų daryti poveikio kitoms diegėjų pareigoms, susijusioms su didelės rizikos DI sistemomis pagal Sąjungos ar nacionalinę teisę;

(92) šiuo reglamentu nedaromas poveikis darbdavių pareigoms apie sprendimus pradėti naudoti arba naudoti DI sistemas informuoti darbuotojus arba jų atstovus arba juos apie tai informuoti ir su jais dėl to konsultuotis pagal Sąjungos ar nacionalinę teisę ir praktiką, įskaitant Europos Parlamento ir Tarybos direktyvą 2002/14/EB[39]. Kai pagal kitas teisines priemones nustatytos sąlygos dėl tokių informavimo arba informavimo ir konsultavimosi pareigų nėra įvykdytos, vis tiek būtina užtikrinti, kad darbuotojai ir jų atstovai būtų informuojami apie planuojamą didelės rizikos DI sistemų diegimą darbo vietoje. Be to, tokia teisė į informaciją yra papildoma ir būtina siekiant tikslo apsaugoti pagrindines teises, kuriomis grindžiamas šis reglamentas. Todėl šiuo tikslu šiame reglamente turėtų būti nustatytas informavimo reikalavimas, nedarant poveikio jokioms esamoms darbuotojų teisėms;

[39] 2002 m. kovo 11 d. Europos Parlamento ir Tarybos direktyva 2002/14/EB dėl bendros darbuotojų informavimo ir konsultavimosi su jais sistemos sukūrimo Europos bendrijoje. (OL L 80, 2002 3 23, p. 29).

(93) nors su DI sistemomis susijusi rizika gali atsirasti dėl sistemos struktūros, ji taip pat gali kilti priklausomai nuo to, kaip DI sistemos naudojamos. Todėl didelės rizikos DI sistemos diegėjai atlieka esminį vaidmenį užtikrindami pagrindinių teisių apsaugą ir taip padeda tiekėjui įvykdyti savo pareigas kuriant DI sistemą. Diegėjai geriausiai supranta, kaip konkrečiai didelės rizikos DI sistema bus naudojama, todėl gali nustatyti potencialiai reikšmingą riziką, kuri nebuvo numatyta kūrimo etape, nes jie turi tikslesnių žinių apie naudojimo kontekstą, asmenis ar jų grupes, kurioms gali būti daromas poveikis, įskaitant pažeidžiamas grupes. Šio reglamento priede išvardytų didelės rizikos DI sistemų diegėjai taip pat atlieka itin svarbų vaidmenį informuodami fizinius asmenis ir, priimdami sprendimus arba padėdami priimti su fiziniais asmenimis susijusius sprendimus, turėtų, kai taikytina, informuoti fizinius asmenis, kad jų atžvilgiu naudojama didelės rizikos DI sistema. Ši informacija turėtų apimti numatytąją paskirtį ir jos priimamų sprendimų rūšį. Diegėjas taip pat turėtų informuoti fizinius asmenis apie jų teisę gauti pagal šį reglamentą pateikiamą paaiškinimą. Kalbant apie teisėsaugos tikslais naudojamas didelės rizikos DI sistemas, ta pareiga turėtų būti įgyvendinama pagal Direktyvos (ES) 2016/680 13 straipsnį;

(94) bet koks biometrinių duomenų tvarkymas, susijęs su DI sistemų naudojimu biometriniam tapatybės nustatymui teisėsaugos tikslais, turi atitikti Direktyvos (ES) 2016/680 10 straipsnį, pagal kurį toks tvarkymas leidžiamas tik kai tai tikrai būtina, taikant tinkamas duomenų subjekto teisių ir laisvių apsaugos priemones ir kai tai leidžiama pagal Sąjungos ar valstybės narės teisę. Toks naudojimas, kai jis leidžiamas, taip pat turi atitikti Direktyvos (ES) 2016/680 4 straipsnio 1 dalyje nustatytus principus, įskaitant teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, tikslumo ir saugojimo apribojimo principus;

(95) nedarant poveikio taikytinai Sąjungos teisei, visų pirma Reglamentui (ES) 2016/679 ir Direktyvai (ES) 2016/680, atsižvelgiant į tai, kad netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos yra intervencinės, netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimui turėtų būti taikomos apsaugos priemonės. Netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos visada turėtų būti naudojamos proporcingai, teisėtai ir tik tiek, kiek būtina, taigi, turėtų būti tikslinės asmenų, kurių tapatybę reikia nustatyti, vietos ir laiko aprėpties atžvilgiu ir grindžiamos uždaru teisėtai įgytos vaizdo medžiagos duomenų rinkiniu. Bet kuriuo atveju netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos neturėtų būti naudojamos teisėsaugos srityje tokiu būdu, kad būtų vykdomas stebėjimas be jokios atrankos. Bet kuriuo atveju netikralaikio nuotolinio biometrinio tapatybės nustatymo sąlygos neturėtų sudaryti pagrindo apeiti draudimo sąlygas ir griežtas išimtis, taikomas tikralaikiam nuotoliniam biometriniam tapatybės nustatymui;

(96) siekiant veiksmingai užtikrinti pagrindinių teisių apsaugą, didelės rizikos DI sistemų diegėjai, kurie yra viešosios teisės reglamentuojamos įstaigos arba viešąsias paslaugas teikiantys privatūs subjektai ir tam tikrų šio reglamento priede išvardytų didelės rizikos DI sistemų diegėjai, pavyzdžiui, bankininkystės subjektai ar draudimo įmonės, prieš pradedant tas sistemas naudoti turėtų atlikti poveikio pagrindinėms teisėms vertinimą. Žmonėms svarbias viešo pobūdžio paslaugas taip pat gali teikti privatūs subjektai. Tokias viešąsias paslaugas teikiantys privatūs veiklos vykdytojai yra siejami su viešojo intereso užduotimis, pavyzdžiui, švietimo, sveikatos priežiūros, socialinių paslaugų, būsto, teisingumo vykdymo srityse. Poveikio pagrindinėms teisėms vertinimo tikslas – kad diegėjas nustatytų konkrečią riziką asmenų ar asmenų grupių, kurie gali būti paveikti, teisėms, ir nustatytų priemones, kurių reikia imtis, jei ta rizika pasireikštų. Poveikio vertinimas turėtų būti atliekamas prieš įdiegiant didelės rizikos DI sistemą ir turėtų būti atnaujinamas, kai diegėjas mano, kad pasikeitė kuris nors svarbus veiksnys. Poveikio vertinime turėtų būti nustatyti atitinkami diegėjo procesai, kuriuos vykdant didelės rizikos DI sistema bus naudojama pagal numatytąją paskirtį, ir turėtų būti aprašytas numatomo sistemos naudojimo laikotarpis ir dažnumas, taip pat konkrečių kategorijų fiziniai asmenys ir grupės, kuriems gali būti daromas poveikis konkrečiomis naudojimo aplinkybėmis.

Vertinimas taip pat turėtų apimti konkrečios žalos, kuri gali turėti įtakos tų asmenų ar grupių pagrindinėms teisėms, rizikos nustatymą. Atlikdamas šį vertinimą diegėjas turėtų atsižvelgti į informaciją, aktualią tinkamam poveikio vertinimui atlikti, įskaitant informaciją, kurią didelės rizikos DI sistemos tiekėjas pateikė naudojimo instrukcijoje, bet ja neapsiribojant. Atsižvelgdami į nustatytą riziką, diegėjai turėtų nustatyti priemones, kurių reikia imtis, jei ta rizika pasireikštų, įskaitant, pavyzdžiui, valdymo priemones tomis konkrečiomis naudojimo aplinkybėmis, pavyzdžiui, žmogaus atliekamos priežiūros, vykdomos laikantis naudojimo instrukcijų, tvarką arba skundų nagrinėjimo ir teisių gynimo procedūras, nes jos galėtų padėti sumažinti riziką pagrindinėms teisėms konkrečiais naudojimo atvejais. Atlikęs tą poveikio vertinimą diegėjas turėtų apie tai pranešti atitinkamai rinkos priežiūros institucijai. Kai tinkama, didelės rizikos DI sistemų diegėjai, ypač tų DI sistemų, kurios yra naudojamos viešajame sektoriuje, siekdami surinkti poveikio vertinimui atlikti būtiną atitinkamą informaciją, į tokių poveikio vertinimų atlikimą ir priemonių, kurių reikia imtis, jei ta rizika pasireikštų, rengimą galėtų įtraukti atitinkamus suinteresuotuosius subjektus, įskaitant asmenų, kuriems DI sistema gali daryti poveikį, grupių atstovus, nepriklausomus ekspertus ir pilietinės visuomenės organizacijas. Europos dirbtinio intelekto tarnyba (toliau - DI tarnyba) turėtų parengti klausimyno šabloną, kad būtų lengviau laikytis reikalavimų ir sumažinama diegėjams tenkanti administracinė našta;

(97) tam, kad būtų užtikrintas teisinis tikrumas, bendrosios paskirties DI modelių sąvoka turėtų būti aiškiai apibrėžta ir atskirta nuo DI sistemų sąvokos. Apibrėžtis turėtų būti grindžiama pagrindinėmis funkcinėmis bendrosios paskirties DI modelio charakteristikomis, visų pirma bendru pobūdžiu ir gebėjimu kompetentingai atlikti įvairias skirtingas užduotis. Šie modeliai paprastai mokomi naudojant didelius duomenų kiekius, taikant įvairius metodus, pavyzdžiui, savipriežiūrą, neprižiūrimą ar sustiprintą mokymąsi. Bendrosios paskirties DI modeliai gali būti pateikiami rinkai įvairiais būdais, be kita ko, per bibliotekas, taikomųjų programų sąsajas (API), tiesiogiai atsisiunčiami arba kaip fizinė kopija. Šie modeliai gali būti toliau keičiami arba pritaikomi prie naujų modelių. Nors DI modeliai yra esminiai DI sistemų komponentai, jie patys savaime nėra DI sistemos. DI modeliams reikia pridėti papildomų komponentų, pavyzdžiui, naudotojo sąsają, kad jie taptų DI sistemomis. DI modeliai paprastai integruojami į DI sistemas ir yra jų dalis. Šiame reglamente nustatomos konkrečios taisyklės, taikomos bendrosios paskirties DI modeliams ir sisteminės rizikos bendrosios paskirties DI modeliams, kurios turėtų būti taikomos ir tada, kai šie modeliai yra integruoti į DI sistemą arba yra jos dalis. Turėtų būti suprantama, kad bendrosios paskirties DI modelių tiekėjų pareigos turėtų būti pradedamos taikyti tuomet, kai bendrosios paskirties DI modeliai pateikiami rinkai.

Kai bendrosios paskirties DI modelio tiekėjas integruoja savo paties modelį į savo paties DI sistemą, kuri tiekiama rinkai arba pradedama naudoti, tas modelis turėtų būti laikomas pateiktu rinkai ir todėl šiame reglamente nustatytos pareigos, susijusios su modeliais, turėtų būti taikomos toliau, kartu su pareigomis, susijusioms su DI sistemomis. Nustatytos su modeliais susijusios pareigos bet kuriuo atveju neturėtų būti taikomos tuomet, kai nuosavas modelis naudojamas tik vidaus procesams, kurie nėra būtini gaminiui tiekti ar paslaugai teikti trečiosioms šalims, ir nedaromas poveikis fizinių asmenų teisėms. Atsižvelgiant į sisteminės rizikos bendrosios paskirties DI modelių galimą didelį neigiamą poveikį, šių modelių atžvilgiu visada turėtų būti taikomos atitinkamos pareigos pagal šį reglamentą. Apibrėžtis neturėtų apimti DI modelių, naudojamų prieš pateikiant juos rinkai tik mokslinių tyrimų, plėtros ir prototipų kūrimo tikslais. Tai nedaro poveikio pareigai laikytis šio reglamento, kai po tokios veiklos modelis pateikiamas rinkai;

(98) kadangi modelio bendras pobūdis, *inter alia*, taip pat galėtų būti nustatomas pagal parametrų skaičių, turėtų būti laikoma, kad modeliai, turintys ne mažiau kaip milijardą parametrų ir apmokyti naudojant didelį duomenų kiekį savipriežiūros būdu, yra labai bendro pobūdžio ir gali kompetentingi atlikti įvairias skirtingas užduotis;

(99) dideli generatyviniai DI modeliai yra tipinis bendrosios paskirties DI modelio pavyzdys, nes jie suteikia galimybę lanksčiai generuoti turinį, pavyzdžiui, teksto, judamo ar nejudamo vaizdo arba garso forma, ir gali lengvai atlikti įvairias atskiras užduotis;

(100) kai bendrosios paskirties DI modelis yra integruotas į DI sistemą arba yra jos dalis, ši sistema turėtų būti laikoma bendrosios paskirties DI sistema, kai dėl šios integracijos ši sistema gali būti naudojama įvairiais tikslais. Bendrosios paskirties DI sistema gali būti naudojama tiesiogiai arba būti integruota į kitas DI sistemas;

(101) bendrosios paskirties DI modelių tiekėjams tenka ypatingas vaidmuo ir atsakomybė visoje DI vertės grandinėje, nes jų tiekiami modeliai gali būti pagrindu įvairioms tolesnės grandies sistemoms, kurias dažnai teikia tolesnės grandies tiekėjai, kuriems reikia gerai suprasti modelius ir jų pajėgumus, kad jie galėtų integruoti tokius modelius į savo gaminius ir vykdyti savo pareigas pagal šį ar kitus reglamentus. Todėl turėtų būti nustatytos proporcingos skaidrumo priemonės, įskaitant dokumentų rengimą ir nuolatinį atnaujinimą, taip pat informacijos apie bendrosios paskirties DI modelį teikimą, kad ja galėtų naudotis tolesnės grandies tiekėjai. Bendrosios paskirties DI modelio tiekėjas turėtų parengti ir nuolat atnaujinti techninius dokumentus, kad paprašius jie būtų pateikiami DI tarnybai ir nacionalinėms kompetentingoms institucijoms. Bent minimalus elementų, kurie turi būti įtraukti į tokius dokumentus, rinkinys turėtų būti pateikiamas specialiuosiuose šio reglamento prieduose. Komisijai turėtų būti suteikiami įgaliojimai deleguotaisiais aktais iš dalies keisti tuos priedus atsižvelgiant į technologinę plėtrą;

(102) programinė įranga ir duomenys, įskaitant modelius, išleidžiami pagal nemokamą ir atvirojo kodo licenciją, pagal kurią jais galima atvirai dalytis, kai naudotojai gali laisvai prieiti prie jų arba pakeistų jų versijų, juos naudoti, keisti ir platinti, gali prisidėti prie mokslinių tyrimų ir inovacijų rinkoje, taip pat gali suteikti reikšmingų Sąjungos ekonomikos augimo galimybių. Turėtų būti laikoma, kad bendrosios paskirties DI modeliai, išleidžiami pagal nemokamas ir atvirojo kodo licencijas, užtikrina aukšto lygio skaidrumą ir atvirumą, jei jų parametrai, įskaitant svorius, informaciją apie modelio architektūrą ir informaciją apie modelio naudojimą, yra skelbiami viešai. Licencija turėtų būti laikoma nemokama ir atvira ir tuo atveju, kai pagal ją naudotojai gali paleisti, kopijuoti, platinti, tirti, keisti ir tobulinti programinę įrangą ir duomenis, įskaitant modelius, su sąlyga, kad būtų nurodytas pirminis modelio tiekėjas ir laikomasi identiškų ar palyginamų platinimo sąlygų;

(103) nemokami ir atvirojo kodo DI komponentai apima programinę įrangą ir duomenis, įskaitant modelius ir bendrosios paskirties DI modelius, DI sistemos priemones, paslaugas ar procesus. Nemokami ir atvirojo kodo DI komponentai gali būti gaunami įvairiais kanalais, įskaitant jų kūrimą atvirose duomenų saugyklose. Šio reglamento tikslais DI komponentams, kurie tiekiami už tam tikrą kainą arba kitaip monetizuojami, be kita ko, teikiant techninės paramos ar kitas paslaugas, taip pat ir per programinės įrangos platformą, susijusias su DI komponentu, arba naudojant asmens duomenis kitais nei tik programinės įrangos saugumo, suderinamumo ar sąveikumo didinimo tikslais, išskyrus sandorius tarp labai mažų įmonių, neturėtų būti taikomos išimtys, kurios yra taikomos nemokamo ir atvirojo kodo DI komponentams. Tai, kad DI komponentai yra prieinami per atviras duomenų saugyklas, neturėtų savaime reikšti monetizavimo;

(104) bendrosios paskirties DI modelių, kurie išleidžiami pagal nemokamą ir atvirojo kodo licenciją ir kurių parametrai, įskaitant svorius, informaciją apie modelio architektūrą ir informaciją apie modelio naudojimą, yra viešai skelbiami, tiekėjams turėtų būti taikomos su skaidrumu susijusių reikalavimų, taikomų bendrosios paskirties DI modeliams, išimtys, nebent jie gali būti laikomi keliančiais sisteminę riziką – tokiu atveju aplinkybė, kad modelis yra skaidrus ir prie jo pridėta atvirojo kodo licencija, neturėtų būti laikoma pakankama priežastimi nesilaikyti šiame reglamente nustatytų pareigų. Bet kuriuo atveju, atsižvelgiant į tai, kad išleidžiant bendrosios paskirties DI modelius pagal laisvojo ir atvirojo kodo licenciją nebūtinai atskleidžiama esminė informaciją apie duomenų rinkinį, naudojamą modeliui mokyti ar pritaikyti, ir apie tai, kaip buvo užtikrintas autorių teisių teisės laikymasis, bendrosios paskirties DI modeliams numatyta išimtis dėl su skaidrumu susijusių reikalavimų laikymosi neturėtų būti taikoma pareigai parengti santrauką apie modelių mokymui naudojamą turinį ir pareigai nustatyti politiką siekiant laikytis Sąjungos autorių teisių teisės, visų pirma siekiant nustatyti išlygas dėl pasiliekamų teisių ir tų išlygų laikytis pagal Europos Parlamento ir Tarybos direktyvos (ES) 2019/790[40] 4 straipsnio 3 dalį;

[40] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/790 dėl autorių teisių ir gretutinių teisių bendrojoje skaitmeninėje rinkoje, kuria iš dalies keičiamos direktyvos 96/9/EB ir 2001/29/EB (OL L 130, 2019 5 17, p. 92).

(105) bendrosios paskirties DI modeliai, visų pirma dideli generatyviniai DI modeliai, galintys generuoti tekstą, vaizdus ir kitą turinį, ne tik suteikia unikalių inovacijų galimybių, bet ir kelia iššūkių menininkams, autoriams ir kitiems kūrėjams ir jų kūrybinio turinio kūrimo, platinimo, naudojimo ir vartojimo būdui. Kuriant ir mokant tokius modelius reikia prieigos prie didžiulio tekstų, vaizdų, vaizdo įrašų ir kitų duomenų kiekio. Šiame kontekste tekstų ir duomenų gavybos metodai gali būti plačiai naudojami tokio turinio, kuris gali būti saugomas autorių teisių ir gretutinių teisių, paieškai ir analizei. Norint naudoti autorių teisių saugomą turinį, reikia gauti atitinkamo teisių turėtojo leidimą, nebent taikomos atitinkamos autorių teisių išimtys ir apribojimai. Direktyvoje (ES) 2019/790 nustatytos išimtys ir apribojimai, pagal kuriuos tam tikromis sąlygomis leidžiamas kūrinių ar kitų objektų atgaminimas ir perkėlimas tekstų ir duomenų gavybos tikslais. Pagal šias taisykles teisių turėtojai gali nuspręsti pasilikti sau teises į savo kūrinius ar kitus objektus, kad užkirstų kelią tekstų ir duomenų gavybai, nebent tai daroma mokslinių tyrimų tikslais. Kai atsisakymo teisės buvo aiškiai tinkamu būdu pasiliktos, bendrosios paskirties DI modelių tiekėjai, norintys vykdyti tokių kūrinių tekstų ir duomenų gavybą, turi gauti teisių turėtojų leidimą;

(106) tiekėjai, kurie pateikia bendrosios paskirties DI modelius Sąjungos rinkai, turėtų užtikrinti, kad būtų vykdomos atitinkamos šiame reglamente nustatytos pareigos. Tuo tikslu bendrosios paskirties DI modelių tiekėjai turėtų nustatyti politiką siekiant laikytis Sąjungos autorių teisių ir gretutinių teisių teisės, visų pirma siekiant pagal Europos Parlamento ir Tarybos direktyvos (ES) 2019/790 4 straipsnio 3 dalį nustatyti išlygas dėl pasiliekamų teisių, apie kurias pareiškė teisių turėtojai, ir tų išlygų laikytis. Bet kuris tiekėjas, pateikiantis bendrosios paskirties DI modelį Sąjungos rinkai, turėtų vykdyti šią pareigą, nepriklausomai nuo jurisdikcijos, kurioje taikomi su autorių teisėmis susiję aktai, kuriais grindžiamas tų bendrosios paskirties DI modelių mokymas. Tai yra būtina siekiant užtikrinti vienodas sąlygas bendrosios paskirties DI modelių tiekėjams, kad nė vienas tiekėjas neįgytų konkurencinio pranašumo Sąjungos rinkoje taikydamas žemesnius autorių teisių standartus nei Sąjungoje taikomi standartai;

(107) siekiant padidinti duomenų, naudojamų bendrosios paskirties DI modelių išankstiniam mokymui ir mokymui, įskaitant autorių teisių teisės saugomus tekstus ir duomenis, skaidrumą, yra tikslinga, kad tokių modelių tiekėjai parengtų ir viešai paskelbtų pakankamai išsamią turinio, naudojamo apmokant bendrosios paskirties DI modelį, santrauką. Tinkamai atsižvelgiant į poreikį apsaugoti komercines paslaptis ir konfidencialią verslo informaciją, ši santrauka turėtų būti išsami iš esmės, o ne detali techniškai, kad teisėtų interesų turinčioms šalims, įskaitant autorių teisių turėtojus, būtų lengviau naudotis savo teisėmis pagal Sąjungos teisę ir užtikrinti jų vykdymą, pavyzdžiui, išvardijant pagrindines duomenų rinkinius, kurie buvo naudojami mokant modelį, kaip antai dideles privačias ar viešas duomenų bazes ar duomenų archyvus, ir pateikiant paaiškinimą apie kitus naudojamus duomenų šaltinius. Tikslinga, kad DI tarnyba pateiktų santraukos šabloną, ir jis turėtų būti paprastas, veiksmingas ir leistų tiekėjui pateikti reikalaujamą santrauką aprašomąja forma;

(108) kalbant apie bendrosios paskirties DI modelių tiekėjams nustatytas pareigas nustatyti politiką siekiant užtikrinti Sąjungos autorių teisių teisės laikymąsi ir viešai paskelbti mokymui naudojamo turinio santrauką, DI tarnyba turėtų stebėti, ar tiekėjas įvykdė tas pareigas, nevykdydama patikrinimo ar nesiimdama mokymo duomenų vertinimo kiekvieno kūrinio atveju, kiek tai susiję su autorių teisių laikymusi. Šiuo reglamentu nedaromas poveikis autorių teisių taisyklių, numatytų pagal Sąjungos teisę, vykdymo užtikrinimui;

(109) bendrosios paskirties DI modelių tiekėjams taikomų pareigų vykdymas turėtų būti atitinkamas ir proporcingas modelio tiekėjo tipui, išskyrus būtinybę laikytis reikalavimų asmenims, kurie modelius kuria arba naudoja neprofesiniais ar mokslinių tyrimų tikslais, tačiau jie turėtų būti skatinami savanoriškai laikytis šių reikalavimų. Nedarant poveikio Sąjungos autorių teisių teisei, užtikrinant tų pareigų vykdymą turėtų būti tinkamai atsižvelgiama į paslaugų teikėjo dydį, o MVĮ, įskaitant startuolius, turėtų būti sudarytos sąlygos vykdyti pareigas supaprastintais būdais, kurie neturėtų būti pernelyg brangūs ir neatgrasytų nuo tokių modelių naudojimo. Modelio pakeitimo arba pritaikymo atveju bendrosios paskirties DI modelių tiekėjų pareigos turėtų apsiriboti tuo pakeitimu arba pritaikymu, pavyzdžiui, esamų techninių dokumentų papildymu informacija apie pakeitimus, įskaitant naujus mokymo duomenų šaltinius, kaip priemonę vykdyti šiame reglamente nustatytas vertės grandinės pareigas;

(110) bendrosios paskirties DI modeliai galėtų kelti sisteminę riziką, kuri apima (bet tuo neapsiriboja) bet kokį faktinį ar pagrįstai numatomą neigiamą poveikį, susijusį su didelėmis avarijomis, sutrikimais ypatingos svarbos sektoriuose ir rimtomis pasekmėmis visuomenės sveikatai ir saugai; bet kokį faktinį ar pagrįstai numatomą neigiamą poveikį demokratiniams procesams, visuomenės ir ekonominiam saugumui; neteisėto, melagingo ar diskriminacinio turinio sklaidą. Turėtų būti suprantama, kad sisteminė rizika auga didėjant modelio pajėgumams ir modelio aprėpčiai, ji gali kilti visą modelio gyvavimo ciklą ir jai įtakos turi netinkamo naudojimo sąlygos, modelio patikimumas, modelio sąžiningumas ir modelio saugumas, modelio savarankiškumo lygis, jo prieiga prie priemonių, naujoviški ar suderinti būdai, išleidimo ir platinimo strategijos, apsaugos priemonių pašalinimo galimybės ir kiti veiksniai. Visų pirma taikant tarptautinius požiūrius iki šiol nustatyta, kad reikia atkreipti dėmesį į riziką, kylančią dėl galimo tyčinio netinkamo naudojimo ar nenumatytų kontrolės problemų, susijusių su derinimu su žmogaus ketinimu; cheminę, biologinę, radiologinę ir branduolinę riziką, pavyzdžiui, būdus, kuriais galima sumažinti patekimo į rinką kliūtis, be kita ko, kiek tai susiję su ginklų kūrimu, projektavimu, įsigijimu ar naudojimu; kibernetinius puolimo pajėgumus, pavyzdžiui, būdus, kuriais gali būti sudarytos sąlygos nustatyti pažeidžiamumą, jį išnaudoti ar juo pasinaudoti operatyviniais tikslais; sąveikos ir priemonių naudojimo poveikį, įskaitant, pavyzdžiui, gebėjimą kontroliuoti fizines sistemas ir trikdyti ypatingos svarbos infrastruktūrą; riziką, kylančią dėl to, kad modeliai kopijuoja patys save, atkartoja save ar moko kitus modelius; būdus, kuriais modeliai gali sukelti žalingą šališkumą ir diskriminaciją, keliančius riziką asmenims, bendruomenėms ar visuomenei; palankių sąlygų dezinformacijai sudarymą arba kenkimą privatumui, sukeliant grėsmę demokratinėms vertybėms ir žmogaus teisėms; riziką, kad konkretus įvykis galėtų sukelti grandininę reakciją ir didelį neigiamą poveikį, kuris galėtų paveikti visą miestą, visos srities veiklą ar visą bendruomenę;

(111) tikslinga nustatyti bendrosios paskirties DI modelių priskyrimo sisteminės rizikos bendrosios paskirties DI modeliams metodiką. Kadangi sisteminė rizika kyla dėl ypač didelių pajėgumų, turėtų būti laikoma, kad bendrosios paskirties DI modelis kelia sisteminę riziką, jei jo pajėgumai daro didelį poveikį, vertinant remiantis tinkamomis techninėmis priemonėmis ir metodikomis, arba reikšmingą poveikį vidaus rinkai dėl jo aprėpties. Didelio poveikio pajėgumai bendrosios paskirties DI modeliuose – tai pajėgumai, kurie atitinka arba viršija pažangiausiuose bendrosios paskirties DI modeliuose užfiksuotus pajėgumus. Visus modelio pajėgumus galima geriau suprasti po to, kai modelis pateiktas į rinką arba kai diegėjai sąveikauja su modeliu. Atsižvelgiant į naujausius technikos laimėjimus šio reglamento įsigaliojimo metu, bendrosios paskirties DI modelio mokymui naudojama bendra skaičiuojamoji galia, išmatuota slankiojo kablelio operacijomis, yra viena iš modelių pajėgumų atitinkamų aproksimacijų. Mokymui naudojama bendra skaičiavimo galia apima skaičiavimą, naudojamą visai veiklai ir metodams, kuriais siekiama padidinti modelio pajėgumus iki jo įdiegimo, pvz., parengiamajam mokymui, sintetinių duomenų generavimui ir pritaikymui. Todėl turėtų būti nustatyta pradinė slankiojo kablelio operacijų ribinė vertė, dėl kurios, jei ją atitinka bendrosios paskirties DI modelis, galima preziumuoti, kad modelis yra sisteminės rizikos bendrosios paskirties DI modelis. Ši ribinė vertė laikui bėgant turėtų būti koreguojama, kad būtų atspindėti technologiniai ir pramonės pokyčiai, pavyzdžiui, algoritmų patobulinimai arba padidėjęs aparatinės įrangos efektyvumas, ir turėtų būti papildyta modelių pajėgumo lyginamaisiais parametrais ir rodikliais.

Šiam tikslui reikalingai informacijai gauti DI tarnyba turėtų bendradarbiauti su mokslo bendruomene, pramonės atstovais, pilietine visuomene ir kitais ekspertais. Pagal ribines vertes, taip pat didelio poveikio pajėgumų vertinimo priemones ir lyginamuosius parametrus turėtų būti prognozuojama, kas yra bendrosios paskirties DI modelių bendroji paskirtis, pajėgumai ir susijusi sisteminė rizika, ir tomis vertėmis, priemonėmis ir lyginamaisiais parametrais galėtų būti atspindima tai, kokiu būdu modelis bus pateiktas rinkai, arba į naudotojų, kuriems jis gali padaryti poveikį, skaičių. Siekiant papildyti šią sistemą, Komisija turėtų turėti galimybę priimti atskirus sprendimus, kuriais bendrosios paskirties DI modelis būtų priskiriamas sisteminės rizikos bendrosios paskirties DI modeliams, jei nustatoma, kad tokio modelio pajėgumai arba poveikis yra lygiaverčiai nustatytoms ribinėms vertėms. Tas sprendimas turėtų būti priimtas remiantis šio reglamento priede pateiktų priskyrimo sisteminės rizikos bendrosios paskirties DI modeliams kriterijų, pavyzdžiui, mokymo duomenų rinkinio kokybės ar dydžio, verslo ir galutinių naudotojų skaičiaus, įvesties ir išvesties būdų, savarankiškumo lygio ir išplečiamumo, arba priemonių, prie kurių turima prieiga, bendru vertinimu. Gavusi pagrįstą tiekėjo, kurio modelis priskirtas sisteminės rizikos bendrosios paskirties DI modeliams, prašymą, Komisija turėtų atsižvelgti į prašymą ir gali nuspręsti iš naujo įvertinti, ar šis bendrosios paskirties DI modelis vis dar gali būti laikomas keliančiu sisteminę riziką;

(112) taip pat būtina paaiškinti priskyrimo sisteminės rizikos bendrosios paskirties DI modeliams procedūrą. Turėtų būti preziumuojama, kad bendrosios paskirties DI modelis, atitinkantis taikytiną didelio poveikio pajėgumų ribinę vertę, yra sisteminės rizikos bendrosios paskirties DI modelis. Tiekėjas turėtų pateikti pranešimą DI tarnybai ne vėliau kaip per dvi savaites nuo reikalavimų įvykdymo arba nuo tada, kai sužinoma, kad bendrosios paskirties DI modelis atitiks reikalavimus, kuriais remiantis daroma tokia prezumpcija. Tai ypač svarbu atsižvelgiant į slankiojo kablelio operacijų ribinę vertę, nes bendrosios paskirties DI modelių mokymo tikslu būtinas išsamus planavimas, kuris apima išankstinį skaičiavimo išteklių paskirstymą, todėl bendrosios paskirties DI modelių tiekėjai gali žinoti, ar jų modelis atitiks ribinę vertę, prieš užbaigiant mokymą. Teikdamas tą pranešimą tiekėjas turėtų galėti įrodyti, kad dėl savo specifinių savybių bendrosios paskirties DI modelis išimtinai nekelia sisteminės rizikos, todėl jis neturėtų būti priskiriamas sisteminės rizikos bendrosios paskirties DI modeliams. Ta informacija yra vertinga DI tarnybai, kad ji galėtų numatyti sisteminės rizikos bendrosios paskirties DI modelių pateikimą rinkai, o tiekėjai gali iš anksto pradėti bendradarbiauti su DI tarnyba. Ta informacija yra itin svarbi dėl bendrosios paskirties DI modelių, kuriuos planuojama išleisti kaip atvirojo kodo modelius, atsižvelgiant į tai, kad po atvirojo kodo modelio išleidimo gali būti sunkiau įgyvendinti būtinas priemones siekiant užtikrinti, kad būtų vykdomos šiame reglamente nustatytos pareigos;

(113) jei Komisijai tampa žinoma, kad bendrosios paskirties DI modelis atitinka priskyrimo sisteminės rizikos bendrosios paskirties DI modeliams reikalavimus, ir šis faktas anksčiau nebuvo žinomas arba apie jį atitinkamas tiekėjas Komisijai nepranešė, Komisijai turėtų būti suteikti įgaliojimai tą modelį atitinkamai priskirti. Kvalifikuotų perspėjimų sistema turėtų užtikrinti, kad mokslinė komisija informuotų DI tarnybą apie bendrosios paskirties DI modelius, kurie galbūt turėtų būti priskirti sisteminės rizikos bendrosios paskirties DI modeliams, taip papildant DI tarnybos vykdomą stebėsenos veiklą;

(114) sisteminės rizikos bendrosios paskirties DI modelių tiekėjams, turėtų būti taikomos ne tik bendrosios paskirties DI modelių tiekėjams numatytos pareigos, bet ir pareigos, kuriomis siekiama nustatyti ir sumažinti tą riziką ir užtikrinti tinkamą kibernetinio saugumo apsaugos lygį, neatsižvelgiant į tai, ar modelis tiekiamas kaip atskiras modelis, ar yra integruotas į DI sistemą arba gaminį. Kad tie tikslai būtų pasiekti, šiuo reglamentu tiekėjams turėtų būti nustatytas reikalavimas atlikti būtinus modelių vertinimus, visų pirma prieš pirmą kartą juos pateikiant rinkai, įskaitant modelių atsparumo kenksmingiems veiksmams bandymą ir dokumentavimą, taip pat, kai tinkama, atliekant vidaus ar nepriklausomą išorės bandymą. Be to, sisteminės rizikos bendrosios paskirties DI modelių tiekėjai turėtų nuolat vertinti ir mažinti sisteminę riziką, be kita ko, pavyzdžiui, nustatydami rizikos valdymo politiką, kaip antai atskaitomybės ir valdymo procesus, įgyvendindami priežiūrą po pateikimo rinkai, imdamiesi tinkamų priemonių per visą modelio gyvavimo ciklą ir bendradarbiaudami su atitinkamais DI vertės grandinės dalyviais;

(115) sisteminės rizikos bendrosios paskirties DI modelių tiekėjai turėtų įvertinti ir mažinti galimą sisteminę riziką. Jei, nepaisant pastangų nustatyti riziką, susijusią su bendrosios paskirties DI modeliu, kuris gali kelti sisteminę riziką, ir užkirsti jai kelią, dėl modelio kūrimo ar naudojimo įvyksta rimtas incidentas, bendrosios paskirties DI modelio tiekėjas turėtų nepagrįstai nedelsdamas stebėti incidentą ir pateikti Komisijai ir nacionalinėms kompetentingoms institucijoms visą svarbią informaciją ir pranešti apie galimas taisomąsias priemones. Be to, tiekėjai turėtų užtikrinti tinkamą modelio ir jo fizinės infrastruktūros kibernetinio saugumo apsaugos lygį, jei tinkama, visą modelio gyvavimo ciklą. Užtikrinant kibernetinį saugumą sisteminės rizikos, susijusios su piktavališku naudojimu ar išpuoliais, atžvilgiu turėtų būti tinkamai atsižvelgiama į atsitiktinį modelio konfidencialios informacijos atskleidimą, neteisėtą išleidimą, saugos priemonių apėjimą ir gynybą nuo kibernetinių išpuolių, neteisėtos prieigos ar modelio vagystės. Tą apsaugą būtų galima palengvinti užtikrinant modelių svorių, algoritmų, serverių ir duomenų rinkinių apsaugą, pavyzdžiui, taikant informacijos saugumui užtikrinti skirtas operatyvines saugumo priemones, konkrečią kibernetinio saugumo politiką, tinkamus techninius ir nustatytus sprendimus, taip pat kibernetinės ir fizinės prieigos kontrolės priemones, tinkančias pagal atitinkamas aplinkybes ir susijusią riziką;

(116) DI tarnyba turėtų skatinti ir palengvinti praktikos kodeksų rengimą, peržiūrą ir pritaikymą, atsižvelgiant į tarptautinius požiūrius. Visi bendrosios paskirties DI modelių tiekėjai galėtų būti pakviesti dalyvauti. Siekiant užtikrinti, kad praktikos kodeksai atspindėtų naujausius technikos laimėjimus ir juose būtų tinkamai atsižvelgta į įvairias perspektyvas, DI tarnyba turėtų bendradarbiauti su atitinkamomis nacionalinėmis kompetentingomis institucijomis ir galėtų, kai tinkama, dėl tokių kodeksų rengimo konsultuotis su pilietinės visuomenės organizacijomis ir kitais atitinkamais suinteresuotaisiais subjektais bei ekspertais, įskaitant specialistų grupę. Praktikos kodeksai turėtų apimti bendrosios paskirties DI modelių ir sisteminės rizikos bendrosios paskirties modelių tiekėjų pareigas. Be to, kiek tai susiję su sistemine rizika, praktikos kodeksai turėtų padėti nustatyti sisteminės rizikos rūšių ir pobūdžio taksonomiją Sąjungos lygmeniu, įskaitant jos šaltinius. Praktikos kodeksuose daug dėmesio turėtų būti skiriama ir konkrečioms rizikos vertinimo ir mažinimo priemonėms;

(117) praktikos kodeksai turėtų būti svarbiausia priemonė, kad bendrosios paskirties DI modelių tiekėjai galėtų tinkamai vykdyti pagal šį reglamentą numatytas pareigas. Tiekėjai turėtų galėti remtis praktikos kodeksais, kad įrodytų, jog vykdo pareigas. Komisija, priimdama įgyvendinimo aktus, gali nuspręsti patvirtinti praktikos kodeksą ir nustatyti jo bendrą galiojimą Sąjungoje arba, kita vertus, nustatyti bendras atitinkamų pareigų vykdymo taisykles, jei iki šio reglamento taikymo pradžios praktikos kodekso negalima užbaigti arba DI tarnyba jį laiko netinkamu. Kai darnusis standartas paskelbiamas ir DI tarnyba jį įvertina kaip tinkamą atitinkamoms pareigoms vykdyti, atitiktis Europos darniajam standartui turėtų suteikti tiekėjų atžvilgiu atitikties prezumpciją. Be to, bendrosios paskirties DI modelių tiekėjai turėtų galėti įrodyti atitiktį naudodami alternatyvias tinkamas priemones, jei praktikos kodeksų ar darniųjų standartų nėra arba jie nusprendžia jais nesiremti;

(118) šiuo reglamentu DI sistemos ir DI modeliai reglamentuojami nustatant tam tikrus reikalavimus ir pareigas atitinkamiems rinkos dalyviams, kurie juos pateikia rinkai, pradeda naudoti arba naudoja Sąjungoje, taip papildant tarpininkavimo paslaugų teikėjų, kurie integruoja tokias sistemas ar modelius į savo paslaugas, pareigas, reglamentuojamas Reglamentu (ES) 2022/2065. Tokiu mastu, kokiu tokios sistemos ar modeliai yra integruoti į interneto platformų ir interneto paieškos sistemų, kurioms suteiktas atitinkamai labai didelių interneto platformų ar labai didelių interneto paieškos sistemų statusas, jiems taikoma Reglamente (ES) 2022/2065 numatyta rizikos valdymo sistema. Todėl turėtų būti preziumuojama, kad atitinkamos šiame reglamente nustatytos pareigos yra įvykdytos, nebent kiltų ir tokiuose modeliuose būtų nustatyta reikšminga sisteminė rizika, kuriai netaikomas Reglamentas (ES) 2022/2065. Pagal šią sistemą labai didelių interneto platformų ir labai didelių interneto paieškos sistemų paslaugų teikėjai privalo įvertinti galimą sisteminę riziką, kylančią dėl jų paslaugų projektavimo, veikimo ir naudojimo, įskaitant tai, kaip teikiant paslaugą naudojamų algoritmų sistemų dizainas gali prisidėti prie tokios rizikos, taip pat sisteminę riziką, kylančią dėl galimo netinkamo naudojimo. Šie paslaugų teikėjai taip pat privalo imtis tinkamų rizikos mažinimo priemonių laikydamiesi pagrindinių teisių;

(119) atsižvelgiant į spartų inovacijų ir technologinės raidos tempą, kiek tai susiję su skaitmeninėmis paslaugomis, kurioms taikomos įvairios Sąjungos teisės priemonės, visų pirma atsižvelgiant į jų gavėjų naudojimąsi jomis ir suvokimą, DI sistemos, kurioms taikomas šis reglamentas, gali būti teikiamos kaip tarpininkavimo paslaugos arba jų dalys, kaip tai suprantama Reglamente (ES) 2022/2065, kurios turėtų būti aiškinamos technologijų atžvilgiu neutraliu būdu. Pavyzdžiui, DI sistemos gali būti naudojamos interneto paieškos sistemoms teikti, visų pirma tiek, kiek DI sistema, pavyzdžiui, internetinis pokalbių robotas, iš esmės atlieka paiešką visose interneto svetainėse, tada rezultatus įtraukia į savo turimas žinias ir naudoja atnaujintas žinias, kad sugeneruotų bendrą išvedinį, apimantį skirtingus informacijos šaltinius;

(120) be to, šiame reglamente tam tikrų DI sistemų tiekėjams ir diegėjams nustatytos pareigos, siekiant sudaryti sąlygas nustatyti ir atskleisti tai, kad tų sistemų išvediniai yra dirbtinai sugeneruoti arba gauti atlikus manipuliacijas, yra itin aktualios siekiant palengvinti veiksmingą Reglamento (ES) 2022/2065 įgyvendinimą. Tai visų pirma taikoma labai didelių interneto platformų arba labai didelių interneto paieškos sistemų paslaugų teikėjų pareigoms nustatyti ir sumažinti sisteminę riziką, galinčią kilti dėl turinio, kuris buvo dirbtinai sugeneruotas ar gautas atlikus manipuliacijas, sklaidos, visų pirma faktinio ar numatomo neigiamo poveikio demokratiniams procesams, pilietiniam diskursui ir rinkimų procesams, be kita ko, pasitelkiant dezinformaciją, riziką;

(121) standartizacija turėtų atlikti svarbų vaidmenį, kad tiekėjams būtų suteikti techniniai sprendimai siekiant užtikrinti atitiktį šiam reglamentui, atsižvelgiant į naujausius technikos laimėjimus, skatinti inovacijas, taip pat konkurencingumą ir augimą bendrojoje rinkoje. Atitiktis darniesiems standartams, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012[41] 2 straipsnio 1 dalies c punkte, kurie, tikėtina, paprastai turėtų būti rengiami atsižvelgiant į naujausius technikos laimėjimus, turėtų būti viena iš priemonių tiekėjams įrodyti atitiktį šio reglamento reikalavimams. Todėl turėtų būti skatinamas subalansuotas atstovavimas interesams, į standartų rengimą įtraukiant visus atitinkamus suinteresuotuosius subjektus, visų pirma MVĮ, vartotojų organizacijas ir aplinkos bei socialinės srities suinteresuotuosius subjektus pagal Reglamento (ES) Nr. 1025/2012 5 ir 6 straipsnius. Kad būtų palengvinta atitiktis, standartizacijos prašymus Komisija turėtų pateikti nepagrįstai nedelsdama. Rengdama standartizacijos prašymą Komisija konsultuojasi su patariamuoju forumu ir valdyba, kad surinktų atitinkamų ekspertinių žinių. Tačiau, nesant atitinkamų nuorodų į darniuosius standartus, Komisija turėtų galėti įgyvendinimo aktais, pasikonsultavusi su patariamuoju forumu, nustatyti tam tikrų šiame reglamente nustatytų reikalavimų bendrąsias specifikacijas.

---

[41] 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).

Bendroji specifikacija turėtų būti išimtinis atsarginis sprendimas siekiant palengvinti tiekėjo pareigą laikytis šio reglamento reikalavimų, kai nė viena iš Europos standartizacijos organizacijų nepriima standartizacijos prašymo arba kai atitinkamuose darniuosiuose standartuose nepakankamai atsižvelgiama į pagrindinių teisių klausimus, arba kai darnieji standartai neatitinka prašymo, arba kai vėluojama priimti tinkamą darnųjį standartą. Jei priimti darnųjį standartą vėluojama dėl techninio to standarto sudėtingumo, Komisija turėtų į tai atsižvelgti prieš svarstydama galimybę nustatyti bendrąsias specifikacijas. Komisija raginama rengiant bendrąsias specifikacijas bendradarbiauti su tarptautiniais partneriais ir tarptautinėmis standartizacijos institucijomis;

(122) tikslinga, kad, nedarant poveikio darniųjų standartų ir bendrųjų specifikacijų naudojimui, turėtų būti laikoma, kad didelės rizikos DI sistemos, kuri buvo išmokyta ir išbandyta naudojant duomenis, atspindinčius konkrečią geografinę, elgsenos, kontekstinę ar funkcinę aplinką, kurioje DI sistemą ketinama naudoti, tiekėjai laikosi atitinkamos priemonės, numatytos pagal šiame reglamente nustatytą duomenų valdymo reikalavimą. Nedarant poveikio šiame reglamente nustatytiems reikalavimams, susijusiems su patvarumu ir tikslumu, vadovaujantis Reglamento (ES) 2019/881 54 straipsnio 3 dalimi, turėtų būti preziumuojama, kad didelės rizikos DI sistemos, kurios buvo sertifikuotos arba kurių atitikties pareiškimas buvo išduotas pagal kibernetinio saugumo sertifikavimo schemą pagal tą reglamentą ir kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, atitinka šiame reglamente nustatytą kibernetinio saugumo reikalavimą tiek, kiek kibernetinio saugumo sertifikatas ar atitikties pareiškimas arba jų dalys tenkina šiame reglamente nustatytą kibernetinio saugumo reikalavimą. Tai nedaro poveikio savanoriškam tos kibernetinio saugumo sertifikavimo schemos pobūdžiui;

(123) 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;

(124) tinkama, kad, siekiant kuo labiau sumažinti naštą veiklos vykdytojams ir išvengti bet kokio galimo dubliavimo, didelės rizikos DI sistemoms, susijusioms su gaminiais, kuriems, remiantis naująja teisės aktų sistema, taikomi esami Sąjungos derinamieji teisės aktai, šių DI sistemų atitiktis šio reglamento reikalavimams turėtų būti vertinama atliekant pagal toje teisėje jau numatytą atitikties vertinimą. Todėl šio reglamento reikalavimų taikymas neturėtų daryti poveikio konkrečiai atitikties vertinimo, atliekamo pagal atitinkamus Sąjungos derinamuosius teisės aktus, logikai, metodikai ar bendrajai struktūrai;

(125) atsižvelgiant į didelės rizikos DI sistemų sudėtingumą ir su jomis susijusią riziką, svarbu sukurti tinkamą didelės rizikos DI sistemų atitikties vertinimo procedūrą, kurioje dalyvautų notifikuotosios įstaigos, vadinamąjį trečiosios šalies atliekamą atitikties vertinimą. Tačiau, atsižvelgiant į dabartinę 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 atsakyti, išskyrus vienintelę išimtį, susijusią su DI sistemomis, kurios skirtos naudoti biometrijos tikslais;

(126) siekiant, kad būtų įvykdyti trečiosios šalies atliekami atitikties vertinimai, kai to reikalaujama, nacionalinės kompetentingos institucijos pagal šį reglamentą turėtų paskirti notifikuotąsias įstaigas, jeigu jos atitinka reikalavimus, visų pirma nepriklausomumo, kompetencijos, interesų konflikto nebuvimo ir tinkamus kibernetinio saugumo reikalavimus. Nacionalinės kompetentingos institucijos turėtų siųsti pranešimus apie šių įstaigų paskyrimą Komisijai ir kitoms valstybėms narėms naudodamosi Komisijos pagal Sprendimo Nr. 768/2008/EB I priedo R23 straipsnį parengta ir prižiūrima elektronine notifikavimo priemone;

(127) laikantis Sąjungos įsipareigojimų pagal Pasaulio prekybos organizacijos susitarimą dėl techninių prekybos kliūčių, yra tinkama palengvinti atitikties vertinimo rezultatų, kuriuos pateikė kompetentingos atitikties vertinimo įstaigos, tarpusavio pripažinimą, nepriklausomai nuo teritorijos, kurioje jos yra įsteigtos, jei tos atitikties vertinimo įstaigos, įsteigtos pagal trečiosios valstybės teisę, atitinka taikytinus šio reglamento reikalavimus ir Sąjunga yra sudariusi tokios apimties susitarimą. Šiame kontekste Komisija turėtų aktyviai nagrinėti galimas tarptautines priemones šiuo tikslu ir visų pirma siekti sudaryti abipusio pripažinimo susitarimus su trečiosiomis valstybėmis;

(128) laikantis bendrai nustatytos gaminių, reglamentuojamų pagal Sąjungos derinamuosius teisės aktus, esminio pakeitimo sąvokos, tinkama, kad visais atvejais, kai įvyksta pokytis, kuris gali turėti įtakos didelės rizikos DI sistemos atitikčiai šiam reglamentui (pvz., operacinės sistemos ar programinės įrangos architektūros pakeitimas), arba pasikeitus sistemos numatytajai paskirčiai, ta DI sistema turėtų būti laikoma nauja DI sistema, kurios atitiktis turėtų būti įvertinta iš naujo. Tačiau DI sistemų, kurios toliau „mokosi“ po to, kai buvo pateiktos rinkai arba pradėtos naudoti (t. y. automatiškai prisitaiko vykdant funkcijas), algoritmo ir veikimo efektyvumo pokyčiai neturėtų būti laikomi esminiu pakeitimu, jeigu tuos pakeitimus tiekėjas numatė iš anksto ir jie buvo įvertinti atitikties vertinimo metu ;

(129) 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. Didelės rizikos DI sistemos, integruotos į gaminį, turėtų būti fiziškai ženklinamos CE ženklu, kuris gali būti papildytas skaitmeniniu CE ženklu. Didelės rizikos DI sistemų, kurios teikiamos tik skaitmenine forma, atveju turėtų būti naudojamas skaitmeninis CE ženklas. 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;

(130) tam tikromis sąlygomis galimybė greitai pasinaudoti inovatyviomis technologijomis gali būti labai svarbi asmenų sveikatos bei saugos, aplinkos apsaugos ir klimato kaitos požiūriu ir visai visuomenei. Todėl išimtinėmis su viešuoju saugumu ar fizinių asmenų gyvybės ir sveikatos apsauga, aplinkos apsauga ir itin svarbių pramonės bei infrastruktūros objektų apsauga susijusiomis aplinkybėmis rinkos priežiūros institucijos galėtų leisti pateikti rinkai arba pradėti naudoti DI sistemas, kurių atitikties vertinimas nebuvo atliktas. Tinkamai pagrįstais atvejais, kaip numatyta šiame reglamente, teisėsaugos institucijos arba civilinės saugos institucijos gali pradėti naudoti konkrečią didelės rizikos DI sistemą be rinkos priežiūros institucijos leidimo, jei tokio leidimo nepagrįstai nedelsiant paprašoma naudojimo metu arba po panaudojimo;

(131) siekiant palengvinti Komisijos ir valstybių narių darbą DI srityje, taip pat suteikti daugiau skaidrumo visuomenei, turėtų būti reikalaujama, kad didelės rizikos DI sistemų, išskyrus DI sistemas, susijusias su gaminiais, kuriems taikomi atitinkami esami Sąjungos derinamieji teisės aktai, tiekėjai, taip pat tiekėjai, kurie laiko, kad į šio reglamento priede pateiktą didelės rizikos atvejų sąrašą įtraukta DI sistema nėra didelės rizikos sistema remiantis nukrypti leidžiančia nuostata, įsiregistruotų patys ir įregistruotų informaciją apie savo didelės rizikos DI sistemą ES duomenų bazėje, kurią sukurs ir tvarkys Komisija. Prieš naudodami į šio reglamento priede pateiktą didelės rizikos atvejų sąrašą įtrauktą DI sistemą, didelės rizikos DI sistemų diegėjai, kurie yra viešojo sektoriaus institucijos, agentūros ar įstaigos, turėtų užsiregistruoti tokioje duomenų bazėje ir pasirinkti sistemą, kurią jie numato naudoti.

Kiti diegėjai turėtų turėti teisę tai daryti savanoriškai. Ši ES duomenų bazės dalis turėtų būti prieinama viešai, nemokamai, informacija turėtų būti lengvai naršoma, suprantama ir kompiuterio skaitoma. ES duomenų bazė taip pat turėtų būti patogi naudoti, pavyzdžiui, suteikiant paieškos funkcijas, be kita ko, naudojant raktinius žodžius, kad plačioji visuomenė galėtų rasti aktualią informaciją, kuri turi būti pateikiama registruojant didelės rizikos DI sistemas, ir informaciją apie didelės rizikos DI sistemų, nurodytų šio reglamento priede, kurias atitinka didelės rizikos DI sistemos, panaudojimo atvejį. Visi esminiai didelės rizikos DI sistemų pakeitimai taip pat turėtų būti registruojami ES duomenų bazėje. Didelės rizikos DI sistemų teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo srityse atveju registravimo pareigos turėtų būti vykdomos saugioje neviešoje ES duomenų bazės dalyje. Prieiga prie saugios neviešos dalies turėtų būti suteikiama tik Komisijai ir rinkos priežiūros institucijoms, kiek tai susiję su jų nacionaline tos duomenų bazės dalimi. Didelės rizikos DI sistemos ypatingos svarbos infrastruktūros srityje turėtų būti registruojamos tik nacionaliniu lygmeniu. Komisija turėtų būti ES duomenų bazės valdytoja, laikantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725. Siekiant užtikrinti visapusišką įdiegtos ES duomenų bazės veikimą, pagal duomenų bazės kūrimo procedūrą turėtų būti numatyta, kad Komisija parengs funkcines specifikacijas ir kad bus parengta nepriklausomo audito ataskaita. Komisija, vykdydama savo, kaip ES duomenų valdytojos, užduotis, turėtų atsižvelgti į kibernetinio saugumo riziką. Siekiant užtikrinti, kad ES duomenų bazė būtų kuo labiau prieinama visuomenei ir kuo plačiau jos naudojama, ES duomenų bazė, įskaitant joje pateikiamą informaciją, turėtų atitikti Direktyvos (ES) 2019/882 reikalavimus;

(132) tam tikros DI sistemos, kurių paskirtis yra sąveikauti su fiziniais asmenimis arba generuoti turinį, gali kelti konkrečią apsimetinėjimo arba apgaulės riziką, nepriklausomai nuo to, ar jos priskiriamos didelės rizikos DI sistemoms. Todėl šių sistemų naudojimui tam tikromis aplinkybėmis turėtų būti taikomos konkrečios skaidrumo pareigos, nedarant poveikio dėl didelės rizikos DI sistemų taikomiems reikalavimams ir pareigoms, taip pat taikomos tikslinės išimtys siekiant atsižvelgti į specifinius teisėsaugos poreikius. Visų pirma fiziniai asmenys turėtų būti informuojami apie tai, kad bendrauja su DI sistema, nebent tai yra akivaizdu fizinio asmens, kuris yra pakankamai informuotas, pastabus ir nuovokus, požiūriu, atsižvelgiant į aplinkybes ir naudojimo kontekstą. Vykdant tą pareigą, reikėtų atsižvelgti į fizinių asmenų, dėl jų amžiaus ar negalios priklausančių pažeidžiamoms grupėms, savybes tiek, kiek DI sistema taip pat skirta bendrauti su tomis grupėmis. Be to, fizinius asmenis reikėtų informuoti apie tai, kad jie sąveikauja su DI sistemomis, kurios, tvarkydamos jų biometrinius duomenis, gali nustatyti ar nuspėti tų asmenų emocijas ar ketinimus arba priskirti juos konkrečioms kategorijoms. Tokios konkrečios kategorijos gali būti susijusios su tokiais aspektais kaip lytis, amžius, plaukų spalva, akių spalva, tatuiruotės, asmeniniai požymiai, etninė kilmė, asmeniniai pomėgiai ir interesai. Tokia informacija ir pranešimai turėtų būti teikiami neįgaliesiems prieinama forma;

(133) įvairios DI sistemos gali sugeneruoti didelį kiekį sintetinio turinio, kurį žmonėms tampa vis sunkiau atskirti nuo žmogaus sukurto ir autentiško turinio. Platus tų sistemų prieinamumas ir didėjantys jų pajėgumai daro reikšmingą poveikį informacinės ekosistemos vientisumui ir patikimumui, todėl kyla nauja klaidingos informacijos ir plataus masto manipuliavimo, sukčiavimo, apsimetimo kitais asmenimis ir vartotojų apgaulės rizika. Atsižvelgiant į tą poveikį, sparčius technologijų pokyčius ir poreikį taikyti naujus metodus ir metodus informacijos kilmei atsekti, yra tikslinga reikalauti, kad tų sistemų tiekėjai integruotų techninius sprendimus, leidžiančius kompiuterio skaitomu formatu pažymėti ir nustatyti, kad išvedinį sugeneravo arba gavo atlikusi manipuliacijas DI sistema, o ne žmogus. Tokie metodai ir būdai turėtų būti pakankamai tvirti, sąveikūs, veiksmingi ir patikimi, kiek tai techniškai įmanoma, atsižvelgiant į turimus metodus arba tokių metodų derinį, pavyzdžiui, kai gali būti tinkama, vandens ženklus, metaduomenų identifikavimą, kriptografinius metodus turinio kilmei ir autentiškumui įrodyti, registravimo metodus, pirštų atspaudus ar kitas priemones. Įgyvendindami šią pareigą, tiekėjai turėtų taip pat atsižvelgti į įvairių rūšių turinio ypatybes ir ribotumus, taip pat į atitinkamus technologijų ir rinkos pokyčius šioje srityje, kuriuos atspindi visuotinai pripažinti technikos laimėjimai. Tokie metodai ir būdai gali būti įgyvendinami DI sistemos lygmeniu arba DI modelio lygmeniu, įskaitant bendrosios paskirties DI modelius, generuojančius turinį, taip palengvinant DI sistemos tolesnės grandies tiekėjui vykdyti šią pareigą. Siekiant išlaikyti proporcingumą, yra tikslinga numatyti, kad ši ženklinimo pareiga neturėtų būti taikoma DI sistemoms, kurios visų pirma atlieka pagalbinę standartinio redagavimo funkciją, arba DI sistemoms, kurios iš esmės nekeičia diegėjo pateiktų įvesties duomenų arba jų semantikos;

(134) diegėjai, kurie naudoja DI sistemą, kad sugeneruotų ar atlikę manipuliacijas gautų judamo ar nejudamo vaizdo arba garso turinį, kuris labai panašus į realius asmenis, daiktus, vietas, subjektus ar įvykius ir kurį asmuo gali klaidingai palaikyti autentišku ar tikrovišku (sintetinė sankaita), turėtų atskleisti ne tik techninius sprendimus, kuriuos naudoja DI sistemos tiekėjai, bet taip pat turėtų aiškiai ir matomai atskleisti, kad turinys buvo dirbtinai sukurtas arba gautas atlikus manipuliacijas, atitinkamai paženklindami DI išvedinį ir atskleisdami informaciją apie jo dirbtinę kilmę. Skaidrumo pareigos vykdymas neturėtų būti aiškinamas taip, kad DI sistemos ar jos išvedinio naudojimas trukdo įgyvendinti teisę į saviraiškos laisvę ir teisę į menų ir mokslo laisvę, garantuojamas Chartijoje, visų pirma tais atvejais, kai turinys yra akivaizdžiai kūrybinio, satyrinio, meninio, išgalvoto ar analogiško kūrinio ar programos dalis, taikant tinkamas trečiųjų šalių teisių ir laisvių apsaugos priemones. Tokiais atvejais šiame reglamente nustatyta skaidrumo pareiga, kiek tai susiję su sintetine sankaita, apima tik atskleidimą, kad esama tokio sugeneruoto ar gauto atlikus manipuliacijas turinio, tinkamu būdu, kuris nekliudytų rodyti kūrinį ar juo mėgautis, įskaitant įprastą jo naudojimą, kartu išlaikant kūrinio naudingumą ir kokybę. Be to, taip pat tikslinga numatyti panašią atskleidimo pareigą, susijusią su DI sugeneruotu arba gautu atlikus manipuliacijas tekstu, jei jis skelbiamas siekiant informuoti visuomenę viešojo intereso klausimais, išskyrus atvejus, kai dirbtinio intelekto sugeneruotam turiniui taikomas žmogaus atliekamos peržiūros ar redakcinės kontrolės procesas arba kai fizinis ar juridinis asmuo prisiima redakcinę atsakomybę dėl turinio paskelbimo;

(135) nedarant poveikio privalomam skaidrumo pareigų pobūdžiui ir visapusiškam jų taikymui, Komisija taip pat gali skatinti ir palengvinti Sąjungos lygmens praktikos kodeksų rengimą, kad būtų sudarytos palankesnės sąlygos veiksmingai įgyvendinti pareigas, susijusias su dirbtinai sugeneruoto ar gauto atlikus manipuliacijas turinio aptikimu ir ženklinimu, be kita ko, remti praktinę tvarką, pagal kurią atitinkamai būtų prieinami aptikimo mechanizmai ir palengvintas bendradarbiavimas su kitais vertės grandinės dalyviais, platinant turinį arba tikrinant jo autentiškumą ir kilmę, kad visuomenė galėtų veiksmingai atskirti DI sugeneruotą turinį;

(136) šiame reglamente tam tikrų DI sistemų tiekėjams ir diegėjams nustatytos pareigos, siekiant sudaryti sąlygas nustatyti ir atskleisti tai, kad tų sistemų išvediniai yra dirbtinai sugeneruoti arba gauti atlikus manipuliacijas, yra itin aktualios siekiant palengvinti veiksmingą Reglamento (ES) 2022/2065 įgyvendinimą. Tai visų pirma taikoma labai didelių interneto platformų arba labai didelių interneto paieškos sistemų paslaugų teikėjų pareigoms nustatyti ir sumažinti sisteminę riziką, galinčią kilti dėl turinio, kuris buvo dirbtinai sugeneruotas ar gautas atlikus manipuliacijas, sklaidos, visų pirma faktinio ar numatomo neigiamo poveikio demokratiniams procesams, pilietiniam diskursui ir rinkimų procesams, be kita ko, pasitelkiant dezinformaciją, riziką. Reikalavimas ženklinti DI sistemų sugeneruotą turinį pagal šį reglamentą nedaro poveikio Reglamento (ES) 2022/2065 16 straipsnio 6 dalyje nustatytai prieglobos paslaugų teikėjų pareigai tvarkyti pranešimus apie neteisėtą turinį, gautus pagal to reglamento 16 straipsnio 1 dalį, ir neturėtų daryti poveikio vertinimui ir sprendimui dėl konkretaus turinio neteisėtumo. Tas vertinimas turėtų būti atliekamas atsižvelgiant tik į turinio teisėtumą reglamentuojančias taisykles;

(137) pirmiau nurodytų skaidrumo pareigų, susijusių su DI sistemomis, kurioms taikomas šis reglamentas, vykdymas neturėtų būti aiškinamas taip, kad DI sistemos ar jos išvedinių naudojimas yra teisėtas pagal šį reglamentą arba kitą Sąjungos ir valstybės narės teisę, ir neturėtų daryti poveikio kitoms Sąjungos ar nacionalinėje teisėje nustatytoms DI sistemų diegėjams taikomoms skaidrumo pareigoms;

(138) DI yra sparčiai besivystanti technologijų grupė, kuriai reikalinga reglamentavimo priežiūra ir saugi ir kontroliuojama eksperimentavimo erdvė, kartu užtikrinant atsakingas inovacijas ir tinkamų apsaugos ir rizikos mažinimo priemonių integraciją. Siekiant užtikrinti inovacijas skatinančią, į ateitį orientuotą ir sutrikdymams atsparią teisinę sistemą, valstybės narės turėtų užtikrinti, kad jų nacionalinės kompetentingos institucijos sukurtų bent vieną apribotą bandomąją DI reglamentavimo aplinką nacionaliniu lygmeniu, kad būtų palengvintas naujoviškų DI sistemų kūrimas ir bandymas taikant griežtą reglamentavimo priežiūrą iki šių sistemų pateikimo rinkai arba pradėjimo naudoti. Valstybės narės taip pat galėtų šią pareigą vykdyti dalyvaudamos jau veikiančiose apribotose bandomosiose reglamentavimo aplinkose arba kartu su vienos ar daugiau valstybių narių kompetentingomis institucijomis sukurdamos apribotą bandomąją aplinką, jei tokiu dalyvavimu dalyvaujančioms valstybėms narėms užtikrinama lygiaverčio lygio nacionalinė aprėptis. DI apribotos bandomosios reglamentavimo aplinkos galėtų būti sukurtos fizine, skaitmenine ar mišria forma ir gali apimti fizinius ir skaitmeninius gaminius. Steigiamosios institucijos taip pat turėtų užtikrinti, kad DI apribotose bandomosiose reglamentavimo aplinkose būtų pakankamai išteklių jų veikimui, įskaitant finansinius ir žmogiškuosius išteklius;

(139) apribotų bandomųjų DI reglamentavimo aplinkų tikslai turėtų būti DI inovacijų skatinimas, kūrimo etapu ir etapu prieš pateikimą rinkai nustatant kontroliuojamą eksperimentavimo ir bandymų aplinką, siekiant užtikrinti naujoviškų DI sistemų atitiktį šiam reglamentui ir kitiems susijusiems Sąjungos ir valstybių narių teisės aktams. Be to, bandomosios DI reglamentavimo aplinkomis turėtų būti siekiama novatorių teisinio tikrumo ir kompetentingų institucijų priežiūros ir supratimo apie DI naudojimo galimybes, naują riziką ir poveikį didinimas, palankesnių sąlygų institucijoms ir įmonėms mokytis reglamentavimo srityje sudarymas, be kita ko, atsižvelgiant į būsimus teisinės sistemos pritaikymus, bendradarbiavimo ir dalijimosi geriausios praktikos pavyzdžiais su institucijomis, susijusiomis su DI apribota bandomąja reglamentavimo aplinka, rėmimas, taip pat patekimo į rinką spartinimas, be kita ko, kliūčių mažosioms ir vidutinėms įmonėms (MVĮ), įskaitant startuolius, pašalinimas. DI apribotos bandomosios reglamentavimo aplinkos turėtų būti plačiai prieinamos visoje Sąjungoje, o ypatingas dėmesys turėtų būti skiriamas jų prieinamumui MVĮ, įskaitant startuolius. Dalyvaujant apribotoje bandomojoje DI reglamentavimo aplinkoje daugiausia dėmesio turėtų būti skiriama klausimams, dėl kurių tiekėjams ir galimiems tiekėjams kyla teisinis netikrumas siekiant diegti inovacijas, eksperimentuoti su DI Sąjungoje ir prisidėti prie faktiniais duomenimis grindžiamo mokymosi reglamentavimo srityje. Todėl DI sistemų priežiūra apribotoje bandomojoje DI reglamentavimo aplinkoje turėtų apimti jų kūrimą, mokymą, bandymą ir validavimą prieš pateikiant sistemas rinkai arba pradedant jas naudoti, taip pat esminio pakeitimo, dėl kurio gali prireikti naujos atitikties vertinimo procedūros, sąvoką ir pasireiškimą. Bet kokia reikšminga rizika, nustatyta kuriant ir bandant tokias DI sistemas, turėtų būti atitinkamai sumažinama, o jeigu tai nepavyksta, kūrimo ir bandymo procesas turėtų būti sustabdomas.

Kai tinkama, nacionalinės kompetentingos institucijos, kuriančios apribotas bandomąsias DI reglamentavimo aplinkas, turėtų bendradarbiauti su kitomis atitinkamomis institucijomis, įskaitant prižiūrinčias pagrindinių teisių apsaugą, ir galėtų sudaryti sąlygas dalyvauti kitiems DI ekosistemos dalyviams, pavyzdžiui, nacionalinėms ar Europos standartizacijos organizacijoms, notifikuotosioms įstaigoms, bandymų ir eksperimentavimo infrastruktūros atstovams, mokslinių tyrimų ir eksperimentavimo laboratorijoms, Europos skaitmeninių inovacijų centrams, atitinkamiems suinteresuotiesiems subjektams ir pilietinės visuomenės organizacijoms. Kad būtų užtikrintas vienodas įgyvendinimas visoje Sąjungoje ir masto ekonomija, yra tinkama sukurti bendras DI apribotų bandomųjų reglamentavimo aplinkų įgyvendinimo taisykles ir atitinkamų institucijų, dalyvaujančių vykdant apribotų bandomųjų aplinkų priežiūrą, bendradarbiavimo sistemą. Pagal šį reglamentą sukurtos DI apribotos bandomosios reglamentavimo aplinkos neturėtų daryti poveikio kitai teisei, pagal kurią leidžiama sukurti kitas apribotas bandomąsias aplinkas, kuriomis siekiama užtikrinti atitiktį kitiems teisės aktams nei šis reglamentas. Kai tinkama, atitinkamos kompetentingos institucijos, atsakingos už tas kitas apribotas bandomąsias reglamentavimo aplinkas, turėtų apsvarstyti tų apribotų bandomųjų aplinkų naudojimo naudą, be kita ko, siekiant užtikrinti DI sistemų atitiktį šiam reglamentui. Nacionalinėms kompetentingoms institucijoms ir apribotos bandomosios DI reglamentavimo aplinkos dalyviams susitarus, bandymai realiomis sąlygomis taip pat gali būti atliekami ir prižiūrimi apribotos bandomosios DI reglamentavimo aplinkos sąlygomis;

(140) šiuo reglamentu turėtų būti nustatytas apribotos bandomosios DI reglamentavimo aplinkos tiekėjams ir galimiems tiekėjams skirtas teisinis pagrindas dėl asmens duomenų, kurie buvo surinkti kitais tikslais, naudojimo, siekiant apribotoje bandomojoje reglamentavimo DI aplinkoje sukurti tam tikras su viešuoju interesu susijusias DI sistemas, tik nurodytomis sąlygomis, laikantis Reglamento (ES) 2016/679 6 straipsnio 4 dalies bei 9 straipsnio 2 dalies g punkto ir Reglamento (ES) 2018/1725 5, 6 ir 10 straipsnių, nedarant poveikio Direktyvos (ES) 2016/680 4 straipsnio 2 daliai ir 10 straipsniui. Visos kitos duomenų valdytojų pareigos ir duomenų subjektų teisės pagal Reglamentą (ES) 2016/679, Reglamentą (ES) 2018/1725 ir Direktyvą (ES) 2016/680 taikomos toliau. Visų pirma šiuo reglamentu neturėtų būti nustatytas teisinis pagrindas, kaip tai suprantama Reglamento (ES) 2016/679 22 straipsnio 2 dalies b punkte ir Reglamento (ES) 2018/1725 24 straipsnio 2 dalies b punkte. Apribotoje DI bandomojoje aplinkoje tiekėjai ir galimi tiekėjai turėtų užtikrinti tinkamas apsaugos priemones ir bendradarbiauti su kompetentingomis institucijomis, be kita ko, vadovautis jų rekomendacijomis ir veikti greitai bei sąžiningai, kad tinkamai sumažintų bet kokią nustatytą reikšmingą riziką saugumui, sveikatai, aplinkai ir pagrindinėms teisėms, kuri gali kilti kuriant, vykdant bandymą ir eksperimentuojant toje apribotoje bandomojoje aplinkoje;

(141) siekiant paspartinti šio reglamento priede išvardytų didelės rizikos DI sistemų kūrimo ir pateikimo rinkai procesą, svarbu, kad tokių sistemų tiekėjai arba galimi tiekėjai taip pat galėtų pasinaudoti specialia tų sistemų bandymo realiomis sąlygomis tvarka, nedalyvaudami DI apribotoje bandomojoje reglamentavimo aplinkoje. Tačiau tokiais atvejais, atsižvelgiant į galimas tokių bandymų pasekmes asmenims, reikėtų užtikrinti, kad tiekėjams ar galimiems tiekėjams šiuo reglamentu būtų nustatytos tinkamos ir pakankamos garantijos bei sąlygos. Tokios garantijos, *inter alia*, turėtų apimti reikalavimą, kad fiziniai asmenys duotų informacija grindžiamą sutikimą dalyvauti bandymuose realiomis sąlygomis, išskyrus teisėsaugą, kai informacija grindžiamo sutikimo prašymas užkirstų kelią DI sistemai išbandyti. Subjektų sutikimas dalyvauti tokiuose bandymuose pagal šį reglamentą skiriasi nuo duomenų subjektų sutikimo tvarkyti jų asmens duomenis pagal atitinkamus duomenų apsaugos teisės aktus ir nedaro jam poveikio.

Taip pat svarbu kuo labiau sumažinti riziką ir sudaryti sąlygas kompetentingoms institucijoms vykdyti priežiūrą, ir todėl reikalauti, kad galimi paslaugų teikėjai kompetentingai rinkos priežiūros institucijai pateiktų bandymo realiomis sąlygomis planą, registruotų bandymą specialiose ES duomenų bazės dalyse, taikant tam tikras ribotas išimtis, nustatytų laikotarpio, per kurį galima atlikti bandymą, trukmę, ir reikalauti papildomų apsaugos priemonių tam tikroms pažeidžiamoms grupėms priklausantiems asmenims, taip pat rašytinio susitarimo, kuriame būtų apibrėžti galimų tiekėjų ir diegėjų vaidmenys ir atsakomybė, ir veiksmingos kompetentingų darbuotojų, dalyvaujančių bandyme realiomis sąlygomis, atliekamos priežiūros. Be to, tikslinga numatyti papildomas apsaugos priemones siekiant užtikrinti, kad DI sistemos predikcijos, rekomendacijos ar sprendimai galėtų būti veiksmingai atšaukti ir į juos galėtų būti neatsižvelgiama, taip pat kad asmens duomenys būtų apsaugomi ir ištrinami, kai subjektai atšaukia savo sutikimą dalyvauti bandyme, nedarant poveikio jų, kaip duomenų subjektų, teisėms pagal Sąjungos duomenų apsaugos teisę. Kalbant apie duomenų perdavimą, taip pat tikslinga numatyti, kad bandymo realiomis sąlygomis tikslais surinkti ir tvarkomi duomenys turėtų būti perduodami trečiosioms valstybėms tik tais atvejais, kai įgyvendinamos tinkamos ir taikytinos pagal Sąjungos teisę apsaugos priemonės, visų pirma remiantis asmens duomenų perdavimo pagrindais pagal Sąjungos teisę duomenų apsaugos srityje, o ne asmens duomenų atžvilgiu nustatytos tinkamos apsaugos priemonės pagal Sąjungos teisę, pavyzdžiui, Europos Parlamento ir Tarybos reglamentus (ES) 2022/868[42] ir (ES) 2023/2854[43].

---

[42] 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/868 dėl Europos duomenų valdymo, kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1724 (Duomenų valdymo aktas) (OL L 152, 2022 6 3, p. 1).

[43] 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828 (Duomenų aktas) (OL L, 2023/2854, 2023 12 22, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) siekiant užtikrinti, kad DI duotų visuomenei ir aplinkai naudingų rezultatų, valstybės narės raginamos remti ir skatinti mokslinius tyrimus ir plėtrą, susijusius su DI sprendimais, kuriais padedama siekti visuomenei ir aplinkai naudingų rezultatų, pavyzdžiui, DI grindžiamais sprendimais siekiant padidinti prieinamumą asmenims su negalia, kovoti su socialine ir ekonomine nelygybe ar pasiekti aplinkos tikslus, skiriant pakankamai išteklių, įskaitant viešąjį ir Sąjungos finansavimą, ir, kai tinkama, visų pirma atsižvelgiant į projektus, kuriais siekiama tokių tikslų, su sąlyga, kad tenkinami tinkamumo ir atrankos kriterijai. Tokie projektai turėtų būti grindžiami DI kūrėjų, nelygybės ir nediskriminavimo, prieigos, vartotojų, aplinkos ir skaitmeninių teisių specialistų, taip pat akademinės bendruomenės narių tarpdalykinio bendradarbiavimo principu;

(143) siekiant skatinti ir apsaugoti inovacijas, svarbu, kad būtų ypač atsižvelgiama į MVĮ, įskaitant startuolius, kurios yra DI sistemų tiekėjos ar diegėjos, interesus. Siekdamos to tikslo, valstybės narės turėtų rengti šiems veiklos vykdytojams skirtas iniciatyvas, įskaitant informuotumo didinimą ir informacijos perdavimą. Valstybės narės turėtų suteikti MVĮ, įskaitant startuolius, kurių registruota buveinė arba filialas yra Sąjungoje, pirmenybinę prieigą prie apribotų bandomųjų DI reglamentavimo aplinkų, jei jos tenkina tinkamumo sąlygas ir atrankos kriterijus, neužkertant kelio kitiems tiekėjams ir galimiems tiekėjams prieiti prie bandomųjų aplinkų, jei jie tenkina tas pačias sąlygas ir kriterijus. Valstybės narės turėtų naudotis esamais kanalais ir, kai tinkama, nustatyti naujus specialius bendravimo su MVĮ, įskaitant startuolius, diegėjais, kitais novatoriais ir atitinkamai su vietos valdžios institucijomis kanalus, kad padėtų MVĮ vystytis – kad būtų teikiamos rekomendacijos ir atsakoma į užklausas dėl šio reglamento įgyvendinimo. Kai tinkama, šie kanalai turėtų bendradarbiauti, kad sukurtų sinergiją ir užtikrintų, kad MVĮ, įskaitant startuolius, ir diegėjams teikiamos gairės būtų vienodos. Be to, valstybės narės turėtų sudaryti palankesnes sąlygas MVĮ ir kitiems atitinkamiems suinteresuotiesiems subjektams dalyvauti standartų rengimo procesuose. Be to, notifikuotosios įstaigos, nustatydamos atitikties vertinimo mokesčius, turėtų atsižvelgti į konkrečius tiekėjų, kurie yra MVĮ, įskaitant startuolius, interesus ir poreikius. Komisija turėtų reguliariai vertinti MVĮ, įskaitant startuolius, išlaidas dėl sertifikavimo ir atitikties, be kita ko, skaidriai konsultuodamasi, ir turėtų bendradarbiauti su valstybėmis narėmis siekiant sumažinti tokias išlaidas.

Pavyzdžiui, tiekėjai ir kiti veiklos vykdytojai, visų pirma smulkieji, gali patirti didelių vertimo raštu išlaidų, susijusių su privalomais dokumentais ir bendravimu su institucijomis. Valstybės narės turėtų numatyti galimybę užtikrinti, kad viena iš jų nustatytų ir priimtinų kalbų, vartojamų atitinkamiems tiekėjams rengiant dokumentus ir bendraujant su veiklos vykdytojais, būtų plačiai suprantama kuo didesniam tarpvalstybinių diegėjų ratui. Siekdama atsižvelgti į konkrečius MVĮ, įskaitant startuolius, poreikius, Komisija Valdybos prašymu turėtų pateikti standartinius šablonus, skirtus sritims, kurioms taikomas šis reglamentas. Be to, Komisija turėtų papildyti valstybių narių pastangas suteikdama bendrą informacinę platformą, kurioje visiems tiekėjams ir diegėjams būtų teikiama paprasta naudoti informacija apie šį reglamentą, organizuodama tinkamas komunikacijos kampanijas, skirtas informuotumui apie šiame reglamente nustatytas pareigas didinti, taip pat vertindama ir skatindama su DI sistemomis susijusių viešųjų pirkimų procedūrų geriausios praktikos konvergenciją. Vidutinės įmonės, kurios iki neseniai buvo laikomos mažosiomis įmonėmis, kaip tai suprantama Komisijos rekomendacijos 2003/361/EB[44] priede, turėtų turėti galimybę naudotis tomis paramos priemonėmis, nes šioms naujoms vidutinėms įmonėms kartais gali trūkti teisinių išteklių ir mokymo, būtinų siekiant užtikrinti, kad šis reglamentas būtų tinkamai suprantamas ir jo būtų laikomasi.

[44] 2003 m. gegužės 6 d. Komisijos rekomendacija dėl labai mažų, mažųjų ir vidutinio dydžio įmonių apibrėžties (OL L 124, 2003 5 20, p. 36).

(144) siekiant skatinti ir apsaugoti inovacijas, reikminė DI platforma, visos atitinkamos Sąjungos finansavimo programos ir projektai, pavyzdžiui, Skaitmeninės Europos programa, programa „Europos horizontas“, kurias įgyvendina Komisija ir valstybės narės Sąjungos arba nacionaliniu lygmeniu, turėtų atitinkamai padėti siekti šio reglamento tikslų;

(145) siekiant kuo labiau sumažinti riziką įgyvendinimui, kuri kyla dėl žinių ir patirties rinkoje trūkumo, taip pat siekiant palengvinti tiekėjams, ypač MVĮ, įskaitant startuolius, ir notifikuotosioms įstaigoms vykdyti pareigas pagal šį reglamentą, reikminė DI platforma, Europos skaitmeninių inovacijų centrai ir Komisijos bei valstybių narių Sąjungos arba nacionaliniu lygmeniu sukurta bandymų ir eksperimentavimo infrastruktūra turėtų padėti įgyvendinti šį reglamentą. Pagal savo atitinkamą misiją ir kompetencijos sritis reikminė DI platforma, Europos skaitmeninių inovacijų centrai ir bandymų ir eksperimentavimo infrastruktūra gali teikti visų pirma techninę ir mokslinę paramą tiekėjams ir notifikuotosioms įstaigoms;

(146) be to, atsižvelgiant į tai, kad kai kurie veiklos vykdytojai yra labai maži, ir siekiant užtikrinti proporcingumą inovacijų išlaidų atžvilgiu, yra tikslinga labai mažoms įmonėms leisti daugiausia atsieinančias pareigas, t. y. nustatyti kokybės valdymo sistemą, įvykdyti supaprastintu būdu, kuriuo administracinė našta ir išlaidos toms įmonėms būtų sumažintos nedarant poveikio apsaugos lygiui ir poreikiui laikytis didelės rizikos DI sistemoms taikomų reikalavimų. Komisija turėtų parengti gaires, kuriose būtų nurodyti kokybės valdymo sistemos elementai, kuriuos tokiu supaprastintu būdu turi įgyvendinti labai mažos įmonės;

(147) tikslinga, kad Komisija, kiek įmanoma, palengvintų 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 komisijas, ekspertų laboratorijas ir etalonines laboratorijas, veikiančias medicinos priemonių srityje pagal reglamentus (ES) 2017/745 ir (ES) 2017/746;

(148) šiuo reglamentu turėtų būti nustatyta valdymo sistema, kuri leistų tiek koordinuoti, tiek remti šio reglamento taikymą nacionaliniu lygmeniu, taip pat stiprinti pajėgumus Sąjungos lygmeniu ir integruoti suinteresuotuosius subjektus DI srityje. Siekiant veiksmingai įgyvendinti šį reglamentą ir užtikrinti jo vykdymą, reikia valdymo sistemos, kuri leistų koordinuoti ir centralizuotai kaupti ekspertines žinias Sąjungos lygmeniu. DI tarnybos, įsteigtos Komisijos sprendimu[45], užduotis – plėtoti Sąjungos ekspertines žinias ir pajėgumus DI srityje ir prisidėti prie Sąjungos teisės DI srityje įgyvendinimo. Valstybės narės turėtų padėti DI tarnybai vykdyti užduotis, kad būtų remiamas Sąjungos ekspertinių žinių ir pajėgumų plėtojimas Sąjungos lygmeniu ir stiprinamas bendrosios skaitmeninės rinkos veikimas. Be to, turėtų būti įsteigta Valdyba, kurią sudarytų valstybių narių atstovai, mokslinė komisija, kad būtų įtraukta mokslo bendruomenė, ir patariamasis forumas, kad suinteresuotieji subjektai galėtų prisidėti prie šio reglamento įgyvendinimo Sąjungos ir nacionaliniu lygmeniu. Plėtojant Sąjungos ekspertines žinias ir pajėgumus taip pat turėtų būti naudojamasi esamais ištekliais ir ekspertinėmis žiniomis, visų pirma pasitelkiant sinergiją su struktūromis, sukurtomis Sąjungos lygmeniu užtikrinant kitų teisės aktų vykdymą, ir sinergiją su susijusiomis iniciatyvomis Sąjungos lygmeniu, pavyzdžiui, bendrąja įmone „EuroHPC“ ir DI bandymų ir eksperimentavimo priemonėmis pagal Skaitmeninės Europos programą;

---

[45] 2024 m. sausio 24 d. Komisijos sprendimas, kuriuo įsteigiama Europos dirbtinio intelekto tarnyba C(2024)390.

(149) siekiant sudaryti sąlygas sklandžiai, veiksmingai ir suderintai įgyvendinti šį reglamentą, turėtų būti įsteigta Valdyba. Valdyboje turėtų būti atstovaujama įvairiems DI ekosistemos interesams ir ją turėtų sudaryti valstybių narių atstovai. Valdyba turėtų būti atsakinga už įvairias patariamąsias užduotis, taip pat nuomonių, rekomendacijų, patarimų teikimą ar prisidėjimą prie gairių šio reglamento įgyvendinimo klausimais, įskaitant klausimus dėl vykdymo užtikrinimo, techninių specifikacijų arba esamų standartų, susijusių su šiame reglamente nustatytais reikalavimais, ir konsultuoti Komisiją, valstybes nares ir jų nacionalines kompetentingas institucijas konkrečiais klausimais, susijusiais su DI. Siekiant suteikti valstybėms narėms tam tikro lankstumo skiriant savo atstovus Valdyboje, tokie atstovai gali būti bet kurie viešiesiems subjektams priklausantys asmenys, kurie turėtų turėti atitinkamą kompetenciją ir įgaliojimus padėti vykdyti koordinavimą nacionaliniu lygmeniu ir prisidėti prie Valdybos užduočių vykdymo. Valdyba turėtų įsteigti du nuolatinius pogrupius, kurie sudarytų sąlygas rinkos priežiūros institucijoms ir notifikuojančiosioms institucijoms bendradarbiauti ir keistis informacija klausimais, susijusiais atitinkamai su rinkos priežiūra ir notifikuotosiomis įstaigomis. Nuolatinis rinkos priežiūros pogrupis turėtų veikti kaip šio reglamento administracinio bendradarbiavimo grupė, kaip tai suprantama Reglamento (ES) 2019/1020 30 straipsnyje. Pagal to reglamento 33 straipsnį, Komisija turėtų remti nuolatinio rinkos priežiūros pogrupio veiklą atlikdama rinkos vertinimus ar tyrimus, visų pirma siekdama nustatyti šio reglamento aspektus, dėl kurių reikalingas konkretus ir skubus rinkos priežiūros institucijų veiksmų koordinavimas. Valdyba atitinkamai gali sudaryti kitus nuolatinius ar laikinuosius pogrupius konkretiems klausimams spręsti. Valdyba taip pat turėtų atitinkamai bendradarbiauti su atitinkamomis Sąjungos įstaigomis, ekspertų grupėmis ir tinklais, veikiančiais atitinkamos Sąjungos teisės kontekste, įskaitant visų pirma tuos, kurie veikia vadovaudamiesi atitinkama Sąjungos teise duomenų, skaitmeninių produktų ir paslaugų srityje;

(150) siekiant užtikrinti suinteresuotųjų subjektų dalyvavimą įgyvendinant ir taikant šį reglamentą, turėtų būti įsteigtas patariamasis forumas, kuris konsultuotų Valdybą ir Komisiją ir teiktų joms techninės ekspertines žinias. Siekiant užtikrinti įvairiapusį ir subalansuotą atstovavimą suinteresuotiesiems subjektams, atsižvelgiant į komercinius ir nekomercinius interesus, taip pat – komercinių interesų kategorijoje – MVĮ ir kitoms įmonėms, patariamąjį forumą turėtų sudaryti, *inter alia*, pramonės atstovai, startuoliai, MVĮ, akademinė bendruomenė, pilietinė visuomenė, įskaitant socialinius partnerius, taip pat Pagrindinių teisių agentūra, ENISA, Europos standartizacijos komitetas (CEN), Europos elektrotechnikos standartizacijos komitetas (CENELEC) ir Europos telekomunikacijų standartų institutas (ETSI);

(151) siekiant remti šio reglamento įgyvendinimą ir vykdymo užtikrinimą, visų pirma DI tarnybos vykdomą stebėsenos veiklą, susijusią su bendrosios paskirties DI modeliais, turėtų būti įsteigta nepriklausomų ekspertų mokslinė komisija. Mokslinę komisiją sudarantys nepriklausomi ekspertai turėtų būti atrenkami remiantis naujausiomis mokslinėmis ar techninėmis ekspertinėmis žiniomis DI srityje ir jie turėtų atlikti savo užduotis nešališkai ir objektyviai, taip pat užtikrinti informacijos ir duomenų, gautų vykdant savo užduotis ir veiklą, konfidencialumą. Kad būtų galima sustiprinti nacionalinius gebėjimus, būtinus veiksmingam šio reglamento vykdymui užtikrinti, valstybės narės turėtų turėti galimybę prašyti mokslinės komisijos ekspertų suteikti paramą jų vykdymo užtikrinimo veiklai;

(152) siekiant remti tinkamą vykdymo užtikrinimą, kiek tai susiję su DI sistemomis, ir sustiprinti valstybių narių gebėjimus, turėtų būti sukurtos Sąjungos DI bandymų pagalbinės struktūros, ir valstybės narės turėtų turėti galimybę jomis naudotis;

(153) labai svarbus vaidmuo taikant šį reglamentą ir užtikrinant jo vykdymą tenka valstybėms narėms. Todėl kiekviena valstybė narė turėtų bent vieną notifikuojančiąją instituciją ir bent vieną rinkos priežiūros instituciją paskirti nacionalinėmis kompetentingomis institucijomis šio reglamento taikymo ir įgyvendinimo priežiūros tikslu. Valstybės narės gali nuspręsti paskirti bet kurį viešąjį subjektą vykdyti nacionalinių kompetentingų institucijų, kaip tai suprantama šiame reglamente, užduotis atsižvelgdamos į konkrečius nacionalinius organizacinius ypatumus ir poreikius. Siekiant padidinti organizacinį veiksmingumą valstybėse narėse ir sukurti bendrąjį kontaktinį punktą, skirtą visuomenei ir kitiems partneriams valstybių narių ir Sąjungos lygmeniu, kiekviena valstybė narė bendruoju kontaktiniu punktu turėtų paskirti rinkos priežiūros instituciją;

(154) nacionalinės kompetentingos institucijos turėtų naudotis savo įgaliojimais nepriklausomai, objektyviai ir nešališkai, kad apsaugotų savo veiklos ir užduočių objektyvumo principus ir užtikrintų šio reglamento taikymą ir įgyvendinimą. Šių institucijų nariai turėtų susilaikyti nuo bet kokių su jų pareigomis nesuderinamų veiksmų ir jiems turėtų būti taikomos konfidencialumo taisyklės pagal šį reglamentą;

(155) siekiant užtikrinti, kad didelės rizikos DI sistemų tiekėjai galėtų atsižvelgti į didelės rizikos DI sistemų naudojimo patirtį, kad patobulintų savo sistemas ir projektavimo bei kūrimo procesą arba laiku galėtų imtis bet kokių galimų taisomųjų veiksmų, visi tiekėjai turėtų turėti veikiančias priežiūros po pateikimo rinkai sistemas. Kai aktualu, stebėsena po pateikimo rinkai turėtų apimti sąveikos su kitomis DI sistemomis, įskaitant kitus prietaisus ir programinę įrangą, analizę. Stebėsena po pateikimo rinkai neturėtų būti taikoma diegėjų, kurie yra teisėsaugos institucijos, neskelbtiniems operatyviniams duomenims. 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. Šiame kontekste taip pat turėtų būti reikalaujama, kad tiekėjai būtų įdiegę sistemą, skirtą pranešti atitinkamoms institucijoms apie bet kokius rimtus incidentus, kilusius dėl jų DI sistemų naudojimo, t. y. apie incidentą ar veikimo sutrikimą, dėl kurio įvyko mirtis arba buvo padaryta didelė žala sveikatai, rimtai ir negrįžtamai sutrikdytas ypatingos svarbos infrastruktūros valdymas ir veikimas, taip pat apie pareigų pagal Sąjungos teisę, kuria siekiama apsaugoti pagrindines teises, pažeidimus, arba didelę žalą turtui ar aplinkai;

(156) 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. Pagal šį reglamentą paskirtos rinkos priežiūros institucijos turėtų turėti visus vykdymo užtikrinimo įgaliojimus, nustatytus šiame reglamente ir Reglamente (ES) 2019/1020, ir turėtų naudotis savo įgaliojimais ir vykdyti savo pareigas nepriklausomai, objektyviai ir nešališkai. Nors daugumai DI sistemų netaikomi konkretūs reikalavimai ir pareigos pagal šį reglamentą, rinkos priežiūros institucijos gali imtis priemonių, susijusių su visomis DI sistemomis, kai dėl jų kyla rizika pagal šį reglamentą. Dėl specifinio Sąjungos institucijų, agentūrų ir įstaigų, kurioms taikomas šis reglamentas, pobūdžio tikslinga Europos duomenų apsaugos priežiūros pareigūną paskirti jų atžvilgiu kompetentinga rinkos priežiūros institucija. Tai neturėtų daryti poveikio valstybių narių atliekamam nacionalinių kompetentingų institucijų skyrimui. Rinkos priežiūros veikla neturėtų daryti poveikio prižiūrimų subjektų gebėjimui nepriklausomai vykdyti savo užduotis, kai tokio nepriklausomumo reikalaujama pagal Sąjungos teisę;

(157) šiuo reglamentu nedaromas poveikis atitinkamų nacionalinių valdžios institucijų ar įstaigų, kurios prižiūri, kaip taikoma Sąjungos teisė, kuria saugomos pagrindinės teisės, įskaitant lygybės institucijas ir duomenų apsaugos institucijas, kompetencijai, užduotims, įgaliojimams ir nepriklausomumui. Prireikus atsižvelgiant į tų nacionalinių valdžios institucijų ar įstaigų įgaliojimus, jos taip pat turėtų turėti prieigą prie bet kokių pagal šį reglamentą sukurtų dokumentų. Siekiant užtikrinti tinkamą ir savalaikį DI sistemoms, keliančioms riziką sveikatai, saugai ir pagrindinėms teisėms, taikomų reikalavimų vykdymą, turėtų būti nustatyta speciali apsaugos procedūra. Tokioms DI sistemoms, dėl kurių kyla rizika, turėtų būti taikoma procedūra, skirta didelės rizikos DI sistemoms, dėl kurių kyla rizika, draudžiamoms sistemoms, pateiktoms rinkai, pradėtoms naudoti arba naudojamoms taikant šiame reglamente nustatytą draudžiamą praktiką, ir DI sistemoms, kurios buvo pateiktos rinkai pažeidžiant šiame reglamente nustatytus skaidrumo reikalavimus ir kelia riziką;

(158) Sąjungos finansinių paslaugų teisėje yra 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 atitinkamų taisyklių ir reikalavimų taikymą ir vykdymo užtikrinimą, už tų teisės aktų priežiūrą ir vykdymo užtikrinimą atsakingos kompetentingos institucijos, visų pirma kompetentingos institucijos, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) Nr. 575/2013[46] ir Europos Parlamento ir Tarybos direktyvose 2008/48/EB[47], 2009/138/EB[48], 2013/36/ES[49], 2014/17/ES[50] ir (ES) 2016/97[51], pagal jų atitinkamą kompetenciją turėtų būti paskirtos kompetentingomis institucijomis, atsakingomis už šio reglamento įgyvendinimo priežiūrą, be kita ko, už rinkos priežiūros veiklą, kiek tai susiję su DI sistemomis, kurias tiekia arba naudoja reguliuojamos ir prižiūrimos finansų įstaigos, nebent valstybės narės nusprendžia paskirti kitą instituciją šioms rinkos priežiūros užduotims atlikti.

---

46 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl riziką ribojančių reikalavimų kredito įstaigoms, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).

47 2008 m. balandžio 23 d. Europos Parlamento ir Tarybos direktyva 2008/48/EB dėl vartojimo kredito sutarčių ir panaikinanti Tarybos direktyvą 87/102/EEB (OL L 133, 2008 5 22, p. 66).

48 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2009 12 17, p. 1).

49 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 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).

50 2014 m. vasario 4 d. Europos Parlamento ir Tarybos direktyva 2014/17/ES dėl vartojimo kredito sutarčių dėl gyvenamosios paskirties nekilnojamojo turto, kuria iš dalies keičiamos direktyvos 2008/48/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 (OL L 60, 2014 2 28, p. 34).

51 2016 m. sausio 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/97 dėl draudimo produktų platinimo (OL L 26, 2016 2 2, p. 19).

Tos kompetentingos institucijos turėtų turėti visus įgaliojimus pagal šį reglamentą ir Reglamentą (ES) 2019/1020, kad užtikrintų šiame reglamente nustatytų reikalavimų ir pareigų vykdymą, įskaitant įgaliojimus vykdyti *ex post* rinkos priežiūros veiklą, kuri atitinkamai gali būti integruota į jų esamus priežiūros mechanizmus ir procedūras pagal atitinkamą Sąjungos finansinių paslaugų teisę. Tikslinga numatyti, kad, veikdamos kaip rinkos priežiūros institucijos pagal šį reglamentą, nacionalinės institucijos, atsakingos už pagal Direktyvą 2013/36/ES reglamentuojamų kredito įstaigų, dalyvaujančių Tarybos reglamentu (ES) Nr. 1024/2013[52] sukurtame bendrame priežiūros mechanizme, priežiūrą, turėtų nedelsdamos pateikti Europos Centriniam Bankui visą vykdant rinkos priežiūros veiklą nustatytą informaciją, kuri gali būti svarbi Europos Centrinio Banko prudencinės priežiūros užduotims, kaip nurodyta tame reglamente. Siekiant toliau didinti šio reglamento ir pagal Direktyvą 2013/36/ES reglamentuojamoms kredito įstaigoms taikomų taisyklių suderinamumą, taip pat yra tinkama kai kurias tiekėjų procedūrines pareigas, susijusias su rizikos valdymu, priežiūra po pateikimo rinkai ir dokumentais, integruoti į esamas Direktyvoje 2013/36/ES nustatytas 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 diegėjams nustatyti stebėsenos pareigą tiek, kiek ji taikoma pagal Direktyvą 2013/36/ES reglamentuojamoms kredito įstaigoms. Ta pati tvarka turėtų būti taikoma draudimo ir perdraudimo įmonėms bei draudimo kontroliuojančiosioms bendrovėms pagal Direktyvą 2009/138/EB ir draudimo tarpininkams pagal Direktyvą (ES) 2016/97, taip pat kitų rūšių finansų įstaigoms, kurioms taikomi vidaus valdymo, tvarkos ar procesų reikalavimai, nustatyti pagal atitinkamą Sąjungos finansinių paslaugų teisę, siekiant užtikrinti nuoseklumą ir vienodas sąlygas finansų sektoriuje;

---

[52] 2013 m. spalio 15 d. Tarybos reglamentas (ES) Nr. 1024/2013, kuriuo Europos Centriniam Bankui pavedami specialūs uždaviniai, susiję su rizikos ribojimu pagrįstos kredito įstaigų priežiūros politika (OL L 287, 2013 10 29, p. 63).

(159) kiekviena šio reglamento priede išvardytų didelės rizikos DI sistemų biometrinių duomenų srityje rinkos priežiūros institucija, jei tos sistemos naudojamos teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo arba teisingumo vykdymo ir demokratinių procesų tikslais, turėtų turėti veiksmingus tyrimo ir taisomuosius įgaliojimus, įskaitant bent įgaliojimus gauti prieigą prie visų tvarkomų asmens duomenų ir visos jos užduotims atlikti būtinos informacijos. Rinkos priežiūros institucijos turėtų galėti vykdyti savo įgaliojimus veikdamos visiškai nepriklausomai. Bet kokie jų prieigos prie neskelbtinų operatyvinių duomenų apribojimai pagal šį reglamentą neturėtų daryti poveikio pagal Direktyvą (ES) 2016/680 joms suteiktiems įgaliojimams. Jokia išimtis dėl duomenų atskleidimo nacionalinėms duomenų apsaugos institucijoms pagal šį reglamentą neturėtų daryti poveikio dabartiniams ar būsimiems tų institucijų įgaliojimams, nepatenkantiems į šio reglamento taikymo sritį;

(160) rinkos priežiūros institucijos ir Komisija turėtų turėti galimybę siūlyti bendrą veiklą, įskaitant bendrus tyrimus, kurią vykdytų kelios rinkos priežiūros institucijos arba rinkos priežiūros institucijos kartu su Komisija ir kurios tikslas – skatinti atitiktį, nustatyti neatitiktį, didinti informuotumą ir teikti su šiuo reglamentu susijusias gaires dėl konkrečių kategorijų didelės rizikos DI sistemų, kurios, kaip nustatyta, kelia didelę riziką dviejose ar daugiau valstybių narių. Bendra veikla, kuria skatinama atitiktis, turėtų būti vykdoma pagal Reglamento (ES) 2019/1020 9 straipsnį. DI tarnyba turėtų teikti bendrų tyrimų koordinavimo paramą;

(161) būtina paaiškinti atsakomybę ir kompetenciją Sąjungos ir nacionaliniu lygmenimis, kiek tai susiję su bendrosios paskirties DI modeliais grindžiamomis DI sistemomis. Siekiant išvengti kompetencijos dubliavimosi, tais atvejais, kai DI sistema grindžiama bendrosios paskirties DI modeliu, ir modelį ir sistemą teikia tas pats tiekėjas, priežiūra turėtų būti vykdoma Sąjungos lygmeniu per DI tarnybą, kuri šiuo tikslu turėtų turėti rinkos priežiūros institucijos įgaliojimus, kaip tai suprantama Reglamente (ES) 2019/1020. Visais kitais atvejais už DI sistemų priežiūrą tebėra atsakingos nacionalinės rinkos priežiūros institucijos. Tačiau dėl bendrosios paskirties DI sistemų, kurias diegėjai gali tiesiogiai naudoti bent vienai paskirčiai, priskiriamai didelės rizikos kategorijai, rinkos priežiūros institucijos turėtų bendradarbiauti su DI tarnyba, kad atliktų atitikties vertinimus ir atitinkamai informuotų Valdybą ir kitas rinkos priežiūros institucijas. Be to, rinkos priežiūros institucijos turėtų turėti galimybę prašyti DI tarnybos pagalbos, kai rinkos priežiūros institucija negali užbaigti didelės rizikos DI sistemos tyrimo dėl to, kad ji negali gauti tam tikros informacijos, susijusios su bendrosios paskirties DI modeliu, kuriuo grindžiama didelės rizikos DI sistema. Tokiais atvejais *mutatis mutandis* turėtų būti taikoma Reglamento (ES) 2019/1020 VI skyriuje nustatyta savitarpio pagalbos tarpvalstybiniais atvejais procedūra;

(162) siekiant kuo geriau pasinaudoti centralizuotomis Sąjungos ekspertinėmis žiniomis ir sinergija Sąjungos lygmeniu, bendrosios paskirties DI modelių tiekėjų priežiūros ir pareigų vykdymo užtikrinimo įgaliojimai turėtų priklausyti Komisijos kompetencijai. DI tarnyba turėtų galėti imtis visų būtinų veiksmų stebėti, ar šis reglamentas įgyvendinamas veiksmingai, kiek tai susiję su bendrosios paskirties DI modeliais. Ji turėtų galėti tirti galimus taisyklių, taikomų bendrosios paskirties DI modelių tiekėjams, pažeidimus tiek savo iniciatyva, atsižvelgdama į savo stebėsenos veiklos rezultatus, tiek rinkos priežiūros institucijų prašymu, laikydamasi šiame reglamente nustatytų sąlygų. Siekiant remti veiksmingą DI tarnybos vykdomą stebėseną, turėtų būti numatyta galimybė tolesnės grandies tiekėjams teikti skundus dėl taisyklių, taikomų bendrosios paskirties DI modelių ir sistemų tiekėjams, galimų pažeidimų;

(163) siekiant papildyti bendrosios paskirties DI modelių valdymo sistemas, mokslinė komisija turėtų remti DI tarnybos stebėsenos veiklą ir tam tikrais atvejais galėtų DI tarnybai teikti kvalifikuotus perspėjimus, dėl kurių reikia imtis tolesnių veiksmų, pavyzdžiui, tyrimų. Taip turėtų būti tuo atveju, kai mokslinė komisija turi pagrindo įtarti, kad bendrosios paskirties DI modelis kelia konkrečią ir nustatomą riziką Sąjungos lygmeniu. Be to, taip turėtų būti tuo atveju, kai mokslinė komisija turi pagrindo įtarti, kad bendrosios paskirties DI modelis atitinka kriterijus, pagal kuriuos jį būtų galima klasifikuoti kaip sisteminės rizikos bendrosios paskirties DI modelį. Tam, kad mokslinei komisijai būtų suteikta toms užduotims atlikti būtina informacija, turėtų būti nustatytas mechanizmas, pagal kurį mokslinė komisija galėtų prašyti Komisijos reikalauti, kad tiekėjas pateiktų dokumentus ar informaciją;

(164) DI tarnyba turėtų galėti imtis būtinų veiksmų stebėti, ar veiksmingai įgyvendinamos šiame reglamente nustatytos bendrosios paskirties DI modelių tiekėjų pareigos ir ar jų laikomasi. DI tarnyba turėtų turėti galimybę tirti galimus pažeidimus pagal šiame reglamente numatytus įgaliojimus, be kita ko, prašydama dokumentų ir informacijos, atlikdama vertinimus ir prašydama, kad bendrosios paskirties DI modelių tiekėjai imtųsi priemonių. Tam, kad atlikdama vertinimus DI tarnyba pasinaudotų nepriklausomomis ekspertinėmis žiniomis, ji turėtų turėti galimybę įtraukti nepriklausomus ekspertus vertinimams jos vardu atlikti. Pareigų vykdymas turėtų būti užtikrinamas, *inter alia*, teikiant prašymus imtis tinkamų priemonių, įskaitant rizikos mažinimo priemones nustatytos sisteminės rizikos atveju, taip pat apribojant tiekimą rinkai, pašalinant ar atšaukiant modelį. Kaip apsaugos priemonė, prireikus viršijant šiame reglamente numatytas procesines teises, bendrosios paskirties DI modelių tiekėjai turėtų turėti Reglamento (ES) 2019/1020 18 straipsnyje numatytas procesines teises, kurios turėtų būti taikomos *mutatis mutandis*, nedarant poveikio konkretesnėms procesinėms teisėms, numatytoms šiame reglamente;

(165) DI sistemų, išskyrus didelės rizikos DI sistemas, kūrimas laikantis šio reglamento reikalavimų gali prisidėti prie platesnio masto etiško ir patikimo DI įsisavinimo Sąjungoje. Didelės rizikos nekeliančių DI sistemų tiekėjai turėtų būti skatinami kurti elgesio kodeksus, įskaitant susijusius valdymo mechanizmus, kuriais būtų skatinama savanoriškai taikyti kai kuriuos arba visus didelės rizikos DI sistemoms taikomus privalomus reikalavimus, pritaikytus atsižvelgiant į numatytąją sistemų paskirtį ir susijusią mažesnę riziką, taip pat atsižvelgiant į turimus techninius sprendimus ir sektoriaus geriausią praktiką, pavyzdžiui, modelių ir duomenų korteles. Visų didelės rizikos arba nerizikingų DI sistemų ir DI modelių tiekėjai ir, kai tinkama, diegėjai taip pat turėtų būti skatinami savanoriškai taikyti papildomus reikalavimus, susijusius, pavyzdžiui, su Sąjungos patikimo DI etikos gairių elementais, aplinkos tvarumu, raštingumo DI srityje priemonėmis, įtraukiu ir įvairiu DI sistemų projektavimu ir kūrimu, įskaitant dėmesį pažeidžiamiems asmenims ir prieinamumą asmenims su negalia, su suinteresuotųjų subjektų dalyvavimu, įtraukiant, kai tinkama, atitinkamus suinteresuotuosius subjektus, pavyzdžiui, verslo ir pilietinės visuomenės organizacijas, akademinę bendruomenę, mokslinių tyrimų organizacijas, profesines sąjungas ir vartotojų apsaugos organizacijas, projektuojant ir kuriant DI sistemas, ir su kūrimo grupių įvairove, įskaitant lyčių pusiausvyrą. Siekiant užtikrinti, kad savanoriški elgesio kodeksai būtų veiksmingi, jie turėtų būti grindžiami aiškiais tikslais ir pagrindiniais veiklos rezultatų rodikliais, kad būtų galima įvertinti, ar tie tikslai pasiekti. Jie taip pat turėtų būti rengiami įtraukiai, kai tinkama, dalyvaujant atitinkamiems suinteresuotiesiems subjektams, pavyzdžiui, verslo ir pilietinės visuomenės organizacijoms, akademinei bendruomenei, mokslinių tyrimų organizacijoms, profesinėms sąjungoms ir vartotojų apsaugos organizacijoms. 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;

(166) svarbu, kad DI sistemos, susijusios su gaminiais, kurie, remiantis šiuo reglamentu, nekelia didelės rizikos ir todėl neprivalo atitikti didelės rizikos DI sistemoms nustatytų reikalavimų, vis tiek būtų saugios jas pateikiant rinkai arba pradedant naudoti. Siekiant prisidėti prie šio tikslo, Europos Parlamento ir Tarybos reglamentas (ES) 2023/988[53] būtų taikomas kaip apsaugos sistema;

(167) siekiant užtikrinti patikimą ir konstruktyvų kompetentingų institucijų bendradarbiavimą Sąjungos ir nacionaliniu lygmenimis, visos šalys, kurios dalyvauja taikant šį reglamentą, turėtų užtikrinti informacijos ir duomenų, gautų vykdant savo užduotis, konfidencialumą pagal Sąjungos ar nacionalinę teisę. Jos turėtų vykdyti savo užduotis ir veiklą taip, kad visų pirma apsaugotų intelektinės nuosavybės teises, konfidencialią verslo informaciją ir komercines paslaptis, veiksmingą šio reglamento įgyvendinimą, visuomenės ir nacionalinio saugumo interesus, baudžiamojo ir administracinio proceso integralumą ir įslaptintos informacijos integralumą;

---

[53] 2023 m. gegužės 10 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/988 dėl bendros gaminių saugos, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 bei Europos Parlamento ir Tarybos direktyva (ES) 2020/1828 ir panaikinamos Europos Parlamento ir Tarybos direktyva 2001/95/EB bei Tarybos direktyva 87/357/EEB (OL L 135, 2023 5 23, p. 1).

(168) šio reglamento laikymasis turėtų būti užtikrinamas nustatant sankcijas ir kitas vykdymo užtikrinimo priemones. 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, ir kad būtų vadovaujamasi principu *ne bis in idem*. Siekiant sugriežtinti ir suderinti administracines sankcijas už šio reglamento pažeidimus, turėtų būti nustatytos viršutinės administracinių baudų už tam tikrus konkrečius pažeidimus ribos. Nustatydamos baudų dydį, valstybės narės kiekvienu atskiru atveju turėtų atsižvelgti į visas svarbias konkrečios situacijos aplinkybes, visų pirma atsižvelgti į pažeidimo pobūdį, sunkumą ir trukmę, sukeltas pasekmes ir tiekėjo dydį, ypač jei tiekėjas yra MVĮ, įskaitant startuolius. Europos duomenų apsaugos priežiūros pareigūnas taip pat turėtų turėti įgaliojimus skirti baudas Sąjungos institucijoms, agentūroms ir įstaigoms, kurios patenka į šio reglamento taikymo sritį;

(169) pagal šį reglamentą nustatytų bendrosios paskirties DI modelių tiekėjų pareigų vykdymas turėtų būti užtikrinamas, *inter alia*, skiriant baudas. Tuo tikslu taip pat turėtų būti nustatyti tinkami baudų dydžiai už tų pareigų pažeidimą, įskaitant priemonių, kurių Komisija prašo imtis pagal šį reglamentą, nesilaikymą, taikant tinkamus laiko ribų terminus pagal proporcingumo principą. Visus pagal šį reglamentą priimtus Komisijos sprendimus pagal SESV gali peržiūrėti Europos Sąjungos Teisingumo Teismas, įskaitant neribotą Teisingumo Teismo jurisdikciją dėl sankcijų pagal SESV 261 straipsnį;

(170) Sąjungos ir nacionalinėje teisėje jau numatytos veiksmingos teisių gynimo priemonės fiziniams ir juridiniams asmenims, kurių teisėms ir laisvėms DI sistemų naudojimas daro neigiamą poveikį. Nedarant poveikio toms teisių gynimo priemonėms, bet kuris fizinis ar juridinis asmuo, turintis pagrindo manyti, kad šis reglamentas buvo pažeistas, gali atitinkamai rinkos priežiūros institucijai pateikti skundą;

(171) asmenys, kuriems daromas poveikis, turėtų turėti teisę gauti paaiškinimą, kai diegėjo sprendimas daugiausia grindžiamas tam tikrų didelės rizikos AI sistemų, kurios patenka į šio reglamento taikymo sritį, išvediniais ir kai tas sprendimas sukelia teisinių pasekmių arba daro panašų didelį poveikį tiems asmenims taip, kad, jų nuomone, daro neigiamą poveikį jų sveikatai, saugai ar pagrindinėms teisėms. Tas paaiškinimas turėtų būti aiškus ir prasmingas ir jis turėtų sudaryti pagrindą, kuriuo remdamiesi asmenys, kuriems daromas poveikis, galėtų naudotis savo teisėmis. Teisė gauti paaiškinimą neturėtų būti taikoma DI sistemų, kurioms taikomos išimtys ar apribojimai pagal Sąjungos ar nacionalinę teisę, naudojimui ir turėtų būti taikoma tik tiek, kiek ši teisė dar nenumatyta Sąjungos teisėje;

(172) asmenys, pranešantys apie šio reglamento pažeidimus, (pranešėjai) turėtų būti apsaugomi pagal Sąjungos teisę. Todėl pranešimams apie šio reglamento pažeidimus ir asmenų, pranešančių apie tokius pažeidimus, apsaugai turėtų būti taikoma Europos Parlamento ir Tarybos direktyva (ES) 2019/1937[54];

[54] 2019 m. spalio 23 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos (OL L 305, 2019 11 26, p. 17).

(173) siekiant užtikrinti, kad prireikus reguliavimo sistemą būtų galima pritaikyti, pagal SESV 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus, kuriais iš dalies keičiamos sąlygos, kuriomis DI sistema nelaikoma keliančia didelę riziką, didelės rizikos DI sistemų sąrašas, nuostatos dėl techninių dokumentų, ES atitikties deklaracijos turinys, nuostatos dėl atitikties vertinimo procedūrų, nuostatos, kuriomis nustatomos didelės rizikos DI sistemos, kurioms turėtų būti taikoma kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu grindžiama atitikties vertinimo procedūra, ribinės vertės, lyginamieji parametrai ir rodikliai, be kita ko, papildant tuos lyginamuosius parametrus ir rodiklius, sisteminės rizikos bendrosios paskirties DI modelių klasifikavimo taisyklėse, sisteminės rizikos bendrosios paskirties DI modelių priskyrimo kriterijai, bendrosios paskirties DI modelių tiekėjams skirti techniniai dokumentai ir skaidrumo informacija bendrosios paskirties DI modelių tiekėjams. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros[55] nustatytais principais. 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;

[55] OL L 123, 2016 5 12, p. 1.

(174) atsižvelgdama į sparčią technologinę plėtrą ir technines ekspertines žinias, reikalingas, kad šis reglamentas būtų veiksmingai taikomas, Komisija ne vėliau kaip … [penkeri metai nuo šio reglamento įsigaliojimo dienos], o vėliau – kas ketverius metus turėtų įvertinti ir peržiūrėti šį reglamentą ir pateikti ataskaitą Europos Parlamentui ir Tarybai. Be to, atsižvelgiant į poveikį šio reglamento taikymo sričiai, Komisija kartą per metus turėtų įvertinti poreikį iš dalies pakeisti didelės rizikos DI sistemų sąrašą ir draudžiamos praktikos sąrašą. Taip pat ne vėliau kaip … [ketveri metai nuo šio reglamento įsigaliojimo dienos], o vėliau – kas ketverius metus Komisija turėtų įvertinti poreikį iš dalies pakeisti šio reglamento priede pateiktą didelės rizikos sričių pavadinimų sąrašą, DI sistemas, kurioms taikomos skaidrumo pareigos, priežiūros ir valdymo sistemos veiksmingumą, pažangą rengiant standartizacijos leidinius, susijusius su bendrosios paskirties DI modelių kūrimu efektyviai vartojant energiją, įskaitant tolesnių priemonių ar veiksmų poreikį, ir pateikti ataskaitą Europos Parlamentui ir Tarybai. Galiausiai ne vėliau kaip … [ketveri metai nuo šio reglamento įsigaliojimo dienos], o vėliau – kas trejus metus Komisija turėtų įvertinti savanoriškų elgesio kodeksų poveikį ir veiksmingumą siekiant skatinti taikyti didelės rizikos DI sistemoms nustatytus reikalavimus kitoms DI sistemoms nei didelės rizikos DI sistemos ir galbūt kitus papildomus tokioms DI sistemoms taikomus reikalavimus;

(175) 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[56];

(176) kadangi šio reglamento tikslo, t. y. pagerinti vidaus rinkos veikimą, skatinti į žmogų orientuoto ir patikimo DI įsisavinimą, kartu užtikrinant aukšto lygio sveikatos, saugos, Chartijoje įtvirtintų pagrindinių teisių apsaugą, įskaitant demokratiją, teisinę valstybę ir aplinkos apsaugą nuo žalingo DI sistemų poveikio Sąjungoje, ir remti inovacijas, valstybės narės negali deramai pasiekti, o dėl siūlomo veiksmo masto arba poveikio to tikslo būtų geriau siekti Sąjungos lygmeniu, laikydamasi ES sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti;

---

[56] 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).

(177) siekiant užtikrinti teisinį tikrumą, veiklos vykdytojams užtikrinti tinkamą prisitaikymo laikotarpį ir išvengti rinkos sutrikdymo, be kita ko, užtikrinant DI sistemų naudojimo tęstinumą, tikslinga, kad šis reglamentas būtų taikomas didelės rizikos DI sistemoms, kurios buvo pateiktos rinkai arba pradėtos naudoti iki jo bendros taikymo pradžios datos, tik tuo atveju, jeigu po tos datos tų sistemų konstrukcija ar numatytoji paskirtis reikšmingai pasikeitė. Tikslinga paaiškinti, kad šiuo atžvilgiu reikšmingo pakeitimo sąvoka turėtų būti suprantama kaip iš esmės lygiavertė esminio pakeitimo sąvokai, kuri pagal šį reglamentą taikoma tik didelės rizikos DI sistemoms. Išimties tvarka ir atsižvelgiant į viešąją atskaitomybę, DI sistemų, kurios yra didelės apimties IT sistemų, nustatytų šio reglamento priede išvardytais teisės aktais, komponentai, operatoriai ir didelės rizikos DI sistemų, kurias ketina naudoti valdžios institucijos, operatoriai atitinkamai turėtų imtis būtinų veiksmų, kad ne vėliau kaip 2030 m. pabaigoje ir ne vėliau kaip … [šešeri metai nuo šio reglamento įsigaliojimo dienos] būtų laikomasi šio reglamento reikalavimų;

(178) didelės rizikos DI sistemų tiekėjai raginami jau pereinamuoju laikotarpiu savanoriškai pradėti vykdyti atitinkamas šiame reglamente nustatytas pareigas;

(179) šis reglamentas turėtų būti taikomas nuo … [dveji metai nuo šio reglamento įsigaliojimo dienos]. Tačiau, atsižvelgiant į nepriimtiną riziką, susijusią su DI naudojimu tam tikrais būdais, draudimai bei bendros šio reglamento nuostatos turėtų būti taikomi jau nuo … [šeši mėnesiai nuo šio reglamento įsigaliojimo dienos]. Nors visapusiškas tų draudimų poveikis užtikrinamas nustačius šio reglamento valdymą ir vykdymo užtikrinimą, svarbu numatyti draudimų taikymą, kad būtų atsižvelgta į nepriimtiną riziką ir būtų daromas poveikis kitoms procedūroms, pavyzdžiui, civilinėje teisėje. Be to, su valdymo struktūra ir atitikties vertinimo sistema susijusi infrastruktūra turėtų būti parengta veikti anksčiau nei … [dveji metai nuo šio reglamento įsigaliojimo dienos], todėl su notifikuotosiomis įstaigomis ir valdymo struktūra susijusios nuostatos turėtų būti taikomos nuo … [12 mėnesių nuo šio reglamento įsigaliojimo dienos]. Atsižvelgiant į spartų technologinės pažangos tempą ir bendrosios paskirties DI modelių diegimą, bendrosios paskirties DI modelių tiekėjų pareigos turėtų būti taikomos nuo … [12 mėnesių nuo šio reglamento įsigaliojimo dienos]. Praktikos kodeksai turėtų būti parengti ne vėliau kaip … [9 mėnesiai nuo šio reglamento įsigaliojimo dienos] siekiant sudaryti tiekėjams sąlygas laiku įrodyti, kad jie laikosi reikalavimų. DI tarnyba turėtų užtikrinti, kad klasifikavimo taisyklės ir procedūros būtų atnaujinamos atsižvelgiant į technologinę plėtrą. Be to, valstybės narės turėtų nustatyti ir pranešti Komisijai apie sankcijų, įskaitant administracines baudas, taisykles ir užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendintos iki šio reglamento taikymo pradžios datos. Todėl nuostatos dėl sankcijų turėtų būti taikomos nuo … [12 mėnesių nuo šio reglamento įsigaliojimo dienos];

(180) vadovaujantis Reglamento (ES) 2018/1725 42 straipsnio 1 ir 2 dalimis buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir Europos duomenų apsaugos valdyba ir jie pateikė savo bendrą nuomonę 2021 m. birželio 18 d.,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius
Bendrosios nuostatos

1 straipsnis

Dalykas

1. Šio reglamento tikslas – pagerinti vidaus rinkos veikimą ir skatinti į žmogų orientuoto ir patikimo dirbtinio intelekto (DI) įsisavinimą, kartu užtikrinant aukšto lygio sveikatos, saugos, Chartijoje įtvirtintų pagrindinių teisių apsaugą, įskaitant demokratiją, teisinę valstybę ir aplinkos apsaugą nuo žalingo DI sistemų poveikio Sąjungoje, ir remiant inovacijas.

2. Šiuo reglamentu nustatoma:

   a) suderintos DI sistemų pateikimo rinkai, pradėjimo naudoti ir naudojimo Sąjungoje taisyklės;

   b) tam tikros su DI susijusios praktikos draudimai;

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

   d) suderintos tam tikroms DI sistemoms taikomos skaidrumo taisyklės;

   e) bendrosios paskirties DI modelių pateikimo rinkai suderintos taisyklės;

f) rinkos stebėsenos, rinkos priežiūros, valdymo ir vykdymo užtikrinimo taisyklės;

g) inovacijų rėmimo priemonės, ypatingą dėmesį skiriant MVĮ, įskaitant startuolius.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas:

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

b) Sąjungoje įsisteigimo vietą turintiems arba esantiems DI diegėjams;

c) trečiojoje valstybėje įsisteigimo vietą turintiems arba esantiems DI sistemų, kurių sugeneruoti išvediniai naudojami Sąjungoje, tiekėjams ir diegėjams;

d) DI sistemų importuotojams ir platintojams;

e) gaminių gamintojams, kurie pateikia rinkai arba pradeda naudoti DI sistemą kartu su savo gaminiu ir savo vardu ar naudodami savo prekių ženklą;

f) ne Sąjungoje įsisteigusių tiekėjų įgaliotiesiems atstovams;

g) Sąjungoje esantiems asmenims, kuriems daromas poveikis.

2. DI sistemoms, kurios pagal 6 straipsnio 1 dalį klasifikuojamos kaip didelės rizikos DI sistemos ir yra susijusios su gaminiais, kuriems taikomi I priedo B skirsnyje išvardyti Sąjungos derinamieji teisės aktai, taikomi tik 6 straipsnio 1 dalis, 102–109 straipsniai ir 112 straipsnis. 57 straipsnis taikomas tik tiek, kiek didelės rizikos DI sistemoms pagal šį reglamentą taikomi reikalavimai buvo integruoti į tuos Sąjungos derinamuosius teisės aktus.

3. Šis reglamentas netaikomas sritims, kurios nepatenka į Sąjungos teisės taikymo sritį, ir bet kuriuo atveju nedaro poveikio valstybių narių kompetencijai nacionalinio saugumo srityje, neatsižvelgiant į subjektų, kuriems valstybės narės patikėjo vykdyti su ta kompetencija susijusias užduotis, rūšį.

Šis reglamentas netaikomas DI sistemoms, kai ir tiek, kiek jos pateikiamos rinkai, pradedamos naudoti arba naudojamos su pakeitimais ar be jų tik kariniais, gynybos ar nacionalinio saugumo tikslais, neatsižvelgiant į tą veiklą vykdančio subjekto rūšį.

Šis reglamentas netaikomas DI sistemoms, kurios nėra pateiktos rinkai ir nėra pradėtos naudoti Sąjungoje, kai jų išvediniai yra naudojami Sąjungoje tik kariniais, gynybos ar nacionalinio saugumo tikslais, neatsižvelgiant į tą veiklą vykdančio subjekto rūšį.

4. Šis reglamentas taip pat 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 vykdydamos tarptautinį bendradarbiavimą arba susitarimus teisėsaugos ir teisminio bendradarbiavimo su Sąjunga arba su viena ar daugiau valstybių narių tikslais, jei tokia trečioji valstybė ar tarptautinė organizacija numato tinkamas saugumo priemones asmenų pagrindinėms teisėms ir laisvėms apsaugoti.

5. Šis reglamentas nedaro poveikio Reglamento (ES) 2022/2065 II skyriuje išdėstytų nuostatų dėl tarpininkavimo paslaugų teikėjų atsakomybės taikymui.

6. Šis reglamentas netaikomas DI sistemoms ar DI modeliams, įskaitant jų išvedinius, kurie specialiai sukurti ir pradėti naudoti vien mokslinių tyrimų ir plėtros tikslais.

7. Asmens duomenims, tvarkomiems atsižvelgiant į šiame reglamente nustatytas teises ir pareigas, taikoma Sąjungos teisė dėl asmens duomenų apsaugos, privatumo ir pranešimų konfidencialumo. Šis reglamentas nedaro poveikio Reglamentui (ES) 2016/679 ar (ES) 2018/1725, Direktyvai 2002/58/EB ar (ES) 2016/680, nedarant poveikio šio reglamento 10 straipsnio 5 daliai ir 59 straipsniui.

8. Šis reglamentas netaikomas jokiai mokslinių tyrimų, bandymų ar plėtros veiklai, susijusiai su DI sistemomis ar DI modeliais, prieš juos pateikiant rinkai ar pradedant naudoti. Tokia veikla vykdoma laikantis taikytinos Sąjungos teisės. Ši nuostata dėl netaikymo netaikoma bandymams realiomis sąlygomis.

9. Šiuo reglamentu nedaromas poveikis kitais Sąjungos teisės aktais, susijusiais su vartotojų apsauga ir gaminių sauga, nustatytoms taisyklėms.

10. Šis reglamentas netaikomas diegėjų, kurie yra fiziniai asmenys, naudojantys DI sistemas vykdydami tik asmeninę neprofesinę veiklą, pareigoms.

11. Šiuo reglamentu Sąjungai ar valstybėms narėms neužkertamas kelias toliau taikyti arba priimti darbuotojams palankesnius įstatymus ir kitus teisės aktus, kiek tai susiję su jų teisių apsauga, kai darbdaviai naudoja DI sistemas, arba skatinti ar leisti taikyti darbuotojams palankesnes kolektyvines sutartis.

12. Šis reglamentas netaikomas DI sistemoms, išleistoms pagal nemokamas atvirojo kodo licencijas, nebent jos pateikiamos rinkai arba pradedamos naudoti kaip didelės rizikos DI sistemos arba kaip DI sistemos, patenkančios į 5 arba 50 straipsnio taikymo sritį.

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) DI sistema – mašina grindžiama sistema, suprojektuota veikti įvairiais autonomijos lygiais, kuri po diegimo gali veikti prisitaikydama ir kuri, siekiant aiškių ar numanomų tikslų, iš gautos įvesties duomenų daro išvadą, kaip generuoti išvedinius, pavyzdžiui, predikcijas, turinį, rekomendacijas ar sprendinius, kurie gali turėti įtakos fizinei ar virtualiai aplinkai;

2) rizika – žalos atsiradimo tikimybės ir tos žalos masto derinys;

3) tiekėjas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kurie kuria DI sistemą arba bendrosios paskirties DI modelį arba nurodo kurti DI sistemą arba bendrosios paskirties DI modelį ir pateikia juos rinkai arba pradeda DI sistemą naudoti savo vardu ar su savo prekių ženklu už atlygį arba nemokamai;

4) diegėjas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, naudojantys DI sistemą pagal savo įgaliojimus , išskyrus atvejus, kai DI sistema naudojama asmeniniais neprofesinės veiklos tikslais;

5) įgaliotasis atstovas – Sąjungoje esantis ar įsisteigęs fizinis arba juridinis asmuo, gavęs ir priėmęs raštišką DI sistemos arba bendrosios paskirties DI modelio tiekėjo įgaliojimą jo vardu vykdyti šiame reglamente nustatytas pareigas ir procedūras;

6) importuotojas – Sąjungoje esantis ar įsisteigęs fizinis arba juridinis asmuo, rinkai pateikiantis DI sistemą, kurios pavadinimas arba prekių ženklas priklauso trečiojoje valstybėje įsisteigusiam fiziniam arba juridiniam asmeniui;

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

8) veiklos vykdytojas – tiekėjas, gaminių gamintojas, diegėjas, įgaliotasis atstovas, importuotojas arba platintojas;

9) pateikimas rinkai – DI sistemos arba bendrosios paskirties DI modelio tiekimas Sąjungos rinkai pirmą kartą;

10) tiekimas rinkai – DI sistemos arba bendrosios paskirties DI modelio tiekimas už atlygį arba nemokamai siekiant juos platinti arba naudoti Sąjungos rinkoje vykdant komercinę veiklą;

11) pradėjimas naudoti –DI sistemos pateikimas pirmą kartą naudoti tiesiogiai diegėjui arba savo reikmėms Sąjungoje pagal jos numatytąją paskirtį;

12) numatytoji paskirtis – tiekėjo numatyta DI sistemos paskirtis, įskaitant konkrečias naudojimo aplinkybes ir sąlygas, nurodyta informacijoje, kurią tiekėjas pateikė naudojimo instrukcijoje, 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, įskaitant kitas DI sistemas;

14) saugos komponentas – gaminio arba DI sistemos komponentas, kuris atlieka to gaminio ar DI 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 siekdamas informuoti diegėją visų pirma apie numatytąją DI sistemos paskirtį bei tinkamą jos naudojimą ;

16) DI sistemos atšaukimas – priemonės, kuriomis siekiama, kad diegėjams jau pateikta DI sistema būtų grąžinta tiekėjui arba kad ji būtų nebenaudojama arba jos naudojimas būtų padarytas neįmanomas;

17) DI sistemos pašalinimas – priemonės, kuriomis siekiama neleisti tiekimo grandinėje esančios DI sistemos tiekti rinkai;

18) DI sistemos veikimo efektyvumas – 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 – įrodymo, kad įvykdyti III skyriaus 2 skirsnyje nustatyti su didelės rizikos DI sistema susiję 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, notifikuota pagal šį reglamentą ir kitus atitinkamus Sąjungos derinamuosius teisės aktus;

23) esminis pakeitimas – rinkai pateiktos arba pradėtos naudoti DI sistemos pakeitimas, kuris nėra numatytas ar suplanuotas tiekėjo atliekamame pradiniame atitikties vertinime ir kuris daro poveikį DI sistemos atitikčiai II skyriaus 2 skirsnyje nustatytiems reikalavimams arba dėl kurio pasikeičia numatytoji paskirtis, dėl kurios DI sistema buvo vertinta;

24) CE ženklas – ženklas, kuriuo tiekėjas nurodo, kad DI sistema atitinka reikalavimus, nustatytus III skyriaus 2 skirsnyje ir kituose taikytinuose Sąjungos derinamuosiuose teisės aktuose, kuriuose numatytas ženklinimas juo;

25) priežiūros po pateikimo rinkai sistema – visa DI sistemų tiekėjų atliekama veikla, skirta rinkai pateiktų arba pradėtų naudoti DI sistemų naudojimo patirčiai 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, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 dalies c punkte;

28) bendroji specifikacija – techninių specifikacijų, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 4 straipsnio 2 punkte, rinkinys, kuriuo užtikrinama, kad būtų laikomasi tam tikrų šiuo reglamentu nustatytų reikalavimų;

29) mokymo duomenys – duomenys, naudojami DI sistemai mokyti pritaikant jos mokymosi 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 nepakankamo mokymosi arba persimokymo;

31) validavimo duomenų rinkinys – atskiras duomenų rinkinys arba mokymo duomenų rinkinio dalis (fiksuota arba kintama);

32) bandymo duomenys – duomenys, naudojami nepriklausomam DI sistemos vertinimui atlikti siekiant patvirtinti numatomą tos sistemos veikimo efektyvumą prieš ją pateikiant rinkai arba pradedant naudoti;

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

34) biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pavyzdžiui, veido atvaizdai arba daktiloskopiniai duomenys;

35) biometrinis tapatybės nustatymas – automatinis žmogaus fizinių, fiziologinių, elgesio ar psichologinių požymių atpažinimas siekiant nustatyti fizinio asmens tapatybę, lyginant to asmens biometrinius duomenis su duomenų bazėje saugomais asmenų biometriniais duomenimis;

36) biometrinis sutikrinimas – automatizuotas vieno su vienu fizinių asmenų tapatybės tikrinimas, įskaitant autentiškumo patvirtinimą, lyginant jų biometrinius duomenis su anksčiau pateiktais biometriniais duomenimis;

37) specialių kategorijų asmens duomenys – tam tikrų kategorijų asmens duomenys, nurodyti Reglamento (ES) 2016/679 9 straipsnio 1 dalyje, Direktyvos (ES) 2016/680 10 straipsnyje ir Reglamento (ES) 2018/1725 10 straipsnio 1 dalyje;

38) neskelbtini operatyviniai duomenys – operatyviniai duomenys, susiję su nusikalstamų veikų prevencijos, nustatymo, tyrimo ar patraukimo baudžiamojon atsakomybėn už jas veikla, kurių atskleidimas galėtų pakenkti baudžiamojo proceso integralumui;

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

40) biometrinio kategorizavimo sistema – DI sistema, kurios paskirtis – remiantis fizinių asmenų biometriniais duomenimis priskirti juos konkrečioms kategorijoms, išskyrus atvejus, kai ji papildo kitą komercinę paslaugą ir yra tikrai būtina dėl objektyvių techninių priežasčių;

41) nuotolinio biometrinio tapatybės nustatymo sistema – DI sistema, kurios paskirtis – nustatyti fizinių asmenų tapatybę jų aktyviai neįtraukiant, paprastai nuotoliniu būdu, lyginant asmens biometrinius duomenis su informacinėje duomenų bazėje esančiais biometriniais duomenimis ;

42) tikralaikio nuotolinio biometrinio tapatybės nustatymo sistema – nuotolinio biometrinio tapatybės nustatymo sistema, kuri fiksuoja, lygina biometrinius duomenis ir nustato tapatybę be didelės delsos; jai būdingas ne tik tapatybės nustatymas iš karto, bet ir apriboti trumpi delsos laikotarpiai, kad būtų išvengta apėjimo;

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

44) viešai prieinama erdvė – viešam ar privačiam subjektui priklausanti fizinė vieta, prieinama neapibrėžtam skaičiui fizinių asmenų, neatsižvelgiant į tai, ar gali būti taikomos tam tikros prieigos prie jos sąlygos, ir neatsižvelgiant į potencialius talpumo apribojimus;

45) teisėsaugos institucija –

a) valdžios institucija, kurios kompetencijai priklauso nusikalstamos veikos prevencija, tyrimas, atskleidimas ar baudžiamasis persekiojimas už ją arba baudžiamųjų sankcijų 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 baudžiamųjų sankcijų vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais;

46) teisėsauga – veikla, kurią teisėsaugos institucijos vykdo ar kuri yra vykdoma jų vardu nusikalstamos veikos prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už ją arba baudžiamųjų sankcijų vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais;

47) DI tarnyba – Komisijos funkcija, skirta padėti įgyvendinti, stebėti ir prižiūrėti DI sistemas ir bendrosios paskirties DI modelių valdymą, numatyta 2024 m. sausio 24 d. Komisijos sprendimu; šiame reglamente daromos nuorodos į DI tarnybą laikomos nuorodomis į Komisiją;

48) nacionalinė kompetentinga institucija – notifikuojančioji institucija arba rinkos priežiūros institucija; kalbant apie DI sistemas, kurias pradeda naudoti arba naudoja Sąjungos institucijos, agentūros, organai ir įstaigos, nuorodos į nacionalines kompetentingas institucijas arba rinkos priežiūros institucijas šiame reglamente aiškinamos kaip nuorodos į Europos duomenų apsaugos priežiūros pareigūną;

49) rimtas incidentas – incidentas arba DI sistemos veikimo sutrikimas, kuris tiesiogiai ar netiesiogiai nulemia:

a) asmens mirtį arba didelę žalą asmens sveikatai;

b) didelį ir negrįžtamą ypatingos svarbos infrastruktūros valdymo ar eksploatavimo sutrikimą;

c) Sąjungos teisėje, kuria siekiama apsaugoti pagrindines teises, nustatytų pareigų nesilaikymą;

d) didelę žalą turtui arba aplinkai;

50) asmens duomenys – asmens duomenys, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 1 dalyje;

51) ne asmens duomenys – duomenys, kurie nėra asmens duomenys, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 1 punkte;

52) profiliavimas – profiliavimas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 4 punkte;

53) bandymo realiomis sąlygomis planas – dokumentas, kuriame aprašomi bandymo realiomis sąlygomis tikslai, metodika, geografinė aprėptis, populiacija ir laiko aprėptis, stebėsena, organizavimas ir eiga;

54) apribotos bandomosios reglamentavimo aplinkos planas – dokumentas, dėl kurio susitarė dalyvaujantis tiekėjas ir kompetentinga institucija ir kuriame aprašomi apribotoje bandomojoje reglamentavimo aplinkoje vykdomos veiklos tikslai, sąlygos, tvarkaraštis, metodika ir reikalavimai;

55) apribota bandomoji DI reglamentavimo aplinka – kompetentingos institucijos sukurta kontroliuojama sistema, pagal kurią DI sistemų tiekėjams arba galimiems tiekėjams suteikiama galimybė (kai tikslinga – realiomis sąlygomis) kurti, mokyti, patvirtinti ir išbandyti novatorišką DI sistemą ribotą laiką pagal apribotos bandomosios reglamentavimo aplinkos planą, prižiūrint reguliavimo institucijoms;

56) raštingumas DI srityje – įgūdžiai, žinios ir supratimas, leidžiantys tiekėjams, diegėjams ir asmenims, kuriems daromas poveikis, atsižvelgiant į atitinkamas jų teises ir pareigas pagal šį reglamentą, vykdyti informacija pagrįstą DI sistemų diegimą, taip pat didinti savo informuotumą apie DI teikiamas galimybes ir riziką bei žalą, kurią gali sukelti DI;

57) bandymas realiomis sąlygomis – laikinas DI sistemos bandymas pagal numatytąją paskirtį realiomis sąlygomis ne laboratorijoje ar kitaip imituojamoje aplinkoje, siekiant surinkti patikimus ir įtikinamus duomenis ir įvertinti bei patikrinti DI sistemos atitiktį šio reglamento reikalavimams; toks bandymas nelaikomas DI sistemos pateikimu rinkai arba pradėjimu naudoti, kaip tai suprantama šiame reglamente, jeigu tenkinamos visos 57 arba 60 straipsnyje nustatytos sąlygos;

58) subjektas – bandymo realiomis sąlygomis tikslu – fizinis asmuo, dalyvaujantis bandyme realiomis sąlygomis;

59) informuoto asmens sutikimas – laisva valia pateiktas, konkretus, vienareikšmiškas ir savanoriškas subjekto noro dalyvauti konkrečiame bandyme realiomis sąlygomis pareiškimas po to, kai jis buvo informuotas apie visus bandymo aspektus, aktualius subjekto sprendimui dalyvauti;

60) sintetinė sankaita – DI generuojamas arba atlikus manipuliacijas gaunamas į realius asmenis, objektus, vietas ar kitus dalykus ar įvykius labai panašus judamo ar nejudamo vaizdo arba garso turinys, kurį asmuo gali klaidingai palaikyti autentišku ar tikru;

61) plačiai paplitęs pažeidimas – asmenų interesų apsaugos Sąjungos teisės aktams prieštaraujantis veiksmas ar neveikimas:

a) kuriuo buvo padaryta žala arba gali būti padaryta žala kolektyviniams interesams asmenų, gyvenančių bent dviejose kitose valstybėse narėse nei ta, kurioje:

i) tas veiksmas ar neveikimas buvo inicijuotas ar įvyko;

ii) fiziškai yra arba yra įsisteigęs atitinkamas tiekėjas arba, jei taikytina, jo įgaliotasis atstovas arba

iii) yra įsisteigęs diegėjas, kai pažeidimą padaro diegėjas;

b) kuris sukėlė, sukelia arba gali sukelti žalą kolektyviniams asmenų interesams, pasižymi bendrais bruožais, įskaitant tą pačią neteisėtą veiką ar to paties intereso pažeidimą, ir vyksta vienu metu, jį vykdant tam pačiam veiklos vykdytojui, bent trijose valstybėse narėse;

62) ypatingos svarbos infrastruktūra – ypatingos svarbos infrastruktūra, kaip apibrėžta Direktyvos (ES) 2022/2557 2 straipsnio 4 punkte;

63) bendrosios paskirties DI modelis – DI modelis, įskaitant atvejus, kai toks DI modelis yra išmokomas pasitelkiant didelį duomenų kiekį taikant didelio masto savipriežiūrą, kuris yra itin bendro pobūdžio ir gali veiksmingai atlikti įvairias skirtingas užduotis, neatsižvelgiant į tai, kaip tas modelis yra pateikiamas rinkai, ir kuris gali būti integruotas į įvairias tolesnės grandies sistemas ar panaudojimo būdus, išskyrus DI modelius, kurie naudojami mokslinių tyrimų, plėtros ar prototipų kūrimo veikloje prieš tai, kai jie pateikiami į rinką;

64) didelio poveikio pajėgumai – pajėgumai, kurie atitinka arba viršija pažangiausiuose bendrosios paskirties DI modeliuose užfiksuotus pajėgumus;

65) sisteminė rizika – bendrosios paskirties DI modelių didelio poveikio pajėgumams būdinga rizika, daranti reikšmingą poveikį Sąjungos rinkai dėl jų paplitimo arba dėl faktinių ar pagrįstai numatomų neigiamų pasekmių visuomenės sveikatai, saugai, visuomenės saugumui, pagrindinėms teisėms arba visai visuomenei, ir galinti dideliu mastu paplisti visoje vertės grandinėje;

66) bendrosios paskirties DI sistema – DI sistema, kuri yra grindžiama bendrosios paskirties DI modeliu ir kurią galima naudoti įvairiais tikslais – tiek naudoti tiesiogiai, tiek integruoti į kitas DI sistemas;

67) slankiojo kablelio operacija– matematinė operacija arba užduotis, kurioje operuojama slankiojo kablelio skaičiais; pastarieji yra realiųjų skaičių poaibis ir kompiuteriuose paprastai atvaizduojami pateikiant fiksuoto tikslumo sveikąjį skaičių ir jo eilę nurodantį fiksuoto pagrindo laipsnio rodiklį;

68) tolesnės grandies tiekėjas – DI sistemos (įskaitant bendrosios paskirties DI sistemą), į kurią integruotas DI modelis, tiekėjas, neatsižvelgiant į tai, ar DI modelis tiekiamas jo paties ir yra vertikaliai integruotas, ar tiekiamas kito subjekto remiantis sutartiniais santykiais.

4 straipsnis

Raštingumas DI srityje

DI sistemų tiekėjai ir diegėjai imasi priemonių kuo geriau užtikrinti savo darbuotojų ir kitų asmenų, dirbančių DI sistemų veikimo ir naudojimo jų vardu srityje, pakankamą raštingumo DI srityje lygį, atsižvelgdami į jų technines žinias, patirtį, išsilavinimą bei pasirengimą ir kontekstą, kuriame tos DI sistemos numatomos naudoti, ir atsižvelgdami į asmenis ar asmenų grupes, kurių atžvilgiu tos DI sistemos numatomos naudoti.

II skyrius
Draudžiama su DI susijusi praktika

5 straipsnis

Draudžiama su DI susijusi praktika

1. Draudžiama taikyti šią su DI susijusią praktiką:

   a) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kurioje pasitelkiami pasąmonę veikiantys metodai, kurių asmuo nesuvokia, arba tikslingai pasitelkiami manipuliavimo ar apgaulės metodai, siekiant iš esmės pakeisti asmens ar asmenų grupės elgesį arba tą elgesį iš esmės pakeičiant, pastebimai susilpninant jų gebėjimą priimti pagrįstą sprendimą, taip juos priverčiant priimti sprendimą, kurio jie kitu atveju nebūtų priėmę, taip, kad jis pats arba kitas asmuo, arba asmenų grupė patiria didelę žalą arba yra pagrįstai tikėtina, kad jis ar kitas asmuo ar asmenų grupė tokią žalą patirs;

   b) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kurioje išnaudojamas fizinio asmens ar konkrečios asmenų grupės pažeidžiamumas dėl jų amžiaus, negalios ar konkrečios socialinės ar ekonominės padėties, siekiant iš esmės pakeisti to asmens ar tai grupei priklausančio asmens elgesį arba to asmens elgesį iš esmės pakeičiant taip, kad jis pats arba kitas asmuo patiria didelę žalą arba yra pagrįstai tikėtina, kad jis ar kitas asmuo tokią žalą patirs;

c) pateikti rinkai, pradėti naudoti arba naudoti DI sistemas fiziniams asmenims ar asmenų grupėms tam tikru laikotarpiu vertinti ar klasifikuoti pagal jų socialinį elgesį arba žinomus, numanomus ar nuspėjamus asmeninius ar asmenybės bruožus, kai socialinis reitingas lemia vieną arba abu toliau išvardytus dalykus:

   i) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar asmenų grupėmis socialiniuose kontekstuose, kurie nėra susiję su kontekstais, kuriuose duomenys buvo iš pradžių sugeneruoti ar surinkti;

   ii) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar asmenų grupėmis, kuris yra nepagrįstas arba neproporcingas jų socialiniam elgesiui ar jo pavojingumui;

d) pateikti rinkai, pradėti naudoti šiuo konkrečiu tikslu arba naudoti DI sistemą fizinių asmenų rizikos vertinimams atlikti, siekiant įvertinti arba prognozuoti, kokia būtų rizika, kad fizinis asmuo įvykdys nusikalstamą veiką, remiantis tik fizinio asmens profiliavimu arba jo asmenybės bruožų ir savybių vertinimu; šis draudimas netaikomas DI sistemoms, naudojamoms žmogaus atliekamam asmens dalyvavimo nusikalstamoje veikloje vertinimui, kuris jau yra pagrįstas objektyviais ir patikrinamais faktais, tiesiogiai susijusiais su nusikalstama veikla;

e) pateikti rinkai, pradėti naudoti šiuo konkrečiu tikslu arba naudoti DI sistemas, kuriomis kuriamos arba išplečiamos veido atpažinimo duomenų bazės, netikslingai renkant veido atvaizdus iš interneto arba apsauginių vaizdo stebėjimo sistemų (AVSS) įrašų;

f) pateikti rinkai, pradėti naudoti šiuo konkrečiu tikslu arba naudoti DI sistemas fizinio asmens emocijoms darbo ir švietimo įstaigų srityse numanyti, išskyrus atvejus, kai DI sistemos naudojimą ketinama įdiegti arba pateikti rinkai dėl medicininių ar saugos priežasčių;

g) pateikti rinkai, pradėti naudoti šiuo konkrečiu tikslu arba naudoti biometrinio kategorizavimo sistemas, pagal kurias fiziniai asmenys individualiai skirstomi į kategorijas pagal jų biometrinius duomenis, kad būtų galima nustatyti ar numanyti jų rasę, politines pažiūras, narystę profesinėse sąjungose, religinius ar filosofinius įsitikinimus, lytinį gyvenimą ar seksualinę orientaciją; šis draudimas netaikomas teisėtai įgytų biometrinių duomenų rinkinių, pavyzdžiui, vaizdų, grindžiamų biometriniais duomenimis ar biometrinių duomenų kategorizavimu teisėsaugos srityje, ženklinimui ar filtravimui;

h) viešai prieinamose erdvėse teisėsaugos tikslais naudoti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas, nebent toks naudojimas tikrai būtinas ir tokiu mastu, kiek jis tikrai būtinas siekiant vieno iš šių tikslų:

   i) vykdyti tikslinę konkrečių pagrobimo, prekybos žmonėmis, seksualinio išnaudojimo aukų, taip pat dingusių asmenų paiešką;

   ii) užkirsti kelią konkrečiai, didelei ir tikrai grėsmei fizinių asmenų gyvybei ar fizinei saugai arba užkirsti kelią realiai ir esamai arba realiai ir numanomai teroristinio išpuolio grėsmei;

iii) lokalizuoti ar nustatyti asmenį, įtariamą įvykdžius nusikalstamą veiką, nusikalstamos veikos tyrimo, baudžiamojo persekiojimo ar baudžiamųjų sankcijų vykdymo už II priede nurodytas nusikalstamas veikas, už kurias atitinkamoje valstybėje narėje baudžiama laisvės atėmimo bausme arba įkalinimu, kurių ilgiausias terminas – bent ketveri metai, tikslais.

Pirmos pastraipos h punktu nedaromas poveikis Reglamento (ES) 2016/679 9 straipsniui dėl biometrinių duomenų tvarkymo kitais nei teisėsaugos tikslais.

2. Kai tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos viešai prieinamose erdvėse teisėsaugos tikslais naudojamos siekiant kurio nors iš 1 dalies pirmos pastraipos h punkte nurodytų tikslų, jos gali būti diegiamos tame punkte išdėstytais tikslais tik siekiant patvirtinti konkrečiai tiriamo asmens tapatybę, ir privalo atsižvelgti į šiuos aspektus:

a) padėties, dėl kurios gali tekti pasinaudoti tokia sistema, pobūdį, visų pirma žalos, kuri būtų padaryta, jei tokia sistema nebūtų naudojama, rimtumą, 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 viešai prieinamose erdvėse teisėsaugos tikslais naudojamos siekiant kurio nors iš šio straipsnio 1 dalies pirmos pastraipos h punkte nurodytų tikslų, atsižvelgiama į būtinas ir proporcingas su jų naudojimu, laikantis jų naudojimą leidžiančių nacionalinės teisės aktų, susijusias apsaugos priemones ir sąlygas, visų pirma laiko, geografinius ir su asmenimis susijusius apribojimus. Tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą viešai prieinamose erdvėse leidžiama naudoti tik tuo atveju, jei teisėsaugos institucija yra atlikusi poveikio pagrindinėms teisėms vertinimą, kaip numatyta 27 straipsnyje, ir yra užregistravusi sistemą ES duomenų bazėje pagal 49 straipsnį. Tačiau deramai pagrįstais skubos atvejais tokias sistemas galima pradėti naudoti be registracijos ES duomenų bazėje, jei tokia registracija užbaigiama nepagrįstai nedelsiant.

3. 1 dalies pirmos pastraipos h punkto ir 2 dalies tikslais tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą naudoti viešai prieinamose erdvėse teisėsaugos tikslais galima tik kiekvienu atveju gavus išankstinį valstybės narės, kurioje tą sistemą ketinama naudoti, teisminės institucijos arba nepriklausomos administracinės institucijos, kurios sprendimas yra privalomas, leidimą, išduotą pateikus pagrįstą prašymą ir laikantis 5 dalyje nurodytų išsamių nacionalinės teisės taisyklių. Tačiau deramai pagrįstais skubos atvejais tokią sistemą galima pradėti naudoti be leidimo su sąlyga, kad tokio leidimo paprašoma nepagrįstai nedelsiant, ne vėliau kaip per 24 valandas. Jei tokį leidimą atsisakoma išduoti, naudojimas nedelsiant nutraukiamas, o visi šio naudojimo atvejo duomenys, taip pat rezultatai ir išvediniai nedelsiant pašalinami ir ištrinami.

Kompetentinga teisminė institucija arba nepriklausoma administracinė institucija, kurios sprendimas yra privalomas, 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 pirmos pastraipos h punkte nustatytų tikslų, ir visų pirma neviršija to, kas tikrai būtina, kiek tai susiję su laiko trukme, geografine ir su asmenimis susijusia taikymo sritimi. Priimdama sprendimą dėl prašymo, ta institucija atsižvelgia į 2 dalyje nurodytus elementus. Negalima priimti jokio sprendimo, kuris sukeltų asmeniui nepalankų teisinį poveikį, remiantis vien tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos išvediniu.

4. Nedarant poveikio 3 daliai, apie kiekvieną tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos naudojimą viešai prieinamose erdvėse teisėsaugos tikslais pranešama atitinkamai rinkos priežiūros institucijai ir nacionalinei duomenų apsaugos institucijai pagal 5 dalyje nurodytas nacionalines taisykles. Pranešime pateikiama bent 6 dalyje nurodyta informacija, bet nepateikiama neskelbtinų operatyvinių duomenų.

5. Valstybė narė gali nuspręsti numatyti galimybę visiškai arba iš dalies leisti tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas naudoti viešai prieinamose erdvėse teisėsaugos tikslais, laikantis 1 dalies pirmos pastraipos h punkte ir 2 bei 3 dalyse nurodytų apribojimų ir sąlygų. Atitinkamos valstybės narės savo nacionalinėje teisėje nustato būtinas išsamias taisykles, kuriomis reglamentuojama 3 dalyje nurodytų leidimų prašymo, išdavimo, vykdymo ir su jais susijusios priežiūros ir ataskaitų teikimo tvarka. Tose taisyklėse taip pat nurodoma, kurių iš 1 dalies pirmos pastraipos h punkte išvardytų ir su kuria to h punkto iii papunktyje nurodyta nusikalstama veika susijusių tikslų siekiant kompetentingoms institucijoms gali būti leidžiama naudoti tas sistemas teisėsaugos tikslais. Valstybės narės apie tas taisykles praneša Komisijai ne vėliau kaip per 30 dienų nuo jų priėmimo. Valstybės narės, laikydamosi Sąjungos teisės, gali priimti griežtesnius teisės aktus dėl nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo.

6. Nacionalinės rinkos priežiūros institucijos ir valstybių narių nacionalinės duomenų apsaugos institucijos, kurioms pagal 4 dalį buvo pranešta apie tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimą viešai prieinamose erdvėse teisėsaugos tikslais, Komisijai teikia metines ataskaitas apie tokį naudojimą. Tuo tikslu Komisija pateikia valstybėms narėms ir nacionalinėms rinkos priežiūros ir duomenų apsaugos institucijoms šabloną, įskaitant informaciją apie kompetentingų teisminių institucijų arba nepriklausomos administracinės institucijos, kurios sprendimas yra privalomas, priimtų sprendimų dėl prašymų suteikti leidimą pagal 3 dalį skaičių ir jų rezultatus.

7. Komisija skelbia metines ataskaitas dėl tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo viešai prieinamose erdvėse teisėsaugos tikslais, remdamasi agreguotais duomenimis valstybėse narėse, pasitelkdama 6 dalyje nurodytas metines ataskaitas. Tose metinėse ataskaitose nepateikiama su susijusia teisėsaugos veikla susijusių neskelbtinų operatyvinių duomenų.

8. Šiuo straipsniu nedaromas poveikis draudimams, taikomiems tais atvejais, kai su DI susijusi praktika pažeidžia kitus Sąjungos teisės aktus.

III skyrius
Didelės rizikos DI sistemos

1 SKIRSNIS
DI SISTEMŲ PRISKYRIMAS PRIE DIDELĖS RIZIKOS SISTEMŲ

6 straipsnis

Didelės rizikos DI sistemų klasifikavimo 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 I priede išvardyti Sąjungos derinamieji teisės aktai, saugos komponentas arba DI sistema pati savaime yra toks gaminys;

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

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

3. Nukrypstant nuo 2 dalies, III priede nurodyta DI sistema nelaikoma didelės rizikos sistema, jei ji nekelia didelės rizikos, susijusios su žala fizinių asmenų sveikatai, saugai ar pagrindinėms teisėms ir, be kita ko, reikšmingai nedaro įtakos sprendimų priėmimo rezultatams.

Pirma pastraipa taikoma, jei tenkinama bet kuri iš šių sąlygų:

a) DI sistema skirta atlikti siaurą procedūrinę užduotį;

b) DI sistema skirta pagerinti veiklos, kurią pirmiau atliko žmogus, rezultatus;

c) DI sistema skirta nustatyti sprendimų priėmimo modelius arba nukrypimus nuo ankstesnių sprendimų priėmimo modelių ir nėra skirta pakeisti vertinimo, kurį pirmiau atliko žmogus, ar daryti jam įtaką be tinkamos žmogaus atliekamos peržiūros arba

d) DI sistema skirta atlikti vieną iš vertinimo, susijusio su III priede išvardytais naudojimo atvejų tikslais, parengiamųjų užduočių.

Nepaisant pirmos pastraipos, III priede nurodyta DI sistema visada laikoma didelės rizikos sistema, kai ji atlieka fizinių asmenų profiliavimą.

4. Tiekėjas, manantis, kad III priede nurodyta DI sistema nėra didelės rizikos sistema, dokumentuoja tos sistemos vertinimą prieš pateikdamas ją rinkai arba pradėdamas ją naudoti. Tokiam tiekėjui taikoma 49 straipsnio 2 dalyje nustatyta registravimo pareiga. Nacionalinėms kompetentingoms institucijoms paprašius tiekėjas pateikia vertinimo dokumentus.

5. Komisija, pasikonsultavusi su Europos dirbtinio intelekto valdyba (toliau – Valdyba) ir ne vėliau kaip … [18 mėnesių nuo šio reglamento įsigaliojimo dienos], pateikia gaires, kuriose nurodomas praktinis šio straipsnio įgyvendinimas pagal 96 straipsnį, taip pat išsamų DI sistemų, kurios yra didelės rizikos sistemos ir kurios nėra didelės rizikos sistemos, naudojimo atvejų praktinių pavyzdžių sąrašą.

6. Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti šio straipsnio 3 dalies antroje pastraipoje nustatytas sąlygas, papildant joje nustatytas sąlygas naujomis sąlygomis arba jas pakeičiant, jei yra konkrečių ir patikimų įrodymų, kad esama į III priedo taikymo sritį patenkančių DI sistemų, kurios nekelia didelės rizikos, susijusios su žala fizinių asmenų sveikatai, saugai ar pagrindinėms teisėms.

7. Komisija pagal 97 straipsnį priima deleguotuosius aktus, kad iš dalies pakeistų šio straipsnio 3 dalies antrą pastraipą išbraukdama bet kurią iš joje nustatytų sąlygų, jei yra konkrečių ir patikimų įrodymų, kad tai būtina siekiant išlaikyti sveikatos, saugos ir pagrindinių teisių apsaugos lygį, nustatytą šiuo reglamentu.

8. Joks 3 dalies antroje pastraipoje nustatytų sąlygų dalinis pakeitimas, priimtas pagal šio straipsnio 6 ir 7 dalis, negali sumažinti bendro sveikatos, saugos ir pagrindinių teisių apsaugos lygio, nustatyto šiuo reglamentu ir juo turi būti užtikrintas suderinamumas su deleguotaisiais aktais, priimtais pagal 7 straipsnio 1 dalį, ir atsižvelgiama į rinkos ir technologinę plėtrą.

7 straipsnis

III priedo daliniai pakeitimai

1. Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, kuriais iš dalies keičiamas III priedas įtraukiant arba pakeičiant didelės rizikos DI sistemų naudojimo atvejus, jei tenkinamos abi šios sąlygos:

   a) DI sistemos yra skirtos naudoti bet kurioje iš III priede išvardytų sričių;

   b) DI sistemos kelia riziką, susijusią su žala sveikatai ir saugai arba neigiamu poveikiu pagrindinėms teisėms, ir ta rizika yra lygiavertė III priede jau nurodytų didelės rizikos DI sistemų keliamai rizikai, susijusiai su žala ar neigiamu poveikiu, arba yra už ją didesnė.

2. Vertindama 1 dalies b punkte pateiktą sąlygą, Komisija atsižvelgia į šiuos kriterijus:

a) numatytąją DI sistemos paskirtį;

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

c) DI sistemos tvarkomų ir naudojamų duomenų pobūdį ir kiekį, visų pirma tai, ar tvarkomi specialių kategorijų asmens duomenys;

d) kokiu mastu DI sistema veikia autonomiškai ir galimybę žmogui panaikinti sprendimą ar rekomendacijas, dėl kurių gali būti padaryta žala;

e) 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 tikimybės, kaip matyti, pavyzdžiui, iš nacionalinėms kompetentingoms institucijoms pateiktų pranešimų arba dokumentais pagrįstų įtarimų, arba atitinkamai iš kitų pranešimų;

f) galimą tokios žalos arba tokio neigiamo poveikio mastą, visų pirma atsižvelgiant į jų dydį ir galėjimą paveikti daugelį asmenų arba padaryti neproporcingą poveikį tam tikrai asmenų grupei;

g) kiek asmenys, kuriems gali būti padaryta žala arba kurie gali nukentėti dėl neigiamo poveikio, priklauso nuo DI sistemos generuotų išvedinių, visų pirma todėl, kad dėl praktinių ar teisinių priežasčių tų išvedinių nėra pagrįstai įmanoma išvengti;

h) kokiu mastu egzistuoja galios disbalansas arba kiek asmenys, kuriems gali būti padaryta žala arba kurie gali nukentėti dėl neigiamo poveikio, yra pažeidžiami DI sistemos diegėjo požiūriu, visų pirma dėl statuso, įgaliojimų, žinių, ekonominių ar socialinių aplinkybių arba amžiaus;

i) kaip lengvai generuotus išvedinius, susijusius su DI sistema, galima ištaisyti ar atšaukti, atsižvelgiant į esamus techninius sprendimus tiems išvediniams ištaisyti ar atšaukti (išvediniai, darantys neigiamą poveikį sveikatai, saugai ar pagrindinėms teisėms, nėra laikomi lengvai ištaisomais ar atšaukiamais);

j) naudos asmenims, grupėms ar plačiajai visuomenei, gaunamos įdiegus DI sistemą, įskaitant galimą gaminių saugos pagerinimą, dydį ir tikimybę;

k) kiek esamuose 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.

3. Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, kuriais III priede pateikiamas sąrašas iš dalies pakeičiamas iš jo išbraukiant didelės rizikos DI sistemas, jei tenkinamos abi šios sąlygos:

a) atitinkama didelės rizikos DI sistema nebekelia jokios didelės rizikos pagrindinėms teisėms, sveikatai ar saugai, atsižvelgiant į 2 dalyje išvardytus kriterijus;

b) išbraukus tokią sistemą nesumažėja bendras sveikatos, saugos ir pagrindinių teisių apsaugos lygis pagal Sąjungos teisę.

2 SKIRSNIS

DIDELĖS RIZIKOS DI SISTEMOMS TAIKOMI REIKALAVIMAI

8 straipsnis

Atitiktis reikalavimams

1. Didelės rizikos DI sistemos turi atitikti šiame skirsnyje nustatytus reikalavimus, atsižvelgiant į jų numatytąją paskirtį ir visuotinai pripažintą pažangą DI ir su DI susijusių technologijų sektoriuose. Užtikrinant atitiktį tiems reikalavimams atsižvelgiama į 9 straipsnyje nurodytą rizikos valdymo sistemą.

2. Jei gaminyje yra DI sistema, kuriai taikomi šio reglamento reikalavimai ir I priedo A skirsnyje išvardytų Sąjungos derinamųjų teisės aktų reikalavimai, tiekėjai yra atsakingi už tai, kad būtų užtikrinta, jog jų gaminys visiškai atitiktų visus taikytinus reikalavimus, kurie yra nustatyti taikytinais Sąjungos derinamaisiais teisės aktais. Siekdami užtikrinti 1 dalyje nurodytų didelės rizikos DI sistemų atitiktį šiame skirsnyje nustatytiems reikalavimams ir kad būtų užtikrintas nuoseklumas, išvengta dubliavimosi ir kuo labiau sumažinta papildoma našta, tiekėjai gali atitinkamai pasirinkti, ar įtraukti reikalingus bandymų ir ataskaitų teikimo procesus, jų teikiamą su jų gaminiu susijusią informaciją ir dokumentus į jau esamus dokumentus ir procedūras, kurių reikalaujama pagal I priedo A skirsnyje išvardytus Sąjungos derinamuosius teisės aktus.

9 straipsnis

Rizikos valdymo sistema

1. Turi būti sukuriamos, įgyvendinamos, dokumentuojamos ir prižiūrimos didelės rizikos DI sistemų keliamos rizikos valdymo sistemos.

2. Rizikos valdymo sistema turi būti suprantama kaip visą didelės rizikos DI sistemos gyvavimo ciklą planuojamas ir vykstantis nuolatinis kartotinis procesas, kurį reikia reguliariai sistemingai peržiūrėti ir atnaujinti. Ją sudaro šie etapai:

   a) žinomos ir pagrįstai numatomos rizikos, kurią didelės rizikos DI sistema gali kelti sveikatai, saugai ar pagrindinėms teisėms, kai didelės rizikos DI sistema naudojama pagal numatytąją paskirtį, nustatymas ir analizė;

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

c) kitos galinčios kilti rizikos vertinimas remiantis duomenų, surinktų taikant 72 straipsnyje nurodytą priežiūros po pateikimo rinkai sistemą, analize;

d) tinkamų ir tikslinių rizikos valdymo priemonių, parengtų šalinti rizikai, nustatytai pagal a punktą, priėmimas.

3. Šiame straipsnyje nurodyta rizika susijusi tik su ta rizika, kurią galima pagrįstai sumažinti arba pašalinti didelės rizikos DI sistemos kūrimo ar projektavimo metu arba suteikiant tinkamą techninę informaciją.

4. Taikant 2 dalies d punkte nurodytas rizikos valdymo priemones deramai atsižvelgiama į poveikį ir galimą sąveiką, kuriuos lemia bendras šiame skirsnyje nustatytų reikalavimų taikymas, siekiant veiksmingiau iki minimumo sumažinti riziką, kartu užtikrinant tinkamą pusiausvyrą įgyvendinant priemones, skirtas tiems reikalavimams įvykdyti.

5. 2 dalies d punkte nurodytos rizikos valdymo priemonės turi būti tokios, kad su kiekvienu pavojumi susijusi atitinkama liekamoji rizika ir bendra didelės rizikos DI sistemų liekamoji rizika būtų laikomos priimtinomis.

Nustatant tinkamiausias rizikos valdymo priemones, užtikrinama, kad:

a) pagal 2 dalį nustatyta ir įvertinta rizika būtų šalinama arba mažinama tinkamomis didelės rizikos DI sistemos projektavimo ir kūrimo priemonėmis, kiek tai techniškai įmanoma;

b) jei rizikos pašalinti neįmanoma, kai tikslinga, į ją reaguojant būtų įgyvendinamos tinkamos rizikos mažinimo ir kontrolės priemonės;

c) būtų teikiama pagal 13 straipsnį reikalaujama informacija ir, kai tikslinga, diegėjams būtų rengiami mokymai.

Siekiant pašalinti arba sumažinti didelės rizikos DI sistemos naudojimo keliamą riziką, turi būti tinkamai atsižvelgiama į technines žinias, patirtį, išsilavinimą ir apmokymą, kurių tikimasi iš diegėjo, ir į numatomą kontekstą, kuriame sistema yra skirta naudoti.

6. Siekiant nustatyti tinkamiausias ir tikslines rizikos valdymo priemones, didelės rizikos DI sistemos turi būti išbandomos. Bandymais užtikrinama, kad didelės rizikos DI sistemos nuosekliai veiktų pagal numatytąją paskirtį ir atitiktų šiame skirsnyje nustatytus reikalavimus.

7. Bandymo procedūros gali apimti bandymą realiomis sąlygomis pagal 60 straipsnį.

8. Prireikus didelės rizikos DI sistemų bandymai atliekami atitinkamai bet kuriuo metu jų kūrimo proceso etapu ir bet kuriuo atveju prieš jas pateikiant rinkai arba pradedant naudoti. Bandymai atliekami taikant iš anksto nustatytą metriką ir tikimybines ribines vertes, atitinkančias didelės rizikos DI sistemos numatytąją paskirtį.

9. Įgyvendindami rizikos valdymo sistemą, kaip numatyta 1–7 dalyse, tiekėjai dėmesį skiria tam, ar, atsižvelgiant į didelės rizikos DI sistemos numatytąją paskirtį, tikėtina, kad ji darys neigiamą poveikį jaunesniems nei 18 metų asmenims ir, atitinkamai, kitoms pažeidžiamoms grupėms.

10. Didelės rizikos DI sistemų, kurioms reikalavimai dėl vidaus rizikos valdymo procesų taikomi pagal kitas atitinkamas Sąjungos teisės nuostatas, tiekėjų atveju 1–9 dalyse pateikti aspektai gali būti įtraukiami į pagal tą teisę nustatytas rizikos valdymo procedūras arba su jomis derinami.

10 straipsnis

Duomenys ir jų valdymas

1. Didelės rizikos DI sistemos, kuriose naudojami DI modelių mokymo pasitelkiant duomenis metodai, kuriamos remiantis mokymo, validavimo ir bandymo duomenų rinkiniais, atitinkančiais 2–5 dalyse nurodytus kokybės kriterijus, kai tokie duomenų rinkiniai naudojami.

2. Mokymo, validavimo ir bandymo duomenų rinkiniams taikoma duomenų valdymo ir tvarkymo praktika, atitinkanti numatytąją didelės rizikos DI sistemos paskirtį. Ta praktika visų pirma yra susijusi su:

a) atitinkamais projektavimo sprendimais;

b) duomenų rinkimo procesais ir duomenų kilme, o asmens duomenų atveju – pradiniu duomenų rinkimo tikslu;

c) atitinkamomis paruošiamosiomis duomenų tvarkymo operacijomis, pavyzdžiui, anotavimu, žymėjimu, valymu, naujinimu, papildymu ir agregavimu;

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

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

f) nagrinėjimu atsižvelgiant į galimą šališkumą, kuris gali turėti įtakos asmenų sveikatai ir saugai, turėti neigiamą poveikį pagrindinėms teisėms arba lemti pagal Sąjungos teisę draudžiamą diskriminaciją, ypač tais atvejais, kai duomenų išvediniai turi įtakos būsimų operacijų įvediniams;

g) tinkamomis priemonėmis pagal f punktą nustatytam galimam šališkumui aptikti, užkirsti jam kelią ir jį sumažinti;

h) atitinkamų duomenų spragų ar trūkumų, kurie trukdo užtikrinti, kad būtų laikomasi šio reglamento, ir galimų jų šalinimo būdų nustatymu.

3. Mokymo, validavimo ir bandymo duomenų rinkiniai turi būti tinkami, pakankamai reprezentatyvūs ir, kiek įmanoma, be klaidų ir išsamūs, atsižvelgiant į numatytąją paskirtį. Jie turi turėti tinkamas statistines savybes, įskaitant, kai taikytina, susijusias su asmenimis ar asmenų grupėmis, kurių atžvilgiu didelės rizikos DI sistema yra skirta naudoti. Šias duomenų rinkinių savybes gali turėti atskiri duomenų rinkiniai arba jų derinys.

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

5. Didelės rizikos DI sistemų tiekėjai, kiek tai tikrai būtina siekiant užtikrinti tų sistemų šališkumo aptikimą ir ištaisymą pagal šio straipsnio 2 dalies f ir g punktus, gali išimties tvarka tvarkyti specialių kategorijų asmens duomenis, taikydami tinkamas fizinių asmenų pagrindinių teisių ir laisvių apsaugos priemones. Be reglamentų (ES) 2016/679 ir (ES) 2018/1725 bei Direktyvos (ES) 2016/680 nuostatų, tokiam duomenų tvarkymui turi būti tenkinamos visos šios sąlygos:

   a) šališkumo nustatymo ir ištaisymo neįmanoma veiksmingai atlikti apdorojant kitus duomenis, įskaitant sintetinius arba anonimizuotus duomenis;

b) specialių kategorijų asmens duomenims taikomi pakartotinio asmens duomenų naudojimo techniniai apribojimai ir pažangiausios saugumo ir privatumo užtikrinimo priemonės, be kita ko, pseudoniminimas;

c) specialių kategorijų asmens duomenims taikomos priemonės, kuriomis užtikrinama, kad tvarkomi asmens duomenys būtų apsaugoti, saugomi taikant tinkamas apsaugos priemones, įskaitant griežtą prieigos kontrolę ir dokumentavimą, siekiant išvengti netinkamo naudojimo ir užtikrinti, kad prieigą prie tų asmens duomenų turėtų tik įgalioti asmenys, turintys atitinkamas konfidencialumo pareigas;

d) specialių kategorijų asmens duomenys negali būti perduodami, perkeliami ar kitaip prieinami kitoms šalims;

e) specialių kategorijų asmens duomenys ištrinami iškart po to, kai ištaisomas šališkumas, arba kai pasibaigia asmens duomenų saugojimo laikotarpis, atsižvelgiant į tai, kuri data yra ankstesnė;

f) duomenų tvarkymo veiklos įrašai pagal reglamentus (ES) 2016/679 ir (ES) 2018/1725 ir Direktyvą (ES) 2016/680 apima priežastis, dėl kurių specialių kategorijų asmens duomenų tvarkymas buvo tikrai būtinas šališkumui nustatyti ir ištaisyti ir dėl kurių to tikslo nebuvo galima pasiekti tvarkant kitus duomenis.

6. Kuriant didelės rizikos DI sistemas nenaudojant DI modelių mokymo metodų, 2–5 dalys taikomos tik bandymo duomenų rinkiniams.

11 straipsnis

Techniniai dokumentai

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

   Techniniai dokumentai parengiami taip, kad iš jų matytųsi, jog didelės rizikos DI sistema atitinka šiame skirsnyje nustatytus reikalavimus, ir nacionalinėms kompetentingoms institucijoms bei notifikuotosioms įstaigoms juose būtų aiškia ir išsamia forma pateikta informacija, būtina DI sistemos atitikčiai tiems reikalavimams įvertinti. Tuos dokumentus turi sudaryti bent IV priede nustatyti elementai. MVĮ, įskaitant startuolius, gali IV priede nurodytų techninių dokumentų elementus pateikti supaprastintai. Tuo tikslu Komisija parengia mažųjų ir labai mažų įmonių poreikiams skirtą supaprastintą techninių dokumentų formą. Jeigu MVĮ, įskaitant startuolius, nusprendžia IV priede reikalaujamą informaciją pateikti supaprastintai, ji naudoja šioje dalyje nurodytą formą. Notifikuotosios įstaigos priima šią formą atitikties vertinimo tikslais.

2. Kai rinkai pateikiama arba pradedama naudoti su gaminiu, kuriam taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, susijusi didelės rizikos DI sistema, parengiamas vienas bendras techninių dokumentų rinkinys, kuriame pateikiama visa 1 dalyje nustatyta informacija ir pagal tuos teisės aktus reikalaujama informacija.

3. Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti IV priedą, kad būtų užtikrinta, jog, atsižvelgiant į technikos pažangą, techniniuose dokumentuose būtų pateikta visa informacija, būtina sistemos atitikčiai šiame skirsnyje nustatytiems reikalavimams įvertinti.

12 straipsnis

Registravimas

1. Didelės rizikos DI sistemos turi būti tokios, kad per visą savo gyvavimo laiką būtų techniškai įmanoma automatiškai registruoti įvykius (žurnaluose).

2. Siekiant užtikrinti tam tikrą didelės rizikos DI sistemos veikimo atsekamumo lygį, kuris būtų tinkamas numatytajai sistemos paskirčiai, registravimo pajėgumais turi būti sudaryta galimybė registruoti įvykius, svarbius:

   a) situacijų, kuriose didelės rizikos DI sistema gali kelti riziką, kaip tai suprantama 79 straipsnio 1 dalyje, arba dėl kurių gali prireikti atlikti esminį pakeitimą, nustatymui;

   b) 72 straipsnyje nurodytos priežiūros po pateikimo rinkai palengvinimui ir

   c) 26 straipsnio 5 dalyje nurodytai didelės rizikos DI sistemų veikimo stebėsenai.

3. III priedo 1 punkto a papunktyje 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 diegėjams

1. Didelės rizikos DI sistemos projektuojamos ir kuriamos taip, kad būtų užtikrinama, kad jos veiktų pakankamai skaidriai, jog diegėjai galėtų tinkamai interpretuoti ir naudoti sistemos išvedinį. Turi būti užtikrintas atitinkamos rūšies ir lygio skaidrumas, kad tiekėjai ir diegėjai galėtų įvykdyti atitinkamas 3 skirsnyje nustatytas pareigas.

2. Su didelės rizikos DI sistemomis pateikiama tinkamo skaitmeninio arba kitokio formato naudojimo instrukcija, kurioje pateikiama glausta, išsami, teisinga ir aiški diegėjams svarbi, prieinama ir suprantama informacija.

3. Naudojimo instrukcija apima bent šią informaciją:

a) tiekėjo ir, kai taikytina, jo įgaliotojo atstovo tapatybę ir kontaktinius duomenis;

b) didelės rizikos DI sistemos veikimo efektyvumo ypatumus, pajėgumus ir ribotumus, įskaitant:

i) jos numatytąją paskirtį;

ii) 15 straipsnyje nurodytą didelės rizikos DI sistemos tikslumo, įskaitant tikslumo metriką, patvarumo 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 ar numatomas aplinkybes, susijusias su didelės rizikos DI sistemos naudojimu pagal numatytąją paskirtį arba pagrįstai numatomo netinkamo naudojimo sąlygomis, dėl kurio gali kilti 9 straipsnio 2 dalyje nurodyta rizika sveikatai ir saugai arba pagrindinėms teisėms;

iv) kai taikytina, didelės rizikos DI sistemos pajėgumus ir ypatumus teikti informaciją, kuri yra svarbi paaiškinant jos išvedinį;

v) kai tikslinga, jos veikimo efektyvumą, susijusį su konkrečiais asmenimis ar asmenų grupėmis, kurių atžvilgiu sistema yra skirta naudoti;

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

vii) kai taikytina, informaciją, kurią pasitelkdami diegėjai galėtų tinkamai interpretuoti ir naudoti didelės rizikos DI sistemos išvedinį;

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

d) 14 straipsnyje nurodytas žmogaus atliekamos priežiūros priemones, įskaitant technines priemones, įdiegtas tam, kad diegėjams būtų lengviau interpretuoti didelės rizikos DI sistemų išvedinius;

e) būtinus kompiuterinio apdorojimo ir aparatinės įrangos išteklius, numatomą didelės rizikos DI sistemos gyvavimo laiką ir visas techninės ir kitos priežiūros priemones, įskaitant jų dažnumą, būtinas tinkamam tos DI sistemos veikimui užtikrinti, įskaitant programinės įrangos atnaujinimą;

f) kai aktualu, į didelės rizikos DI sistemą įtrauktų mechanizmų, suteikiančių galimybę diegėjams tinkamai rinkti, saugoti ir interpretuoti žurnalus pagal 12 straipsnį, aprašymą.

14 straipsnis

Žmogaus atliekama priežiūra

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

2. Žmogaus atliekama 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 skirsnyje nustatytų reikalavimų taikymo.

3. Priežiūros priemonės turi būti proporcingos didelės rizikos DI sistemos keliamai rizikai, autonomijos lygiui ir naudojimo aplinkybėms ir turi būti užtikrinamos viena arba abiem šių rūšių 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 diegėjui įgyvendinti.

4. 1, 2 ir 3 dalių įgyvendinimo tikslu didelės rizikos DI sistema diegėjui tiekiama taip, kad fiziniai asmenys, kuriems pavesta atlikti tokią priežiūrą, galėtų, jei tai tinkama ir proporcinga:

   a) tinkamai suprasti atitinkamas didelės rizikos DI sistemos gebėjimus ir ribotumus ir sugebėti tinkamai stebėti jos veikimą, be kita ko, siekiant aptikti ir pašalinti anomalijas, sutrikimus ir netikėtą veikimą ;

b) nepamiršti galimos tendencijos automatiškai arba pernelyg pasikliauti didelės rizikos DI sistemos generuotu išvediniu (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 išvedinį, atsižvelgiant, pavyzdžiui, į turimas interpretavimo priemones bei metodus;

d) nuspręsti nenaudoti didelės rizikos DI sistemos tam tikroje situacijoje arba kitaip nepaisyti tos didelės rizikos DI sistemos išvedinio, jį panaikinti ar ištaisyti;

e) įsikišti į didelės rizikos DI sistemos veikimą arba sistemą išjungti „stop“ mygtuku ar panašiu būdu, leidžiančiu saugiai sustabdyti sistemą.

5. III priedo 1 punkto a papunktyje nurodytų didelės rizikos DI sistemų atveju šio straipsnio 3 dalyje nurodytomis priemonėmis turi būti užtikrinta, kad, be minėtų dalykų, diegėjas nesiimtų jokių veiksmų ir nepriimtų jokių sprendimų remdamasis sistemos pateiktu tapatybės nustatymo rezultatu, nebent tą rezultatą atskirai patikrino ir patvirtino bent du fiziniai asmenys, kurie turi reikiamą kompetenciją, kvalifikaciją ir įgaliojimus.

Reikalavimas dėl to, kad rezultatą būtų atskirai patikrinę bent du fiziniai asmenys, netaikomas didelės rizikos DI sistemoms, naudojamoms teisėsaugos, migracijos, sienų kontrolės ar prieglobsčio tikslais, kai pagal Sąjungos ar nacionalinę teisę šio reikalavimo taikymas laikomas neproporcingu.

15 straipsnis

Tikslumas, patvarumas ir kibernetinis saugumas

1. Didelės rizikos DI sistemos projektuojamos ir kuriamos taip, kad būtų pasiektas tinkamas tikslumo, patvarumo ir kibernetinio saugumo lygis ir kad tuo atžvilgiu jos veiktų nuosekliai per visą jų gyvavimo ciklą.

2. Siekdama atsižvelgti į techninius 1 dalyje nustatyto tinkamo tikslumo ir patvarumo lygio ir visos kitos susijusios veikimo efektyvumo metrikos matavimo aspektus, Komisija, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais ir organizacijomis, pavyzdžiui, metrologijos ir lyginamosios analizės institucijomis, atitinkamai skatina rengti lyginamuosius parametrus ir matavimo metodikas.

3. Didelės rizikos DI sistemų tikslumo lygiai ir atitinkama tikslumo metrika nurodomi pridedamoje naudojimo instrukcijoje.

4. Didelės rizikos DI sistemos turi būti kiek įmanoma 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. Šiuo atžvilgiu imamasi techninių ir organizacinių priemonių.

   Didelės rizikos DI sistemų patvarumą galima užtikrinti techniniais atsarginio dubliavimo sprendimais, kurie gali apimti atsarginio kopijavimo arba atsparumo gedimams planus.

Kuriant didelės rizikos DI sistemas, kurios, pateiktos rinkai arba pradėtos naudoti, toliau mokosi, turi būti užtikrinta, kad būtų pašalinta arba kuo labiau sumažinta išvedinių, kurie gali būti šališki ir daryti įtaką būsimų operacijų įvediniui (grįžtamojo ryšio grandinių), rizika ir kad būtų užtikrinta, kad bet kokių tokių grįžtamojo ryšio grandinių atžvilgiu būtų deramai taikomos tinkamos rizikos mažinimo priemonės.

5. Didelės rizikos DI sistemos turi būti atsparios leidimo neturinčių trečiųjų šalių bandymams pakeisti jų naudojimo paskirtį, išvedinius ar veikimo efektyvumą 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, aptikti, reaguoti ir rasti sprendimą dėl išpuolių, kuriais bandoma manipuliuoti mokymo duomenų rinkiniu (klaidingų duomenų įrašymo), arba iš anksto išmokytų komponentų, kurie naudojami mokyme (klaidingų modelių įrašymo), įvedinių, kurių paskirtis – priversti DI modelį padaryti klaidą (priešiškų pavyzdžių arba modelio vengimo), konfidencialumo pažeidimo išpuolių arba modelių trūkumų, ir juos kontroliuoti.

3 SKIRSNIS

DIDELĖS RIZIKOS DI SISTEMŲ TIEKĖJŲ BEI DIEGĖJŲ 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 2 skirsnyje nustatytus reikalavimus;

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

c) įdiegia 17 straipsnio reikalavimus atitinkančią kokybės valdymo sistemą;

d) saugo 18 straipsnyje nurodytus dokumentus;

e) saugo savo didelės rizikos DI sistemų automatiškai generuojamus žurnalus, jei tik tie žurnalai yra jų žinioje, kaip nurodyta 19 straipsnyje;

f) užtikrina, kad prieš pateikiant rinkai arba pradedant naudoti didelės rizikos DI sistemą būtų atliekama atitinkama jos atitikties vertinimo procedūra, kaip nurodyta 43 straipsnyje;

g) parengia ES atitikties deklaraciją pagal 47 straipsnį;

h) siekdami parodyti, kad jų didelės rizikos DI sistemos atitinka šio reglamento reikalavimus, pagal 48 straipsnį jas paženklina CE ženklu arba, jei to padaryti neįmanoma, paženklina jos pakuotę arba prie jos pridedamus dokumentus;

i) vykdo 49 straipsnio 1 dalyje nurodytas registravimo pareigas;

j) imasi būtinų taisomųjų veiksmų ir teikia informaciją, kaip reikalaujama 20 straipsnyje;

k) nacionalinės kompetentingos institucijos pagrįstu prašymu įrodo, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus;

l) užtikrina, kad didelės rizikos DI sistema atitiktų prieinamumo reikalavimus pagal direktyvas (ES) 2016/2102 ir (ES) 2019/882.

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 raštiškuose politikos, procedūrų ir nurodymų dokumentuose ir apima bent šiuos aspektus:

   a) atitikties reguliavimo normoms 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, atliekant jos kokybės patikrinimą ir vykdant su ja susijusią kokybės užtikrinimo veiklą;

d) tikrinimo, bandymo ir validavimo procedūras, atliktinas prieš kuriant didelės rizikos DI sistemą, jos kūrimo metu ir ją sukūrus, ir kokiu dažnumu jos turi būti atliekamos;

e) taikytinas technines specifikacijas, įskaitant standartus, ir, jei atitinkami darnieji standartai taikomi ne visa apimtimi arba apima ne visus atitinkamus 2 skirsnyje nustatytus reikalavimus, priemones, naudotinas siekiant užtikrinti, kad didelės rizikos DI sistema atitiktų tuos reikalavimus;

f) duomenų tvarkymo sistemas ir procedūras, įskaitant duomenų gavimo, duomenų rinkimo, duomenų analizės, duomenų žymėjimo, duomenų laikymo, duomenų filtravimo, duomenų gavybos, duomenų agregavimo, duomenų saugojimo ir bet kokią kitą su duomenimis susijusią operaciją, 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 72 straipsnį;

i) pranešimo apie rimtą incidentą pagal 73 straipsnį procedūras;

j) ryšių su nacionalinėmis kompetentingomis institucijomis, kitomis atitinkamomis institucijomis, įskaitant tas, kurios teikia arba palaiko 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. Bet kuriuo atveju tiekėjai turi laikytis tokio kruopštumo ir apsaugos lygio, kokio reikia, kad būtų užtikrinta jų didelės rizikos DI sistemų atitiktis šiam reglamentui.

3. Didelės rizikos DI sistemų tiekėjai, kuriems pagal atitinkamą sektorių Sąjungos teisę taikomos pareigos dėl kokybės valdymo sistemų ar lygiaverčių funkcijų, gali įtraukti 1 dalyje išdėstytus aspektus į pagal tą teisę nustatytas rizikos valdymo sistemas.

4. Kalbant apie tiekėjus, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi su vidaus valdymu, tvarka ar procesais susiję reikalavimai, pareiga įdiegti kokybės valdymo sistemą, išskyrus šio straipsnio 1 dalies g, h ir i punktuose nustatytas nuostatas, laikoma įvykdyta, jei laikomasi atitinkamuose Sąjungos finansinių paslaugų teisės aktuose nustatytų taisyklių dėl vidaus valdymo, tvarkos ar procesų. Tuo tikslu atsižvelgiama į visus 40 straipsnyje nurodytus darniuosius standartus.

18 straipsnis

Dokumentų saugojimas

1. Tiekėjas 10 metų po didelės rizikos 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) kai taikytina, su notifikuotųjų įstaigų patvirtintais pakeitimais susijusius dokumentus;

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

e) 47 straipsnyje nurodytą ES atitikties deklaraciją.

2. Kiekviena valstybė narė nustato sąlygas, kuriomis nacionalinės kompetentingos institucijos gali 1 dalyje nurodytu laikotarpiu susipažinti su toje dalyje nurodytais dokumentais tais atvejais, kai jos teritorijoje įsisteigęs tiekėjas arba jo įgaliotasis atstovas bankrutuoja arba nutraukia savo veiklą nepasibaigus tam laikotarpiui.

3. Tiekėjai, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi su jų vidaus valdymu, tvarka ar procesais susiję reikalavimai, techninius dokumentus tvarko kaip dalį dokumentų, saugomų pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus.

19 straipsnis

Automatiškai generuojami žurnalai

1. Didelės rizikos DI sistemų diegėjai saugo jų didelės rizikos DI sistemų automatiškai generuojamus 12 straipsnio 1 dalyje nurodytus žurnalus, jei tik tokie žurnalai yra jų žinioje. Nedarant poveikio taikytinai Sąjungos ar nacionalinei teisei, žurnalai saugomi laikotarpį, kuris yra tinkamas atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį, ir ne trumpiau kaip šešis mėnesius, nebent taikytinoje Sąjungos ar nacionalinėje teisėje, visų pirma Sąjungos teisėje dėl asmens duomenų apsaugos, numatyta kitaip.

2. Tiekėjai, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi su vidaus valdymu, tvarka ar procesais susiję reikalavimai, jų didelės rizikos DI sistemų automatiškai generuojamus žurnalus tvarko kaip dalį dokumentų, saugomų pagal atitinkamus finansinių paslaugų teisės aktus.

20 straipsnis

Taisomieji veiksmai ir pareiga informuoti

1. 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, reikalingų siekiant atitinkamai užtikrinti tos sistemos atitiktį, ją pašalinti iš rinkos, ją išjungti arba atšaukti. Jie apie tai informuoja atitinkamos didelės rizikos DI sistemos platintojus ir, kai taikytina, diegėjus, įgaliotuosius atstovus bei importuotojus.

2. Jei didelės rizikos DI sistema kelia riziką, kaip tai suprantama 79 straipsnio 1 dalyje, ir tiekėjas sužino apie tą riziką, jis nedelsdamas ištiria priežastis bendradarbiaudamas su apie riziką pranešusiu diegėju, kai taikytina, ir informuoja už tas didelės rizikos DI sistemas kompetentingas rinkos priežiūros institucijas ir, kai taikytina, notifikuotąją įstaigą, išdavusią tos didelės rizikos DI sistemos sertifikatą pagal 44 straipsnį, visų pirma apie neatitikties pobūdį ir atitinkamus taisomuosius veiksmus, kurių buvo imtasi.

21 straipsnis

Bendradarbiavimas su kompetentingomis institucijomis

1. Gavę kompetentingos institucijos pagrįstą prašymą, didelės rizikos DI sistemų tiekėjai tai institucijai jai lengvai suprantama kalba, viena iš oficialiųjų Sąjungos institucijų kalbų, kurią nurodo atitinkama valstybė narė, pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus.

2. Gavę pagrįstą kompetentingos institucijos prašymą, tiekėjai prašymą pateikusiai kompetentingai institucijai taip pat atitinkamai suteikia prieigą prie 12 straipsnio 1 dalyje nurodytų automatiškai generuojamų didelės rizikos DI sistemos žurnalų, jei tokie žurnalai yra jų žinioje.

3. Visa kompetentingos institucijos pagal šį straipsnį gauta informacija tvarkoma laikantis 78 straipsnyje nustatytų konfidencialumo pareigų.

22 straipsnis

Didelės rizikos DI sistemų tiekėjų įgaliotieji atstovai

1. Prieš pateikdami savo didelės rizikos DI sistemas Sąjungos rinkai, trečiosiose valstybėse įsisteigę tiekėjai rašytiniu įgaliojimu paskiria Sąjungoje įsisteigusį įgaliotąjį atstovą.

2. Tiekėjas paveda įgaliotajam atstovui atlikti tiekėjo suteiktame įgaliojime nurodytas užduotis.

3. Įgaliotasis atstovas atlieka tiekėjo suteiktame įgaliojime nurodytas užduotis. Gavęs prašymą, jis pateikia rinkos priežiūros institucijoms įgaliojimo kopiją viena iš oficialiųjų Sąjungos institucijų kalbų, kurią nurodo kompetentinga institucija. Šio reglamento tikslais įgaliojimu įgaliotajam atstovui suteikiama teisė atlikti šias užduotis:

a) patikrinti, ar parengti 47 straipsnyje nurodyta ES atitikties deklaracija ir 11 straipsnyje nurodyti techniniai dokumentai ir ar tiekėjas atliko tinkamą atitikties vertinimo procedūrą;

b) 10 metų po didelės rizikos DI sistemos pateikimo rinkai arba pradėjimo naudoti dienos saugoti tiekėjo, kuris yra paskyręs įgaliotąjį atstovą, kontaktinius duomenis, 47 straipsnyje nurodytos ES atitikties deklaracijos kopiją, techninius dokumentus, ir, jei taikytina, notifikuotosios įstaigos išduotą sertifikatą, kad juos galėtų patikrinti kompetentingos institucijos arba 74 straipsnio 10 dalyje nurodytos nacionalinės institucijos ar įstaigos;

c) gavus pagrįstą prašymą, pateikti kompetentingai institucijai visą informaciją ir dokumentus, įskaitant nurodytuosius šios pastraipos b punkte, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus, be kita ko, suteikti galimybę susipažinti su didelės rizikos DI sistemos automatiškai generuojamais 12 straipsnio 1 dalyje nurodytais žurnalais, jei tik tokie žurnalai yra tiekėjo žinioje ;

d) gavus pagrįstą prašymą, bendradarbiauti su kompetentingomis institucijomis įgyvendinant veiksmus, kurių pastarosios imasi didelės rizikos DI sistemos atžvilgiu, visų pirma siekdamos sumažinti ir sušvelninti didelės rizikos DI sistemų keliamą riziką;

e) kai taikytina, laikytis 49 straipsnio 1 dalyje nustatytų pareigų užregistruoti sistemą arba, jei ją užregistruoja pats tiekėjas, užtikrinti, kad VIII priedo A skirsnio 3 punkte pateikta informacija būtų teisinga.

Dėl visų aspektų, susijusių su šio reglamento laikymosi užtikrinimu, pagal įgaliojimą į įgaliotąjį atstovą, be tiekėjo arba vietoj jo, kreipiasi kompetentingos institucijos.

4. Įgaliotasis atstovas nutraukia įgaliojimą, jei mano arba turi pagrindo manyti, kad tiekėjo veikla prieštarauja pagal šį reglamentą nustatytoms jo pareigoms. Tokiu atveju jis nedelsdamas informuoja atitinkamą rinkos priežiūros instituciją, taip pat, kai taikytina, atitinkamą notifikuotąją įstaigą, apie įgaliojimo panaikinimą ir jo priežastis.

23 straipsnis

Importuotojų pareigos

1. Prieš pateikdami rinkai didelės rizikos DI sistemą, importuotojai užtikrina, kad sistema atitiktų šį reglamentą, patikrindami, kad:

a) didelės rizikos DI sistemos tiekėjas būtų atlikęs atitinkamą 43 straipsnyje nurodytą atitikties vertinimo procedūrą;

b) tiekėjas būtų pagal 11 straipsnį ir IV priedą parengęs techninius dokumentus;

c) sistema būtų paženklinta reikiamu CE ženklu ir kartu su ja būtų pateikiamos 47 straipsnyje nurodyta ES atitikties deklaracija ir naudojimo instrukcija;

d) tiekėjas būtų paskyręs įgaliotąjį atstovą pagal 22 straipsnio 1 dalį.

2. Jei importuotojas turi pakankamą priežastį manyti, kad didelės rizikos DI sistema neatitinka šio reglamento reikalavimų, yra suklastota arba su ja pateikiami suklastoti dokumentai, jis nepateikia tos sistemos rinkai tol, kol neužtikrinama jos atitiktis. Jei didelės rizikos sistema kelia riziką, kaip tai suprantama 79 straipsnio 1 dalyje, importuotojas apie tai informuoja DI sistemos tiekėją, įgaliotuosius atstovus ir rinkos priežiūros institucijas.

3. Importuotojai ant didelės rizikos DI sistemos ir, kai taikytina, 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, kai taikytina, nepakenktų jos atitikčiai 2 skirsnyje nustatytiems reikalavimams.

5. Importuotojai 10 metų po didelės rizikos DI sistemos pateikimo rinkai arba pradėjimo naudoti dienos saugo notifikuotosios įstaigos išduoto sertifikato, kai taikytina, naudojimo instrukcijos ir 47 straipsnyje nurodyta ES atitikties deklaracijos kopiją.

6. Gavę pagrįstą prašymą importuotojai atitinkamoms kompetentingoms institucijoms joms lengvai suprantama kalba pateikia visą informaciją ir dokumentus, įskaitant nurodytuosius 5 dalyje, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus. Šiuo tikslu jie taip pat užtikrina, kad tos institucijos galėtų susipažinti su techniniais dokumentais.

7. Importuotojai bendradarbiauja su atitinkamomis kompetentingomis institucijomis joms imantis bet kurių veiksmų dėl importuotojų rinkai pateiktos didelės rizikos DI sistemos, visų pirma siekiant sumažinti arba sušvelninti jos keliamą riziką.

24 straipsnis

Platintojų pareigos

1. Prieš tiekdami didelės rizikos DI sistemą rinkai, platintojai patikrina, ar ji pažymėta reikiamu CE ženklu, ar kartu su ja pateikiama 47 straipsnyje nurodyta ES atitikties deklaracijos kopija ir naudojimo instrukcija ir ar tos sistemos tiekėjas ir importuotojas, jei taikytina, įvykdė savo atitinkamas 16 straipsnio b ir c punktuose ir 23 straipsnio 3 dalyje nustatytas pareigas.

2. Jei platintojas, remdamasis turima informacija, mano arba turi pagrindo manyti, kad didelės rizikos DI sistema neatitinka 2 skirsnyje nustatytų reikalavimų, jis netiekia tos sistemos rinkai tol, kol neužtikrinama jos atitiktis tiems reikalavimams. Be to, jei didelės rizikos DI sistema kelia riziką, kaip tai suprantama 79 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 2 skirsnyje nustatytiems reikalavimams.

4. Platintojas, kuris, remdamasis turima informacija, mano arba turi pagrindo manyti, kad rinkai jo tiekiama didelės rizikos DI sistema neatitinka 2 skirsnyje 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 tai suprantama 79 straipsnio 1 dalyje, platintojas nedelsdamas apie tai praneša sistemos tiekėjui arba importuotojui ir už atitinkamas didelės rizikos DI sistemas kompetentingoms institucijoms ir pateikia išsamią informaciją, visų pirma apie neatitiktį ir taisomuosius veiksmus, kurių imtasi.

5. Gavę pagrįstą atitinkamos kompetentingos institucijos prašymą, didelės rizikos DI sistemos platintojai jai pateikia visą informaciją ir dokumentus, susijusius su savo veiksmais pagal 1–4 dalis, kurie būtini siekiant įrodyti, kad ta sistema atitinka 2 skirsnyje nustatytus reikalavimus.

6. Platintojai bendradarbiauja su atitinkamomis kompetentingomis institucijomis joms imantis bet kurių veiksmų dėl rinkai platintojų pateiktos didelės rizikos DI sistemos, visų pirma siekiant sumažinti arba sušvelninti jos keliamą riziką.

25 straipsnis

DI vertės grandinės dalyvių atsakomybė

1. Šio reglamento tikslais platintojas, importuotojas, diegėjas ar kita trečioji šalis laikomi didelės rizikos DI sistemos tiekėjais ir turi vykdyti 16 straipsnyje nustatytas tiekėjo pareigas bet kuriomis iš šių aplinkybių:

   a) jei jie nurodo savo pavadinimą ar prekių ženklą ant rinkai jau pateiktos ar pradėtos naudoti didelės rizikos DI sistemos, nedarant poveikio sutartiniams susitarimams, kuriais nustatyta, kad pareigos paskirstomos kitaip;

   b) jei jie atlieka esminį didelės rizikos DI sistemos, kuri jau buvo pateikta rinkai arba jau buvo pradėta naudoti, pakeitimą taip, kad ji išlieka didelės rizikos DI sistema pagal 6 straipsnį;

c) jei jie pakeičia DI sistemos, įskaitant bendrosios paskirties DI sistemą, kuri nebuvo priskirta didelės rizikos DI sistemoms ir jau buvo pateikta rinkai arba pradėta naudoti, numatytąją paskirtį taip, kad atitinkama DI sistema tampa didelės rizikos DI sistema pagal 6 straipsnį.

2. Atsiradus bet kuriai iš 1 dalyje nurodytų aplinkybių, DI sistemą iš pradžių rinkai pateikęs arba pradėjęs naudoti tiekėjas nustojamas laikyti tos konkrečios DI sistemos tiekėju šio reglamento taikymo tikslais. Tas pirminis tiekėjas glaudžiai bendradarbiauja su naujais tiekėjais ir pateikia būtiną informaciją bei suteikia pagrįstai tikėtiną techninę prieigą ir kitą pagalbą, kurių reikia šiame reglamente nustatytoms pareigoms vykdyti, visų pirma kiek tai susiję su didelės rizikos DI sistemų atitikties vertinimo reikalavimų laikymusi. Ši dalis netaikoma tais atvejais, kai pirminis tiekėjas yra aiškiai nurodęs, kad jo DI sistema negali būti pakeista į didelės rizikos DI sistemą ir kad dėl šios priežasties jos atžvilgiu netaikoma pareiga perduoti dokumentus.

3. Didelės rizikos DI sistemų, kurios yra gaminių, kuriems taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, saugos komponentai, atveju didelės rizikos DI sistemos tiekėju laikomas gaminio gamintojas ir jam taikomos 16 straipsnyje numatytos pareigos, jei yra kuri nors iš šių aplinkybių:

a) didelės rizikos DI sistema pateikiama rinkai kartu su gaminiu, naudojant gaminio gamintojo pavadinimą ar prekių ženklą;

b) didelės rizikos DI sistema pradedama naudoti su gaminio gamintojo pavadinimu arba prekių ženklu po to, kai gaminys pateikiamas rinkai.

4. Didelės rizikos DI sistemos tiekėjas ir trečioji šalis, tiekianti DI sistemą, priemones, paslaugas, komponentus ar procesus, kurie naudojami didelės rizikos DI sistemoje arba yra į ją integruoti, raštu sudarytoje sutartyje išsamiai apibūdina būtiną informaciją, pajėgumus, techninę prieigą ir kitą pagalbą, grindžiamus visuotinai pripažintais pažangiausiais metodais, kad didelės rizikos DI sistemos tiekėjas galėtų visapusiškai laikytis šiame reglamente nustatytų pareigų. Ši dalis netaikoma trečiosioms šalims, pagal nemokamą ir atvirojo kodo licenciją teikiančioms viešai prieinamas priemones, paslaugas, procesus ar komponentus, išskyrus bendrosios paskirties DI modelius.

DI tarnyba gali parengti ir rekomenduoti neprivalomas pavyzdines sutarčių tarp didelės rizikos DI sistemų tiekėjų ir trečiųjų šalių, tiekiančių priemones, paslaugas, komponentus ar procesus, kurie naudojami didelės rizikos DI sistemoms arba yra į jas integruoti, sąlygas. Rengdama tas neprivalomas pavyzdines sąlygas, DI tarnyba atsižvelgia į galimus sutartinius reikalavimus, taikomus konkretiems sektoriams ar verslo atvejams. Neprivalomos sąlygos paskelbiamos ir turi būti nemokamai prieinamos lengvai naudojamu elektroniniu formatu.

5. 2 ir 3 dalimis nedaromas poveikis būtinybei laikytis intelektinės nuosavybės teisių, konfidencialios verslo informacijos ir komercinių paslapčių bei jas apsaugoti pagal Sąjungos ir nacionalinę teisę.

26 straipsnis

Didelės rizikos DI sistemų diegėjų pareigos

1. Didelės rizikos DI sistemų diegėjai imasi tinkamų techninių ir organizacinių priemonių užtikrinti, kad jie tokias sistemas naudotų laikydamiesi kartu su jomis pateiktos naudojimo instrukcijos ir vadovaudamiesi 3–6 dalių nuostatomis.

2. Įgyvendinti žmogaus atliekamą priežiūrą diegėjai paveda fiziniams asmenims, kurie turi reikiamą kompetenciją, kvalifikaciją ir įgaliojimus tai daryti ir kuriems teikiama būtina parama.

3. 1 ir 2 dalyse nustatytos pareigos nedaro poveikio kitoms diegėjų pareigoms pagal Sąjungos ar nacionalinę teisę ir diegėjų laisvei savo nuožiūra organizuoti savo išteklius ir veiklą siekiant taikyti tiekėjo nurodytas žmogaus vykdomos priežiūros priemones.

4. Nedarant poveikio 1 ir 2 dalims, tiek, kiek diegėjas kontroliuoja įvesties duomenis, jis užtikrina, kad tie įvesties duomenys būtų aktualūs ir pakankamai reprezentatyvūs atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį.

5. Diegėjai stebi didelės rizikos DI sistemos veikimą, atsižvelgdami į jos naudojimo instrukciją ir, kai aktualu, informuoja tiekėjus pagal 72 straipsnį. Jei diegėjai turi pagrindo manyti, kad pagal naudojimo instrukciją naudojama DI didelės rizikos sistema gali kelti DI sistemos riziką, kaip tai suprantama 79 straipsnio 1 dalyje, jie nepagrįstai nedelsdami apie tai informuoja tiekėją arba platintoją ir atitinkamą rinkos priežiūros instituciją bei sustabdo tos sistemos naudojimą. Jei diegėjai nustato rimtą incidentą, jie taip pat nedelsdami apie tą incidentą pirma informuoja tiekėją, o tada importuotoją arba platintoją ir atitinkamas rinkos priežiūros institucijas. Jei diegėjas negali susisiekti su tiekėju, *mutatis mutandis* taikomas 73 straipsnis. Ši pareiga netaikoma DI sistemos diegėjų, kurie yra teisėsaugos institucijos, neskelbtiniems operatyviniams duomenims.

Jei diegėjai yra finansų įstaigos, kurioms taikomi su vidaus valdymu, tvarka ar procesais susiję reikalavimai pagal Sąjungos finansinių paslaugų teisės aktus, pirmoje pastraipoje nustatyta stebėsenos pareiga laikoma įvykdyta, jei laikomasi atitinkamuose finansinių paslaugų teisės aktuose nustatytų taisyklių dėl vidaus valdymo priemonių, procesų ir mechanizmų.

6. Didelės rizikos DI sistemos diegėjai saugo tos didelės rizikos DI sistemos automatiškai generuojamus žurnalus, jei tokie žurnalai yra jo žinioje , laikotarpį , kuris yra tinkamas atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį, ir ne trumpiau kaip šešis mėnesius, nebent taikytinuose Sąjungos ar nacionalinės teisės aktuose, visų pirma Sąjungos teisės aktuose dėl asmens duomenų apsaugos, numatyta kitaip.

Diegėjai, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi su vidaus valdymu, tvarka ar procesais susiję reikalavimai, žurnalus saugo kartu su dokumentais, saugomais pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus.

7. Prieš pradėdami naudoti arba prieš naudodami didelės rizikos DI sistemą darbo vietoje, diegėjai darbdaviai informuoja darbuotojų atstovus ir darbuotojus, kurie bus paveikti, kad jų atžvilgiu bus naudojama didelės rizikos DI sistema. Ši informacija teikiama, kai taikytina, laikantis taisyklių ir procedūrų pagal Sąjungos ir nacionalinės teisės aktus ir praktiką dėl darbuotojų ir jų atstovų informavimo.

8. Didelės rizikos DI sistemų diegėjai, kurie yra viešojo sektoriaus institucijos arba Sąjungos institucijos, įstaigos, organai ar agentūros, vykdo 49 straipsnyje nurodytas registravimo pareigas. Nustatę, kad didelės rizikos DI sistema, kurią jie ketina naudoti, nėra įregistruota 71 straipsnyje nurodytoje ES duomenų bazėje, tokie diegėjai tos sistemos nenaudoja ir apie tai informuoja tiekėją arba platintoją.

9. Kad įvykdytų Reglamento (ES) 2016/679 35 straipsnyje arba Direktyvos (ES) 2016/680 27 straipsnyje nustatytą pareigą atlikti poveikio duomenų apsaugai vertinimą, didelės rizikos DI sistemų diegėjai, kai taikytina, naudojasi pagal šio reglamento 13 straipsnį pateikta informacija.

10. Nedarant poveikio Direktyvai (ES) 2016/680, kai vykdomas tyrimas siekiant surasti konkretų asmenį, kuris įtariamas įvykdžius nusikalstamą veiką arba kuriam už tokią veiką yra paskelbtas apkaltinamasis nuosprendis, didelės rizikos DI sistemos, skirtos netikralaikiam nuotoliniam biometriniam tapatybės nustatymui, diegėjas *ex ante* arba nepagrįstai nedelsdamas ir ne vėliau kaip per 48 valandas paprašo teisminės institucijos arba administracinės institucijos, kurios sprendimai yra privalomi ir jiems taikoma teisminė peržiūra, leidimo naudoti tą sistemą, išskyrus atvejus, kai ji naudojama pradiniam galimo įtariamojo tapatybės nustatymui remiantis tiesiogiai su nusikalstama veika susijusiais objektyviais ir patikrinamais faktais. Kiekvienas naudojimas negali viršyti to, kas tikrai būtina konkrečiai nusikalstamai veikai ištirti.

Jei atsisakoma išduoti pagal pirmą pastraipą prašomą išduoti leidimą, su tuo prašomu leidimu susijęs netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemos naudojimas nedelsiant nutraukiamas, o asmens duomenys, susiję su didelės rizikos DI sistemos naudojimu, kuriam prašyta suteikti leidimą, ištrinami.

Tokia netikralaikiam nuotoliniam biometriniam tapatybės nustatymui skirta didelės rizikos DI sistema jokiu būdu teisėsaugos tikslais negali būti naudojama netikslingai, be jokios sąsajos su nusikalstama veika, baudžiamuoju procesu, tikra ir esama arba tikra ir numatoma nusikalstamos veikos grėsme, arba konkretaus dingusio asmens paieškai. Turi būti užtikrinama, kad remdamosi vien tokių netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų išvediniais teisėsaugos institucijos negalėtų priimti jokio sprendimo, kuris sukeltų asmeniui nepalankų teisinį poveikį.

Šia pastraipa nedaromas poveikis Reglamento (ES) 2016/679 9 straipsniui ir Direktyvos (ES) 2016/680 10 straipsniui biometrinių duomenų tvarkymo atžvilgiu.

Neatsižvelgiant į tikslą ar diegėją, kiekvienas tokios didelės rizikos DI sistemos panaudojimas yra užfiksuojamas atitinkamos policijos bylos dokumente ir su tokiu dokumentu leidžiama susipažinti atitinkamai rinkos priežiūros institucijai ir nacionalinei duomenų apsaugos institucijai, gavus pastarųjų prašymą, užtikrinant, kad nebūtų atskleidžiami su teisėsauga susiję neskelbtini operatyviniai duomenys. Šia pastraipa nedaromas poveikis įgaliojimams, kurie Direktyva (ES) 2016/680 yra suteikti priežiūros institucijoms.

Diegėjai atitinkamoms rinkos priežiūros institucijoms ir nacionalinėms duomenų apsaugos institucijoms teikia metines ataskaitas apie netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimą, bet neatskleidžia su teisėsauga susiję neskelbtini operatyviniai duomenys. Gali būti parengiama jungtinė ataskaita, apimanti daugiau nei vieną diegėjo sistemą.

Valstybės narės, laikydamosi Sąjungos teisės, gali priimti griežtesnius teisės aktus dėl netikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimo.

11. Nedarant poveikio šio reglamento 50 straipsniui, III priede nurodytų didelės rizikos DI sistemų diegėjai, kurie priima su fiziniais asmenimis susijusius sprendimus arba padeda juos priimti, informuoja fizinius asmenis, kad jų atžvilgiu naudojama didelės rizikos DI sistema. Didelės rizikos DI sistemas naudojant teisėsaugos tikslais, taikomas Direktyvos (ES) 2016/680 13 straipsnis.

12. Diegėjai bendradarbiauja su atitinkamomis kompetentingomis institucijomis dėl visų veiksmų, kurių tos institucijos imasi didelės rizikos DI sistemos atžvilgiu, kad įgyvendintų šį reglamentą.

27 straipsnis

Didelės rizikos DI sistemų poveikio pagrindinėms teisėms vertinimas

1. Prieš diegdami 6 straipsnio 2 dalyje nurodytą didelės rizikos DI sistemą, išskyrus didelės rizikos DI sistemas, skirtas naudoti III priedo 2 punkte nurodytoje srityje, diegėjai, kurie yra viešosios teisės reglamentuojamos įstaigos arba yra viešąsias paslaugas teikiantys privatūs subjektai, ir didelės rizikos DI sistemų, nurodytų III priedo 5 punkto b ir c papunkčiuose, diegėjai atlieka poveikio pagrindinėms teisėms, kurį gali turėti tokios sistemos naudojimas, vertinimą. Tuo tikslu diegėjai atlieka vertinimą, kurį sudaro šie elementai:

   a) diegėjo procesų, kuriuose didelės rizikos DI sistema bus naudojama pagal numatytąją paskirtį, aprašymas;

   b) aprašymas, kokį laikotarpį ir kaip dažnai kiekviena didelės rizikos DI sistema yra skirta naudoti;

c) fizinių asmenų kategorijos ir grupės, kurias gali paveikti jos naudojimas konkrečiame kontekste;

d) konkreti rizika, kad bus padaryta žala, kuri gali turėti poveikį pagal šios dalies c punktą nustatytoms fizinių asmenų kategorijoms ar asmenų grupėms, atsižvelgiant į tiekėjo pagal 13 straipsnį pateiktą informaciją;

e) žmogaus vykdomos priežiūros priemonių, kaip nurodyta naudojimo instrukcijoje, įgyvendinimo aprašymas;

f) priemonės, kurių reikia imtis, jei tokia rizika pasireiškia, įskaitant vidaus valdymo priemones ir skundų nagrinėjimo mechanizmus.

2. 1 dalyje nustatyta pareiga taikoma naudojant didelės rizikos DI sistemą pirmą kartą. Panašiais atvejais diegėjas gali remtis anksčiau atliktais poveikio pagrindinėms teisėms vertinimais arba esamais tiekėjo atliktais poveikio vertinimais. Jei diegėjui naudojant didelės rizikos DI sistemą jis mano, kad kuris nors iš 1 dalyje išvardytų elementų pasikeitė arba nebeatspindi padėties, diegėjas imasi būtinų veiksmų informacijai atnaujinti.

3. Atlikęs šio straipsnio 1 dalyje nurodytą vertinimą, diegėjas praneša rinkos priežiūros institucijai jo rezultatus, kartu su pranešimu pateikdamas užpildytą šio straipsnio 5 dalyje nurodytą šabloną. 46 straipsnio 1 dalyje nurodytu atveju diegėjai gali būti atleisti nuo tos pareigos pranešti.

4. Jei atlikus poveikio duomenų apsaugai vertinimą pagal Reglamento (ES) 2016/679 35 straipsnį arba Direktyvos (ES) 2016/680 27 straipsnį jau laikomasi kurios nors iš šiame straipsnyje nustatytų pareigų, tas poveikio duomenų apsaugai vertinimas papildomas šio straipsnio 1 dalyje nurodytu poveikio pagrindinėms teisėms vertinimu.

5. DI tarnyba parengia klausimyno šabloną, be kita ko, naudodama automatizuotą priemonę, kad diegėjams būtų sudarytos sąlygos paprasčiau vykdyti savo pareigas pagal šį straipsnį.

4 SKIRSNIS

NOTIFIKUOJANČIOSIOS INSTITUCIJOS IR NOTIFIKUOTOSIOS ĮSTAIGOS

28 straipsnis

Notifikuojančiosios institucijos

1. Kiekviena valstybė narė paskiria arba įsteigia bent vieną notifikuojančiąją instituciją, atsakingą už reikiamų atitikties vertinimo įstaigų vertinimo, paskyrimo, notifikavimo ir stebėjimo procedūrų nustatymą ir vykdymą. Tos procedūros rengiamos bendradarbiaujant visų valstybių narių notifikuojančiosioms institucijoms.

2. Valstybės narės gali nuspręsti, kad 1 dalyje nurodytą vertinimą ir stebėseną turi vykdyti nacionalinė akreditacijos įstaiga, kaip tai suprantama Reglamente (EB) Nr. 765/2008, laikantis to reglamento nuostatų.

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 pagal 78 straipsnį užtikrina informacijos, kurią jos gauna, konfidencialumą.

7. Notifikuojančiosiose institucijose turi būti pakankamai kompetentingų darbuotojų, galinčių tinkamai atlikti savo užduotis. Kompetentingi darbuotojai turi turėti reikiamų ekspertinių žinių, kai taikytina, kad galėtų vykdyti savo funkcijas tokiose srityse kaip informacinės technologijos, DI ir teisė, įskaitant pagrindinių teisių priežiūrą.

29 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 DI sistemų tipų, kuriuos 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 31 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 visus patvirtinamuosius dokumentus, būtinus jos atitikčiai 31 straipsnyje nustatytiems reikalavimams patikrinti, patvirtinti ir reguliariai stebėti.

4. 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. Notifikuotoji įstaiga atnaujina šio straipsnio 2 ir 3 dalyse nurodytus dokumentus kaskart, kai įvyksta svarbių pasikeitimų, kad už notifikuotąsias įstaigas atsakinga institucija galėtų stebėti ir tikrinti, ar toliau laikomasi visų 31 straipsnyje nustatytų reikalavimų.

30 straipsnis

Notifikavimo procedūra

1. Notifikuojančiosios institucijos gali notifikuoti tik tas atitikties vertinimo įstaigas, kurios atitinka 31 straipsnyje nustatytus reikalavimus.

2. Apie kiekvieną 1 dalyje nurodytą atitikties vertinimo įstaigą notifikuojančiosios institucijos praneša Komisijai ir kitoms valstybėms narėms, naudodamosi Komisijos sukurta ir administruojama elektronine notifikavimo priemone.

3. Šio straipsnio 2 dalyje nurodytame notifikavimo pranešime pateikiama išsami informacija apie atitikties vertinimo veiklą, atitikties vertinimo modulį ar modulius, atitinkamų DI sistemų tipus ir atitinkamą kompetencijos patvirtinimą. Jei notifikavimas nėra pagrįstas akreditacijos pažymėjimu, kaip nurodyta 29 straipsnio 2 dalyje, notifikuojančioji institucija Komisijai ir kitoms valstybėms narėms pateikia dokumentus, kuriais patvirtina atitikties vertinimo įstaigos kompetenciją ir tai, kad yra tvarka, kuria užtikrinama, kad ta įstaiga bus reguliariai stebima ir toliau atitiks 31 straipsnyje nustatytus reikalavimus.

4. Atitinkama atitikties vertinimo įstaiga notifikuotosios įstaigos veiklą gali vykdyti tik jeigu Komisija ar kitos valstybės narės nepareiškia prieštaravimų per dvi savaites nuo notifikuojančiosios įstaigos pateikto notifikavimo pranešimo gavimo, kai prie jo yra pridėtas 29 straipsnio 2 dalyje nurodytas akreditacijos pažymėjimas, arba per du mėnesius nuo notifikuojančiosios įstaigos pateikto notifikavimo pranešimo gavimo, kai prie jo yra pridėti 29 straipsnio 3 dalyje nurodyti patvirtinamieji dokumentai.

5. Jei pareiškiama prieštaravimų, Komisija nedelsdama pradeda konsultacijas su atitinkamomis valstybėmis narėmis ir atitikties vertinimo įstaiga. Atsižvelgdama į tai Komisija nusprendžia, ar leidimas yra pagrįstas. Savo sprendimą Komisija skiria atitinkamai valstybei narei ir atitinkamai atitikties vertinimo įstaigai.

31 straipsnis

Notifikuotosioms įstaigoms taikomi reikalavimai

1. Notifikuotoji įstaiga turi būti įsteigta pagal valstybės narės nacionalinę teisę ir turi turėti juridinio asmens statusą.

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

3. Notifikuotųjų įstaigų organizacinė struktūra, atsakomybės paskirstymas, atskaitomybės ryšiai ir veikla turi užtikrinti pasitikėjimą jų veiklos veiksmingumu ir jų vykdomos atitikties vertinimo veiklos 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 vertinamomis didelės rizikos DI sistemomis susijusių ekonominių interesų, taip pat nuo tiekėjo konkurentų. Šis draudimas netrukdo naudoti atitikties vertinimo įstaigos veiklai reikalingų įvertintų didelės rizikos DI sistemų arba naudoti tokių didelės rizikos DI sistemų asmeninėms reikmėms.

5. Nei atitikties vertinimo įstaiga, nei jos vyresnioji vadovybė, nei už atitikties vertinimo užduočių atlikimą atsakingi darbuotojai tiesiogiai nedalyvauja projektuojant, kuriant, parduodant ar naudojant didelės rizikos DI sistemas ir jie neatstovauja toje veikloje dalyvaujančioms šalims. Notifikuotosios įstaigos nesiima jokios veiklos, kuri gali kliudyti joms nepriklausomai priimti sprendimus ar sąžiningai atlikti atitikties vertinimo užduotis, dėl kurių joms suteiktas notifikuotosios įstaigos statusas. Tai visų pirma taikoma konsultavimo paslaugoms.

6. 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.

7. Notifikuotosios įstaigos taiko dokumentuotas procedūras, kuriomis užtikrinama, kad jų darbuotojai, komitetai, pavaldžiosios įstaigos, subrangovai, visos susijusios įstaigos ar išorės įstaigų darbuotojai pagal 78 straipsnį išlaikytų informacijos, kurią jie gauna vykdydami atitikties vertinimo veiklą, konfidencialumą, išskyrus atvejus, kai ją atskleisti reikalaujama pagal teisės aktus. Notifikuotųjų įstaigų darbuotojai visą informaciją, kurią jie gauna atlikdami savo užduotis pagal šį reglamentą, privalo saugoti kaip profesinę paslaptį – tai netaikoma tik valstybės narės, kurioje tos įstaigos vykdo savo veiklą, notifikuojančiųjų institucijų atžvilgiu.

8. Notifikuotosios įstaigos savo veiklą vykdo taikydamos procedūras, kuriomis deramai atsižvelgiama į tiekėjo dydį, sektorių, kuriame jis veikia, jo struktūrą ir atitinkamos DI sistemos sudėtingumo laipsnį.

9. Notifikuotosios įstaigos turi turėti tinkamą su jų vykdoma atitikties vertinimo veikla susijusį civilinės atsakomybės draudimą, nebent šią atsakomybę pagal nacionalinę teisę prisiima valstybė narė, kurioje jos yra įsteigtos, arba kai ta valstybė narė pati tiesiogiai atsako už atitikties vertinimą.

10. Notifikuotosios įstaigos turi būti pajėgios atlikti visas savo užduotis pagal šį reglamentą, 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.

11. Notifikuotosios įstaigos turi turėti pakankamai vidinės kompetencijos, kad galėtų veiksmingai įvertinti jų vardu užduotis atliekančių išorės subjektų darbą. Notifikuotoji įstaiga visada turi turėti pakankamai administracinių, techninių, teisės srities ir mokslinių darbuotojų, turinčių patirties ir žinių, susijusių su atitinkamais DI sistemų tipais, duomenimis ir duomenų kompiuterija ir su 2 skirsnyje nustatytais reikalavimais.

12. 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.

32 straipsnis

Atitikties notifikuotosioms įstaigoms taikomiems reikalavimams prezumpcija

Jei atitikties vertinimo įstaiga įrodo, kad atitinka kriterijus, nustatytus atitinkamuose darniuosiuose standartuose arba jų dalyse, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, preziumuojama, kad ji atitinka 31 straipsnyje nustatytus reikalavimus tiek, kiek juos apima taikomi darnieji standartai.

33 straipsnis

Notifikuotųjų įstaigų pavaldžiosios įstaigos ir subranga

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 31 straipsnyje nustatytus reikalavimus, ir apie tai informuoja notifikuojančiąją instituciją.

2. Notifikuotosios įstaigos prisiima visą atsakomybę už subrangovų ar pavaldžiųjų įstaigų atliekamas užduotis.

3. Pavesti veiklą vykdyti subrangovui ar pavaldžiajai įstaigai galima tik gavus tiekėjo sutikimą. Notifikuotosios įstaigos viešai skelbia savo pavaldžiųjų įstaigų sąrašą.

4. Aktualūs dokumentai, susiję su subrangovo ar pavaldžiosios įstaigos kvalifikacijos vertinimu ir jų pagal šį reglamentą atliktu darbu, saugomi penkerius metus nuo subrangos pabaigos dienos, kad notifikuojančioji institucija galėtų juos patikrinti.

34 straipsnis

Notifikuotųjų įstaigų veiklos pareigos

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

2. Vykdydamos savo veiklą notifikuotosios įstaigos vengia nereikalingos naštos tiekėjams ir deramai atsižvelgia į tiekėjo dydį, sektorių, kuriame jis vykdo veiklą, jo struktūrą ir į atitinkamos didelės rizikos DI sistemos sudėtingumo laipsnį, visų pirma, kad kuo labiau sumažintų administracinę naštą ir reikalavimų laikymosi išlaidas labai mažoms ir mažosioms įmonėms, kaip tai suprantama Rekomendacijoje 2003/361/EB. Tačiau notifikuotoji įstaiga laikosi tokio kruopštumo ir apsaugos lygio, kokio reikia, kad būtų užtikrinta didelės rizikos DI sistemos atitiktis šio reglamento reikalavimams.

3. Notifikuotosios įstaigos sudaro 28 straipsnyje nurodytai notifikuojančiajai institucijai sąlygas susipažinti su visais reikiamais dokumentais, įskaitant tiekėjo dokumentus, ir gavusios prašymą juos pateikia tai institucijai, kad ji galėtų vykdyti vertinimo, paskyrimo, notifikavimo ir stebėsenos veiklą ir kad būtų lengviau atlikti šiame skirsnyje aprašytą vertinimą.

35 straipsnis

Notifikuotųjų įstaigų identifikaciniai numeriai ir sąrašai

1. Komisija kiekvienai notifikuotajai įstaigai suteikia vieną identifikacinį numerį, net jei įstaiga yra notifikuota pagal daugiau nei vieną Sąjungos aktą.

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

36 straipsnis

Notifikavimo pakeitimai

1. Notifikuojančioji institucija, naudodamasi 30 straipsnio 2 dalyje nurodyta elektronine notifikavimo priemone, Komisijai ir kitoms valstybėms narėms praneša apie visus svarbius notifikuotosios įstaigos notifikavimo pakeitimus.

2. Notifikavimo aprėpties išplėtimui taikomos 29 ir 30 straipsniuose nustatytos procedūros.

   Jei notifikavimo pakeitimai nėra susiję su jo aprėpties išplėtimu, taikomos 3-9 dalyse nustatytos procedūros.

3. Kai notifikuotoji įstaiga nusprendžia nutraukti atitikties vertinimo veiklą, ji kuo greičiau, o planuojamo veiklos nutraukimo atveju – likus bent vieniems metams iki veiklos nutraukimo, apie tai informuoja notifikuojančiąją instituciją ir atitinkamus tiekėjus. Notifikuotosios įstaigos sertifikatai gali toliau galioti devynių mėnesių po jos veiklos nutraukimo laikotarpį su sąlyga, kad kita notifikuotoji įstaiga raštu yra patvirtinusi, kad ji prisiims atsakomybę už didelės rizikos DI sistemas, kurioms išduoti tie sertifikatai. Pastaroji notifikuotoji įstaiga iki to devynių mėnesių laikotarpio pabaigos užbaigia susijusių didelės rizikos DI sistemų visapusišką vertinimą, prieš išduodama naujus sertifikatus toms sistemoms. Jei notifikuotoji įstaiga savo veiklą nutraukia, notifikuojančioji institucija paskyrimą panaikina.

4. Jei notifikuojančioji institucija turi pakankamą pagrindą manyti, kad notifikuotoji įstaiga nebeatitinka 31 straipsnyje nustatytų reikalavimų arba nevykdo savo pareigų, notifikuojančioji 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 notifikuotoji įstaiga nebeatitinka 31 straipsnyje nustatytų reikalavimų arba nevykdo savo pareigų, ji atitinkamai apriboja, sustabdo arba panaikina paskyrimą atsižvelgdama į tų reikalavimų nebeatitikimo arba tų pareigų nevykdymo rimtumą. Ji nedelsdama apie tai informuoja Komisiją ir kitas valstybes nares.

5. Jei notifikuotosios įstaigos paskyrimas sustabdomas, apribojamas arba visai ar iš dalies panaikinamas, ji per 10 dienų apie tai informuoja atitinkamus tiekėjus.

6. Jei paskyrimas apribojamas, sustabdomas ar panaikinamas, notifikuojančioji institucija imasi tinkamų priemonių, kuriomis užtikrinama, kad atitinkamos notifikuotosios įstaigos bylos būtų saugomos ir su jomis galėtų susipažinti to prašančios kitų valstybių narių notifikuojančiosios institucijos ir rinkos priežiūros institucijos.

7. Paskyrimo apribojimo, sustabdymo arba panaikinimo atveju notifikuojančioji institucija:

   a) įvertina poveikį notifikuotosios įstaigos išduotiems sertifikatams;

   b) per tris mėnesius nuo pranešimo apie paskyrimo pakeitimus Komisijai ir kitoms valstybėms narėms pateikia savo išvadų ataskaitą;

c) reikalauja, kad notifikuotoji įstaiga per pagrįstą laikotarpį, kurį nustato institucija, sustabdytų arba panaikintų visus nepagrįstai išduotus sertifikatus, kad būtų užtikrinta rinkoje esančių didelės rizikos DI sistemų nuolatinė atitiktis;

d) informuoja Komisiją ir valstybes nares apie sertifikatus, kuriuos ji pareikalavo sustabdyti arba panaikinti;

e) pateikia valstybės narės, kurioje yra tiekėjo registruota buveinė, nacionalinėms kompetentingoms institucijoms visą svarbią informaciją apie sertifikatus, kuriuos ji pareikalavo sustabdyti arba panaikinti. Ta institucija prireikus imasi tinkamų priemonių, kad būtų išvengta galimos rizikos sveikatai, saugai ar pagrindinėms teisėms.

8. Išskyrus nepagrįstai išduotus sertifikatus, ir tais atvejais, kai paskyrimas buvo sustabdytas ar apribotas, sertifikatai toliau galioja esant vienai iš šių aplinkybių:

a) notifikuojančioji institucija per mėnesį nuo sustabdymo ar apribojimo yra patvirtinusi, kad nėra rizikos sveikatai, saugai ar pagrindinėms teisėms, susijusios su sertifikatais, kuriems turi įtakos tas sustabdymas arba apribojimas, ir notifikuojančioji institucija yra nustačiusi veiksmų sustabdymui ar apribojimui panaikinti tvarkaraštį arba

b) notifikuojančioji institucija yra patvirtinusi, kad sustabdymo ar apribojimo laikotarpiu su sustabdymu susiję sertifikatai nebus išduodami, iš dalies keičiami arba išduodami pakartotinai, ir nurodžiusi, ar notifikuotoji įstaiga yra pajėgi tęsti esamų išduotų sertifikatų stebėseną ir toliau būti už juos atsakinga sustabdymo arba apribojimo laikotarpiu. Jeigu notifikuojančioji institucija nustato, kad notifikuotoji įstaiga nėra pajėgi prižiūrėti galiojančių išduotų sertifikatų, sistemos, kuriai taikomas sertifikatas, tiekėjas per tris mėnesius nuo sustabdymo arba apribojimo pateikia valstybės narės, kurioje yra jo registruota buveinė, nacionalinėms kompetentingoms institucijoms rašytinį patvirtinimą, kad kita reikalavimus atitinkanti notifikuotoji įstaiga laikinai prisiima notifikuotosios įstaigos funkcijas, kad vykdytų sertifikatų stebėseną ir būtų atsakinga už juos sustabdymo arba apribojimo laikotarpiu.

9. Išskyrus nepagrįstai išduotus sertifikatus, ir tais atvejais, kai paskyrimas buvo panaikintas, sertifikatai toliau galioja devynis mėnesius šiomis aplinkybėmis:

a) valstybės narės, kurioje yra didelės rizikos DI sistemos, kuriai išduotas sertifikatas, tiekėjo registruota buveinė, nacionalinė kompetentinga institucija yra patvirtinusi, kad nėra su atitinkamomis didelės rizikos DI sistemomis susijusios rizikos sveikatai, saugai ar pagrindinėms teisėms, ir

b) kita notifikuotoji įstaiga yra raštu patvirtinusi, kad ji nedelsiant prisiims atsakomybę už šias DI sistemas ir užbaigs vertinimą per 12 mėnesių nuo paskyrimo panaikinimo dienos.

Pirmoje pastraipoje nurodytomis aplinkybėmis valstybės narės, kurioje yra sistemos, kuriai išduotas sertifikatas, tiekėjo registruota buveinė, nacionalinė kompetentinga institucija gali pratęsti laikinąjį sertifikatų galiojimą papildomiems trijų mėnesių laikotarpiams, kurie iš viso negali sudaryti ilgesnio kaip 12 mėnesių laikotarpio.

Nacionalinė kompetentingas institucija arba notifikuotoji įstaiga, prisiimanti notifikuotosios įstaigos, kurios paskyrimas yra pakeistas, funkcijas, apie tai nedelsdama praneša Komisijai, kitoms valstybėms narėms ir kitoms notifikuotosioms įstaigoms.

37 straipsnis

Notifikuotųjų įstaigų kompetencijos užginčijimas

1. Prireikus, Komisija ištiria visus atvejus, kuriais esama pagrindo abejoti notifikuotosios įstaigos kompetencija arba tuo, ar notifikuotoji įstaiga vis dar atitinka 31 straipsnyje nustatytus reikalavimus ir toliau vykdo jai taikytinas pareigas.

2. Pateikus prašymą notifikuojančioji institucija pateikia Komisijai visą aktualią informaciją, susijusią su atitinkamos notifikuotosios įstaigos notifikavimu ar kompetencijos išlaikymu.

3. Komisija užtikrina, kad visa neskelbtina informacija, gaunama atliekant šiame straipsnyje nurodytus tyrimus, būtų tvarkoma konfidencialiai pagal 78 straipsnį.

4. Jei Komisija nustato, kad notifikuotoji įstaiga neatitinka arba nebeatitinka jos notifikavimo reikalavimų, ji apie tai praneša notifikuojančiajai valstybei narei ir jos paprašo imtis būtinų taisomųjų priemonių, įskaitant, jei būtina, notifikavimo galiojimo sustabdymą ar panaikinimą. Jei valstybė narė nesiima būtinų taisomųjų priemonių, Komisija gali priimti įgyvendinimo aktą, kuriuo paskyrimas būtų sustabdytas, apribotas ar panaikintas. Tas įgyvendinimo aktas priimamas laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

38 straipsnis

Notifikuotųjų įstaigų veiklos koordinavimas

1. Komisija užtikrina, kad didelės rizikos DI sistemų atveju per sektoriaus notifikuotųjų įstaigų grupę būtų organizuojamas ir tinkamai vykdomas notifikuotųjų įstaigų, pagal šį reglamentą atliekančių atitikties vertinimo procedūras, veiklos koordinavimas ir jų bendradarbiavimas.

2. Kiekviena notifikuojančioji institucija užtikrina, kad jos notifikuotos įstaigos tiesiogiai arba per paskirtus atstovus dalyvautų 1 dalyje nurodytos grupės veikloje.

3. Komisija pasirūpina, kad notifikuojančiosios institucijos tarpusavyje keistųsi žiniomis ir geriausios praktikos pavyzdžiais.

39 straipsnis

Trečiųjų valstybių atitikties vertinimo įstaigos

Pagal trečiųjų valstybių, su kuriomis Sąjunga yra sudariusi susitarimus, teisę įsteigtoms atitikties vertinimo įstaigoms gali būti leidžiama vykdyti šiame reglamente nurodytą notifikuotųjų įstaigų veiklą, jeigu jos atitinka 31 straipsnyje nustatytus reikalavimus arba užtikrina lygiavertę atitiktį.

5 SKIRSNIS

STANDARTAI, ATITIKTIES VERTINIMAS, SERTIFIKATAI, REGISTRACIJA

40 straipsnis

Darnieji standartai ir standartizacijos leidiniai

1. Preziumuojama, kad didelės rizikos DI sistemos ir bendrosios paskirties DI modeliai, atitinkantys darniuosius standartus ar jų dalis, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje* pagal Reglamentą (ES) Nr. 1025/2012, atitinka šio skyriaus 2 skirsnyje nustatytus reikalavimus arba, jei taikytina, šio reglamento V skyriaus 2 ir 3 skirsniuose išdėstytus įpareigojimus, tokiu mastu, kokiu tie standartai apima tuos reikalavimus ar įpareigojimus.

2. Vadovaudamasi Reglamento (ES) Nr. 1025/2012 10 straipsniu Komisija nedelsdama pateikia standartizacijos prašymus, apimančius visus šio skyriaus 2 skirsnyje nustatytus reikalavimus ir, kai taikytina, standartizacijos prašymus, apimančius šio reglamento V skyriaus 2 ir 3 skirsniuose išdėstytas pareigas. Standartizacijos prašyme taip pat prašoma parengti leidinius, susijusius su ataskaitų teikimo ir dokumentavimo procesais, siekiant pagerinti DI sistemų išteklių naudojimo efektyvumą, pavyzdžiui, sumažinti didelės rizikos DI sistemų energijos ir kitų išteklių suvartojimą per jų gyvavimo ciklą, taip pat leidinius, susijusius su efektyviu energijos vartojimu grindžiamu bendrosios paskirties DI modelių kūrimu. Rengdama standartizacijos prašymą Komisija konsultuojasi su Valdyba ir atitinkamais suinteresuotaisiais subjektais, įskaitant patariamąjį forumą.

Pateikdama standartizacijos prašymą Europos standartizacijos organizacijoms Komisija nurodo, kad standartai turi būti aiškūs, tarpusavyje derėti, be kita ko, su įvairiuose sektoriuose parengtais standartais, skirtais gaminiams, kuriems taikomi I priede išvardyti esami Sąjungos derinamieji teisės aktai, ir kad jais turi būti siekiama užtikrinti, kad Sąjungoje rinkai pateikiamos arba pradedamos naudoti didelės rizikos DI sistemos ar bendrosios paskirties DI modeliai atitiktų atitinkamus šiame reglamente nustatytus reikalavimus ar pareigas.

Remdamasi Reglamento (ES) Nr. 1025/2012 24 straipsniu Komisija prašo Europos standartizacijos organizacijų pateikti įrodymų, jog dedamos visos pastangos, kad būtų pasiekti šios dalies pirmoje ir antroje pastraipose nurodyti tikslai.

3. Standartizacijos proceso dalyviai siekia skatinti investicijas ir inovacijas DI srityje, be kita ko, užtikrinant daugiau teisinio tikrumo, taip pat skatinti Sąjungos rinkos konkurencingumą bei augimą, padeda stiprinti pasaulinį bendradarbiavimą standartizacijos srityje ir rėmimąsi tais esamais tarptautiniais DI srities standartais, kurie atitinka Sąjungos vertybes, pagrindines teises ir interesus, ir stiprina įvairių suinteresuotųjų subjektų dalyvavimu grindžiamą valdymą, užtikrinant subalansuotą atstovavimą interesams ir veiksmingą visų atitinkamų suinteresuotųjų subjektų dalyvavimą, kaip numatyta Reglamento (ES) Nr. 1025/2012 5, 6 ir 7 straipsniuose.

41 straipsnis

Bendrosios specifikacijos

1. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomos šio skyriaus 2 skirsnyje išdėstytų reikalavimų arba, kai taikytina, V skyriaus 2 ir 3 skirsniuose išdėstytų pareigų bendrosios specifikacijos, jei yra tenkinamos šios sąlygos:

   a) Komisija pagal Reglamento (ES) Nr. 1025/2012 10 straipsnio 1 dalį yra paprašiusi vienos ar daugiau Europos standartizacijos organizacijų parengti šio skyriaus 2 skirsnyje išdėstytų reikalavimų arba atitinkamai V skyriaus 2 ir 3 skirsniuose išdėstytų pareigų darnųjį standartą, ir:

      i) nė viena Europos standartizacijos organizacija Komisijos prašymo nepriėmė arba

ii) darnieji standartai pagal tą prašymą nebuvo parengti iki termino, nustatyto pagal Reglamento (ES) Nr. 1025/2021 10 straipsnio 1 dalį, arba

iii) atitinkamuose darniuosiuose standartuose nepakankamai atsižvelgiama į pagrindinių teisių klausimus, arba

iv) darnieji standartai neatitinka prašymo ir

b) *Europos Sąjungos oficialiajame leidinyje* pagal Reglamentą (ES) Nr. 1025/2012 nebuvo paskelbtos nuorodos į darniuosius standartus, apimančius šio skyriaus 2 skirsnyje nurodytus reikalavimus arba atitinkamai V skyriaus 2 ir 3 skirsniuose nurodytas pareigas, ir tokios nuorodos per pagrįstą laikotarpį nenumatoma paskelbti.

Rengdama bendrąsias specifikacijas, Komisija konsultuojasi su 67 straipsnyje nurodytu patariamuoju forumu.

Šios dalies pirmoje pastraipoje nurodyti įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

2. Prieš rengdama įgyvendinimo akto projektą, Komisija informuoja Reglamento (ES) Nr. 1025/2021 22 straipsnyje nurodytą komitetą apie tai, kad, jos nuomone, šio straipsnio 1 dalyje nustatytos sąlygos yra tenkinamos.

3. Preziumuojama, kad 1 dalyje nurodytas bendrąsias specifikacijas arba tų specifikacijų dalis atitinkančios didelės rizikos DI sistemos ir bendrosios paskirties DI modeliai atitinkantys šio skyriaus 2 skirsnyje nustatytus reikalavimus arba atitinkamai V skyriaus 2 ir 3 skirsniuose nurodytas pareigas tiek, kiek tos bendrosios specifikacijos apima tuos reikalavimus ir tas pareigas.

4. Kai Europos standartizacijos organizacija priima darnųjį standartą ir Komisijai pasiūloma paskelbti jo nuorodą *Europos Sąjungos oficialiajame leidinyje*, Komisija įvertina darnųjį standartą pagal Reglamentą (ES) Nr. 1025/2012. Kai *Europos Sąjungos oficialiajame leidinyje* paskelbiama darniojo standarto nuoroda, Komisija panaikina 1 dalyje nurodytus įgyvendinimo aktus arba jų dalis, kurie apima tuos pačius kaip šio skyriaus 2 skirsnyje nustatytieji reikalavimus arba atitinkamai tas pačias V skyriaus 2 ir 3 skirsniuose išdėstytas pareigas.

5. Jei didelės rizikos DI sistemų ar bendrosios paskirties DI modelių tiekėjai nesilaiko 1 dalyje nurodytų bendrųjų specifikacijų, jie tinkamai pagrindžia, kad yra įdiegę techninius sprendimus, užtikrinančius bent lygiavertę atitiktį šio skyriaus 2 skirsnyje išdėstytiems reikalavimams arba atitinkamai laikosi V skyriaus 2 ir 3 skirsniuose išdėstytų pareigų.

6. Jei valstybė narė mano, kad bendroji specifikacija ne visiškai atitinka šio skyriaus 2 skirsnyje išdėstytus reikalavimus arba, kai taikoma, ne visiškai laikosi V skyriaus 2 ir 3 skirsniuose išdėstytų pareigų, ji apie tai informuoja Komisiją, pateikdama išsamų paaiškinimą. Komisija įvertina tą informaciją ir, jei tinkama, iš dalies pakeičia įgyvendinimo aktą, kuriuo nustatyta atitinkama bendroji specifikacija.

42 straipsnis

Atitikties tam tikriems reikalavimams prezumpcija

1. Jei didelės rizikos DI sistema buvo mokoma ir bandoma naudojant duomenis, atspindinčius konkrečią geografinę, elgsenos, kontekstinę ar funkcinę aplinką, kurioje ją ketinama naudoti, preziumuojama, kad ji atitinka 10 straipsnio 4 dalyje nustatytus atitinkamus reikalavimus.

2. Jei didelės rizikos DI sistema yra, laikantis Reglamento (ES) 2019/881, sertifikuota pagal kibernetinio saugumo sertifikavimo schemą, kurios nuoroda yra paskelbta *Europos Sąjungos oficialiajame leidinyje*, arba jai pagal šią schemą yra išduotas atitikties pareiškimas, preziumuojama, 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. III priedo 1 punkte išvardytų didelės rizikos DI sistemų atveju, kai tiekėjas, siekdamas įrodyti, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus, taiko 40 straipsnyje nurodytus darniuosius standartus arba, kai taikytina, 41 straipsnyje nurodytas bendrąsias specifikacijas, jis pasirenka taikyti vieną iš šių atitikties vertinimo procedūrų, grindžiamų:

   a) vidaus kontrole, kaip nurodyta VI priede, arba

   b) kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu, dalyvaujant notifikuotajai įstaigai, kaip nurodyta VII priede.

   Siekdamas įrodyti, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus, tiekėjas taiko VII priede nustatytą atitikties vertinimo procedūrą, jeigu:

   a) 40 straipsnyje nurodytų darniųjų standartų ir 41 straipsnyje nurodytų bendrųjų specifikacijų nėra;

   b) tiekėjas netaiko darniojo standarto arba jį taiko tik iš dalies;

   c) a punkte nurodytos bendrosios specifikacijos yra, tačiau tiekėjas jų netaiko;

d) vienas ar daugiau a punkte nurodytų darniųjų standartų yra paskelbtas su apribojimais – tik tos standarto dalies, kuriai taikomas apribojimas, atžvilgiu.

VII priede nurodytai atitikties vertinimo procedūrai atlikti tiekėjas gali pasirinkti bet kurią notifikuotąją įstaigą. Tačiau jei didelės rizikos DI sistemą ketinama naudoti teisėsaugos, imigracijos arba prieglobsčio institucijose, arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, notifikuotosios įstaigos funkcijas atlieka atitinkamai 74 straipsnio 8 arba 9 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.

3. Didelės rizikos DI sistemų, kurioms taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, atveju tiekėjas taiko atitinkamą tuose teisės aktuose reikalaujamą atitikties vertinimo procedūrą. Toms didelės rizikos DI sistemoms taikomi šio skyriaus 2 skirsnyje 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 2 skirsnyje 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 31 straipsnio 4, 5, 10 ir 11 dalyse nustatytiems reikalavimams.

Kai pagal teisės aktą, įtrauktą į I priedo A skirsnio sąrašą, gaminio gamintojas gali netaikyti trečiosios šalies atliekamo atitikties vertinimo su sąlyga, kad gamintojas taiko visus darniuosius standartus, apimančius visus atitinkamus reikalavimus, tas gamintojas ta galimybe gali pasinaudoti tik jei jis taiko ir darniuosius standartus arba, kai taikytina, 41 straipsnyje nurodytas bendrąsias specifikacijas, apimančius visus šio skyriaus 2 skirsnyje nustatytus reikalavimus.

4. Iš esmės pakeitus didelės rizikos DI sistemą, kuriai jau taikyta atitikties vertinimo procedūra, atliekama nauja jos atitikties vertinimo procedūra, neatsižvelgiant į tai, ar pakeistą sistemą ketinama papildomai platinti, ar ja toliau naudosis dabartinis diegėjas.

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 suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti VI ir VII priedus, kad juos atnaujintų atsižvelgiant į techninę pažangą.

6. Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti šio straipsnio 1 ir 2 dalis, kad III priedo 2–8 punktuose nurodytoms didelės rizikos DI sistemoms būtų taikoma VII priede nurodyta atitikties vertinimo procedūra arba jos dalis. 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 valstybės narės, kurioje yra įsisteigusi notifikuotoji įstaiga, atitinkamoms institucijoms lengvai suprantama kalba.

2. Sertifikatai galioja juose nurodytą laikotarpį, kuris DI sistemų, kurioms taikomas I priedas, atveju negali būti ilgesnis nei penkeri metai, o DI sistemų, kurioms taikomas III priedas, atveju – ketveri metai. Tiekėjui paprašius, remiantis pakartotiniu vertinimu pagal taikytinas atitikties vertinimo procedūras, sertifikato galiojimas gali būti pratęstas papildomiems laikotarpiams, kurių nė vienas DI sistemų, kurioms taikomas I priedas, atveju negali būti ilgesnis nei penkeri metai, o DI sistemų, kurioms taikomas III priedas, atveju – ketveri metai. Bet koks sertifikato papildymas galioja tol, kol galioja sertifikatas, kurį jis papildo.

3. Jei notifikuotoji įstaiga nustato, kad DI sistema nebeatitinka 2 skirsnyje nustatytų reikalavimų, ji, atsižvelgdama į proporcingumo principą, laikinai sustabdo arba panaikina išduoto sertifikato galiojimą arba nustato jo galiojimo apribojimus, nebent sistemos tiekėjas per atitinkamą notifikuotosios įstaigos nustatytą laikotarpį tinkamais taisomaisiais veiksmais užtikrina atitiktį tiems reikalavimams. Notifikuotoji įstaiga nurodo savo sprendimo priežastis.

Turi būti nustatyta notifikuotųjų įstaigų sprendimų, įskaitant sprendimus dėl išduotų atitikties sertifikatų, apskundimo procedūra.

45 straipsnis

Notifikuotųjų įstaigų pareiga informuoti

1. Notifikuotoji įstaiga informuoja notifikuojančiąją instituciją apie:

a) visus Sąjungos techninių dokumentų įvertinimo sertifikatus, tų sertifikatų papildymus ir visus 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 valdymo sistemų patvirtinimus;

b) Sąjungos 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 tipų DI sistemų atitikties vertinimo veiklą, teikia aktualią informaciją klausimais, susijusiais su neigiamais ir, jei prašoma, teigiamais atitikties vertinimo rezultatais.

4. Notifikuotosios įstaigos laikydamosi 78 straipsnio saugo gautos informacijos konfidencialumą.

46 straipsnis

Nukrypti nuo atitikties vertinimo procedūros leidžianti nuostata

1. Nukrypdama nuo 43 straipsnio ir gavusi deramai pagrįstą prašymą, bet kuri rinkos priežiūros institucija gali dėl išskirtinių priežasčių, susijusių su visuomenės saugumu arba žmonių gyvybės ir sveikatos, aplinkos ar 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, atsižvelgiant į išimtines nukrypti leidžiančią nuostatą pagrindžiančias priežastis. Tos procedūros užbaigiamos nepagrįstai nedelsiant.

2. Deramai pagrįstais skubos atvejais dėl išskirtinių visuomenės saugumo priežasčių arba konkrečios didelės ir neišvengiamos grėsmės fizinių asmenų gyvybei ar fiziniam saugumui atveju teisėsaugos institucijos arba civilinės saugos institucijos gali pradėti naudoti konkrečią didelės rizikos DI sistemą be 1 dalyje nurodyto leidimo, jeigu tokio leidimo nederamai nedelsiant paprašoma jos naudojimo metu arba po jo. Jei 1 dalyje nurodytą leidimą atsisakoma išduoti, didelės rizikos DI sistemos naudojimas nedelsiant nutraukiamas, o visi šio naudojimo rezultatai ir išvediniai nedelsiant ištrinami.

3. 1 dalyje nurodytas leidimas išduodamas tik jei rinkos priežiūros institucija padaro išvadą, kad didelės rizikos DI sistema atitinka 2 skirsnyje nustatytus reikalavimus. Rinkos priežiūros institucija informuoja Komisiją ir kitas valstybes nares apie visus pagal 1 ir 2 dalis išduotus leidimus. Ši pareiga netaikoma su teisėsaugos institucijų veikla susijusiems neskelbtiniems operatyviniams duomenims.

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

5. Jei per 15 kalendorinių dienų nuo 3 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 3 dalį valstybių narių padaryta išvada dėl sistemos atitikties yra nepagrįsta, Komisija nedelsdama pradeda konsultacijas su atitinkama valstybe nare. Konsultuojamasi su atitinkamais veiklos vykdytojais ir jiems suteikiama galimybė pareikšti savo nuomonę. Atsižvelgdama į tai, Komisija nusprendžia, ar leidimas yra pagrįstas. Savo sprendimą Komisija skiria atitinkamai valstybei narei ir atitinkamiems veiklos vykdytojams.

6. Jei Komisija nusprendžia, kad leidimas nepagrįstas, atitinkamos valstybės narės rinkos priežiūros institucija jį panaikina.

7. Didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi I priedo A skirsnyje nurodyti Sąjungos derinamieji teisės aktai, atveju taikomos tik tuose Sąjungos derinamuosiuose teisės aktuose nustatytos nukrypti nuo atitikties vertinimo procedūros leidžiančios nuostatos.

47 straipsnis

ES atitikties deklaracija

1. Tiekėjas parengia kiekvienos didelės rizikos DI sistemos rašytinę kompiuterio skaitomą, fizinę arba elektroniniu būdu pasirašytą ES atitikties deklaraciją ir saugo ją 10 metų po tos didelės rizikos DI sistemos pateikimo rinkai arba naudojimo pradžios dienos, kad nacionalinės kompetentingos institucijos galėtų ją patikrinti. ES atitikties deklaracijoje nurodoma, kokiai konkrečiai didelės rizikos DI sistemai 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 2 skirsnyje nustatytus reikalavimus. ES atitikties deklaracijoje pateikiama V priede nurodyta informacija ir ta deklaracija išverčiama į valstybių narių, kuriose didelės rizikos DI sistema pateikiama rinkai ar tiekiama, nacionalinėms kompetentingoms institucijoms lengvai suprantamą kalbą.

3. Jei didelės rizikos DI sistemoms taikomi ir kiti Sąjungos derinamieji teisės aktai, kuriuose taip pat reikalaujama ES atitikties deklaracijos, 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 2 skirsnyje nustatytiems reikalavimams. Tiekėjas užtikrina, kad ES atitikties deklaracija būtų tinkamai atnaujinama.

5. Komisija suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti V priedą, kad būtų atnaujintas tame priede išdėstytos ES atitikties deklaracijos turinys, siekiant į jį įtraukti elementus, kurie tampa būtini atsižvelgiant į technikos pažangą.

48 straipsnis

CE ženklas

1. Ženklinimui CE ženklu taikomi Reglamento (EB) Nr. 765/2008 30 straipsnyje nustatyti bendrieji principai.

2. Didelės rizikos DI sistemų, kurios teikiamos skaitmenine forma, atveju skaitmeninis CE ženklas naudojamas tik tuo atveju, jei jį galima lengvai pasiekti per sąsają, kuria naudojantis galima prisijungti prie tos sistemos, arba per lengvai prieinamą kompiuterio skaitomą kodą ar kitas elektronines priemones.

3. Didelės rizikos DI sistemos CE ženklu ženklinamos taip, kad jis būtų matomas, įskaitomas ir nenutrinamas. Tais atvejais, kai toks ženklinimas neįmanomas arba neužtikrinamas dėl didelės rizikos DI sistemos pobūdžio, šiuo ženklu atitinkamai pažymima pakuotė arba pridedami dokumentai.

4. Jei taikytina, prie CE ženklo nurodomas notifikuotosios įstaigos, atsakingos už 43 straipsnyje nustatytas atitikties vertinimo procedūras, identifikacinis numeris. Notifikuotosios įstaigos identifikaciniu numeriu gaminį pažymi pati notifikuotoji įstaiga arba jos nurodymu tą padaro tiekėjas arba tiekėjo įgaliotasis atstovas. Identifikacinis numeris taip pat nurodomas visoje reklaminėje medžiagoje, kurioje nurodoma, kad didelės rizikos DI sistema atitinka žymėjimo CE ženklu reikalavimus.

5. Jeigu didelės rizikos DI sistemoms taikomi kiti Sąjungos teisės aktai, kuriais taip pat numatytas ženklinimas CE ženklu, CE ženklu nurodoma, kad didelės rizikos DI sistemos atitinka ir tų kitų teisės aktų reikalavimus.

49 straipsnis

Registravimas

1. Prieš pateikdamas rinkai arba pradėdamas naudoti III priede nurodytą didelės rizikos DI sistemą, išskyrus III priedo 2 punkte nurodytas didelės rizikos DI sistemas, tiekėjas arba, jei taikytina, įgaliotasis atstovas 71 straipsnyje nurodytoje ES duomenų bazėje užsiregistruoja pats ir užregistruoja savo sistemas.

2. Prieš pateikdamas rinkai arba pradėdamas naudoti DI sistemą, kurios atžvilgiu tiekėjas yra padaręs išvadą, kad tai nėra didelės rizikos sistema pagal 6 straipsnio 3 dalį, tas tiekėjas arba, jei taikytina, įgaliotasis atstovas 71 straipsnyje nurodytoje ES duomenų bazėje užsiregistruoja pats ir užregistruoja tą sistemą.

3. Prieš pradėdami naudoti arba naudodami III priede nurodytą didelės rizikos DI sistemą, išskyrus III priedo 2 punkte išvardytas didelės rizikos DI sistemas, diegėjai, kurie yra valdžios institucijos, Sąjungos institucijos, įstaigos, organai ar agentūros arba jų vardu veikiantys asmenys, 71 straipsnyje nurodytoje ES duomenų bazėje užsiregistruoja patys, pasirenka sistemą ir užregistruoja jos naudojimą.

4. III priedo 1, 6 ir 7 punktuose nurodytos didelės rizikos DI sistemos, taikomos teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo srityse, pagal šio straipsnio 1, 2 ir 3 dalis užregistruojamos 71 straipsnyje nurodytos ES duomenų bazės saugioje neviešoje dalyje ir, kai taikytina, apima tik šią informaciją, nurodytą:

   a) VIII priedo A skirsnio 1–10 punktuose, išskyrus 6, 8 ir 9 punktus;

   b) VIII priedo B skirsnio 1–5 punktuose ir 8 bei 9 punktuose;

   c) VIII priedo C skirsnio 1–3 punktuose;

   d) IX priedo 1, 2 ir 3 punktuose bei 5 punkte.

Tik Komisijai ir nacionalinėms institucijoms, nurodytoms 74 straipsnio 8 dalyje, suteikiama prieiga prie atitinkamų šios dalies pirmoje pastraipoje išvardytų ES duomenų bazės riboto naudojimo dalių.

5. III priedo 2 punkte nurodytos didelės rizikos DI sistemos užregistruojamos nacionaliniu lygmeniu.

IV skyrius
Tam tikrų DI sistemų tiekėjams ir diegėjams taikomos skaidrumo pareigos

50 straipsnis

Tam tikrų DI sistemų tiekėjams ir diegėjams taikomos skaidrumo pareigos

1. Tiekėjai užtikrina, kad DI sistemos, kurių paskirtis – tiesiogiai sąveikauti su fiziniais asmenimis, būtų suprojektuotos ir sukurtos taip, kad atitinkami fiziniai asmenys būtų informuojami apie tai, kad jie sąveikauja su DI sistema, nebent fiziniam asmeniui, kuris yra pagrįstai informuotas, pastabus ir nuovokus, tai būtų akivaizdu, atsižvelgiant į aplinkybes ir naudojimo kontekstą. Ši pareiga netaikoma DI sistemoms, kurias pagal teisės aktus leidžiama naudoti siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ir už jas patraukti baudžiamojon atsakomybėn, taikant atitinkamas trečiųjų šalių teisių ir laisvių apsaugos priemones, nebent tomis sistemomis leidžiama naudotis visuomenei pranešimo apie nusikalstamą veiką tikslais.

2. DI sistemų, įskaitant bendrosios paskirties DI sistemas, kuriomis sugeneruojamas sintetinis judamo ar nejudamo vaizdo arba garso ar tekstinis turinys, tiekėjai užtikrina, kad DI sistemos išvediniai būtų pažymėti kompiuterio skaitomu formatu ir kad būtų galima atpažinti, jog jie yra sugeneruoti dirbtinai arba manipuliuojant. Tiekėjai užtikrina, kad jų techniniai sprendimai būtų veiksmingi, sąveikūs, pagrįsti ir patikimi, kiek tai techniškai įmanoma, atsižvelgiant į įvairių rūšių turinio ypatumus ir ribotumus, įgyvendinimo sąnaudas ir visuotinai pripažintus pažangiausius metodus, kurie gali būtų atspindėti atitinkamuose techniniuose standartuose. Ši pareiga netaikoma, jei DI sistemomis atliekama pagalbinė standartinio redagavimo funkcija arba iš esmės nepakeičiami diegėjo pateikti įvesties duomenys ar jų semantika, arba kai tai leidžiama pagal teisės aktus siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ar už jas patraukti baudžiamojon atsakomybėn.

3. Emocijų atpažinimo sistemos arba biometrinio kategorizavimo sistemos diegėjai informuoja fizinius asmenis, kuriems šios sistemos taikomos, apie jų veikimą, o asmens duomenis tvarko laikydamiesi atitinkamai reglamentų (ES) 2016/679 bei (ES) 2018/1725 ir Direktyvos (ES) 2016/680. Ši pareiga netaikoma DI sistemoms, naudojamoms biometriniam kategorizavimui ir emocijų atpažinimui, kurias pagal teisės aktus leidžiama naudoti siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ir už jas patraukti baudžiamojon atsakomybėn, taikant atitinkamas trečiųjų šalių teisių bei laisvių apsaugos priemones ir laikantis Sąjungos teisės.

4. DI sistemos, kuria generuojamas arba atlikus manipuliacijas gaunamas sintetinę sankaitą sudarantis judamo ar nejudamo vaizdo arba garso turinys, diegėjai atskleidžia, kad toks turinys yra sugeneruotas dirbtinai arba manipuliuojant. Ši pareiga netaikoma, kai naudojimas leidžiamas pagal teisės aktus siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ar už jas patraukti baudžiamojon atsakomybėn. Tais atvejais, kai turinys yra akivaizdžiai meninio, kūrybinio, satyrinio, išgalvoto ar analogiško kūrinio ar programos dalis, šioje dalyje nustatyti skaidrumo reikalavimai apima tik tokio sugeneruoto turinio ar turinio, gauto atlikus manipuliacijas, buvimo fakto atskleidimą tinkamu būdu, kuris netrukdo rodyti kūrinį ar juo mėgautis.

DI sistemos, kuria generuojamas arba kuria atlikus manipuliacijas gaunamas tekstas, paskelbiamas siekiant informuoti visuomenę viešojo intereso klausimais, diegėjai atskleidžia, kad tekstas yra sugeneruotas dirbtinai arba manipuliuojant. Ši pareiga netaikoma tais atvejais, kai naudoti leidžiama pagal teisės aktus siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ar už jas patraukti baudžiamojon atsakomybėn arba kai DI sugeneruotam turiniui buvo taikomas žmogaus atliekamos peržiūros arba redakcinės kontrolės procesas, o fizinis ar juridinis asmuo prisiima redakcinę atsakomybę už turinio paskelbimą.

5. 1–4 dalyse nurodyta informacija atitinkamiems fiziniams asmenims pateikiama aiškiai ir matomai ne vėliau nei pirmosios sąveikos arba sistemos panaudojimo jų atžvilgiu metu. Informacija turi atitikti taikomus prieinamumo reikalavimus.

6. 1–4 dalys nedaro poveikio III skyriuje nustatytiems reikalavimams bei pareigoms ir nedaro poveikio kitoms Sąjungos ar nacionalinės teisės aktuose nustatytoms DI sistemų diegėjų skaidrumo pareigoms.

7. DI tarnyba skatina ir palengvina praktikos kodeksų rengimą Sąjungos lygmeniu, kad būtų sudarytos palankesnės sąlygos veiksmingai įgyvendinti pareigas, susijusias su turinio, kuris yra sugeneruotas dirbtinai arba manipuliuojant, aptikimu ir ženklinimu. Komisija gali priimti įgyvendinimo aktus, kuriais tie praktikos kodeksai būtų patvirtinti laikantis 56 straipsnio 6 dalyje nustatytos tvarkos. Jei Komisija mano, kad kodeksas nėra tinkama priemonė, ji gali priimti įgyvendinimo aktą, kuriame būtų išsamiai nustatytos bendros tų pareigų vykdymo taisyklės, laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

V skyrius
Bendrosios paskirties DI modeliai

1 SKIRSNIS
PRISKYRIMO TAISYKLĖS

51 straipsnis
Bendrosios paskirties DI modelių priskyrimas
sisteminės rizikos bendrosios paskirties DI modeliams

1. Bendrosios paskirties DI modelis priskiriamas sisteminės rizikos bendrosios paskirties DI modeliui, jei jis atitinka kurią nors iš šių sąlygų:

   a) turi didelio poveikio pajėgumų, vertinamų remiantis atitinkamomis techninėmis priemonėmis ir metodikomis, įskaitant rodiklius ir lyginamuosius parametrus;

b) remiantis Komisijos sprendimu, *ex officio* arba gavus kvalifikuotą mokslinės komisijos perspėjimą, jo pajėgumai arba poveikis, atsižvelgiant į XIII priede nustatytus kriterijus, yra lygiaverčiai a punkte nustatytiems pajėgumams arba poveikiui.

2. Preziumuojama, kad bendrosios paskirties DI modelis turi didelio poveikio pajėgumų pagal 1 dalies a punktą, kai jo mokymui naudojama bendra skaičiuojamoji galia, išreikšta slankiojo kablelio operacijomis, yra didesnė nei 10^{25}.

3. Komisija pagal 97 straipsnį priima deleguotuosius aktus, kuriais iš dalies keičiamos šio straipsnio 1 ir 2 dalyse išvardytos ribinės vertės, taip pat papildomi lyginamieji parametrai ir rodikliai, atsižvelgiant į vykstančią technologinę plėtrą, pavyzdžiui, algoritmų patobulinimus arba padidėjusį aparatinės įrangos efektyvumą, kad prireikus šios ribinės vertės atspindėtų pažangiausius metodus.

52 straipsnis

Procedūra

1. Jei bendrosios paskirties DI modelis atitinka 51 straipsnio 1 dalies a punkte nurodytą sąlygą, atitinkamas tiekėjas nedelsdamas ir bet kuriuo atveju per dvi savaites po to, kai reikalavimas įvykdomas arba sužinoma, kad jis bus įvykdytas, praneša apie tai Komisijai. Tame pranešime pateikiama informacija, būtina įrodyti, kad atitinkamas reikalavimas įvykdytas. Jei Komisija sužino apie bendrosios paskirties DI modelį, kuris kelia sisteminę riziką, ir apie kurį jai nebuvo pranešta, ji gali nuspręsti jį priskirti sisteminės rizikos modeliams.

2. Bendrosios paskirties DI modelio, atitinkančio 51 straipsnio 1 dalies a punkte nurodytą sąlygų, tiekėjas kartu su pranešimu gali pateikti pakankamai pagrįstų argumentų, kad įrodytų, jog bendrosios paskirties DI modelis, nors ir atitinka tą reikalavimą, dėl savo specifinių savybių nekelia sisteminės rizikos, todėl išimties tvarka neturėtų būti priskiriamas sisteminės rizikos bendrosios paskirties DI modeliams.

3. Jei Komisija padaro išvadą, kad pagal 2 dalį pateikti argumentai nėra pakankamai pagrįsti ir atitinkamas tiekėjas nepajėgė įrodyti, kad bendrosios paskirties DI modelis dėl savo specifinių savybių nekelia sisteminės rizikos, ji tuos argumentus atmeta, o bendrosios paskirties DI modelis laikomas sisteminės rizikos bendrosios paskirties DI modeliu.

4. Komisija gali priskirti bendrosios paskirties DI modelį sisteminės rizikos modeliams *ex officio* arba gavusi kvalifikuotą mokslinės komisijos perspėjimą pagal 90 straipsnio 1 dalies a punktą, remdamasi XIII priede nustatytais kriterijais.

   Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, siekiant iš dalies pakeisti XIII priedą, patikslindama ir atnaujindama tame priede išdėstytus kriterijus.

5. Gavusi pagrįstą tiekėjo, kurio bendrosios paskirties DI modelis pagal 4 dalį priskirtas sisteminės rizikos modeliams, prašymą, Komisija atsižvelgia į prašymą ir gali nuspręsti iš naujo įvertinti, ar remiantis XIII priede nustatytais kriterijais šis bendrosios paskirties DI modelis vis dar gali būti laikomas sisteminės rizikos modeliu. Tokiame prašyme nurodomos objektyvios, išsamios ir naujos priežastys, atsiradusios po sprendimo dėl priskyrimo priėmimo. Tiekėjai gali prašyti atlikti pakartotinį vertinimą ne anksčiau kaip praėjus šešiems mėnesiams po sprendimo dėl priskyrimo priėmimo. Jei Komisija, atlikusi pakartotinį vertinimą, nusprendžia, kad atitinkamas modelis turi likti priskirtas sisteminės rizikos bendrosios paskirties DI modeliams, tiekėjai gali prašyti atlikti pakartotinį vertinimą ne anksčiau kaip praėjus šešiems mėnesiams po to sprendimo priėmimo.

6. Komisija užtikrina, kad būtų paskelbtas sisteminės rizikos bendrosios paskirties DI modelių sąrašas, ir nuolat jį atnaujina, nedarant poveikio poreikiui paisyti intelektinės nuosavybės teisių ir verslo informacijos konfidencialumo ar komercinių paslapčių ir juos saugoti pagal Sąjungos ir nacionalinę teisę.

2 SKIRSNIS

BENDROSIOS PASKIRTIES DI MODELIŲ TIEKĖJŲ PAREIGOS

53 straipsnis

Bendrosios paskirties DI modelių tiekėjų pareigos

1. Bendrosios paskirties DI modelių tiekėjai:

   a) rengia ir nuolat atnaujina modelio, be kita ko, jo mokymo ir bandymo proceso, taip pat jo vertinimo rezultatų, techninius dokumentus, į kuriuos įtraukiami bent XI priede nustatyta informacija, kad paprašius ji būtų pateikta DI tarnybai ir nacionalinėms kompetentingoms institucijoms;

   b) rengia, nuolat atnaujina ir teikia informaciją ir dokumentus DI sistemų tiekėjams, kurie ketina bendrosios paskirties DI modelį integruoti į savo DI sistemas. Nedarant poveikio poreikiui gerbti ir apsaugoti intelektinės nuosavybės teises ir verslo informacijos konfidencialumą arba komercines paslaptis pagal Sąjungos ir nacionalinę teisę, informacija ir dokumentai:

      i) sudaro sąlygas DI sistemų tiekėjams gerai suprasti bendrosios paskirties DI modelio pajėgumus bei ribotumus ir vykdyti savo pareigas pagal šį reglamentą ir

      ii) apima bent XII priede nustatytus elementus;

c) padeda įdiegti politiką, kad būtų laikomasi Sąjungos autorių ir gretutinių teisių teisės, visų pirma nustatyti teisių apribojimą pagal Direktyvos (ES) 2019/790 4 straipsnio 3 dalį, ir jos laikytis, be kita ko, pasitelkiant pažangiausias technologijas;

d) parengia ir viešai paskelbia pakankamai išsamią turinio, naudojamo bendrosios paskirties DI modelio mokymui, santrauką pagal DI tarnybos pateiktą šabloną.

2. 1 dalies a ir b punktuose nustatytos pareigos netaikomos DI modelių, kurie išleidžiami pagal nemokamą ir atvirojo kodo licenciją, kuria suteikiama prieiga prie modelio, leidžiama jį naudoti, keisti ir platinti, tiekėjams, ir kurių parametrai, įskaitant svorius, informaciją apie modelio architektūrą ir informaciją apie modelio naudojimą, skelbiami viešai. Ši išimtis netaikoma sisteminės rizikos bendrosios paskirties DI modeliams.

3. Naudodamiesi savo kompetencija ir įgaliojimais pagal šį reglamentą bendrosios paskirties DI modelių tiekėjai prireikus bendradarbiauja su Komisija ir nacionalinėmis kompetentingomis institucijomis.

4. Bendrosios paskirties DI modelių tiekėjai, siekdami įrodyti, kad laikosi šio straipsnio 1 dalyje nustatytų pareigų, gali remtis praktikos kodeksais, kaip tai suprantama 56 straipsnyje, kol bus paskelbtas darnusis standartas. Atitiktis preziumuojama, jei tiekėjai laikosi Europos darniųjų standartų, tokia apimtimi, kokia tie standartai apima tas pareigas. Bendrosios paskirties DI modelių tiekėjai, kurie nesilaiko patvirtinto praktikos kodekso arba nesilaiko Europos darniojo standarto, privalo įrodyti alternatyvias tinkamas atitikties užtikrinimo priemones, kad jas įvertintų Komisija.

5. Siekdama sudaryti palankesnes sąlygas laikytis XI priedo, ypač jo 2 punkto d ir e papunkčių, Komisijai suteikiami įgaliojimai pagal 97 straipsnį priimti deleguotuosius aktus, kuriuose išsamiai išdėstomos matavimo ir skaičiavimo metodikos, kad būtų galima parengti palyginamus ir patikrinamus dokumentus.

6. Komisijai suteikiami įgaliojimai pagal 97 straipsnio 2 dalį priima deleguotuosius aktus, kuriais, atsižvelgiant į vykstančią technologinę plėtrą, iš dalies keičiami XI ir XII priedai.

7. Visa pagal šį straipsnį gauta informacija ir dokumentai, įskaitant komercines paslaptis, tvarkomi laikantis 78 straipsnyje nustatytų konfidencialumo pareigų.

54 straipsnis

Bendrosios paskirties DI modelių tiekėjų įgaliotieji atstovai

1. Prieš pateikdami bendrosios paskirties DI modelį Sąjungos rinkai, trečiosiose valstybėse įsisteigę tiekėjai rašytiniu įgaliojimu paskiria Sąjungoje įsisteigusį įgaliotąjį atstovą.

2. Tiekėjas paveda įgaliotajam atstovui atlikti tiekėjo suteiktame įgaliojime nurodytas užduotis.

3. Įgaliotasis atstovas atlieka tiekėjo suteiktame įgaliojime nurodytas užduotis. Gavęs prašymą, jis DI tarnybai pateikia įgaliojimo kopiją viena iš oficialiųjų Sąjungos institucijų kalbų. Šio reglamento tikslais įgaliojimu įgaliotajam atstovui suteikiama teisė atlikti šias užduotis:

a) tikrinti, ar parengti XI priede nurodyti techniniai dokumentai ir ar tiekėjas įvykdė visas 53 straipsnyje ir, kai taikytina, 55 straipsnyje nurodytas pareigas;

b) 10 metų po bendrosios paskirties DI modelio pateikimo rinkai saugoti XI priede nurodytų techninių dokumentų kopijas, kad DI tarnyba ir nacionalinės kompetentingos institucijos galėtų juos patikrinti, ir, įgaliotąjį atstovą paskyrusio tiekėjo kontaktinius duomenis;

c) gavus pagrįstą prašymą, teikti DI tarnybai visą informaciją ir dokumentus, be kita ko, nurodytus b punkte, būtinus įrodyti šiame skyriuje nustatytų pareigų laikymąsi;

d) gavus pagrįstą prašymą bendradarbiauti su DI tarnyba ir kompetentingomis institucijomis atliekant veiksmus, kurių jos imasi bendrosios paskirties DI modelio atžvilgiu, be kita ko, atvejais, kai modelis yra integruotas į DI sistemas, pateiktas rinkai arba pradėtas naudoti Sąjungoje.

4. Įgaliojimu numatoma, kad DI tarnyba arba kompetentingos institucijos dėl visų aspektų, susijusių su šio reglamento laikymosi užtikrinimu, galėtų kreiptis ne vien į tiekėją, bet ir, papildomai, į įgaliotąjį atstovą, arba tik į įgaliotąjį atstovą vietoj tiekėjo.

5. Įgaliotasis atstovas nutraukia įgaliojimą, jei mano arba turi pagrindo manyti, kad tiekėjo veikla prieštarauja pagal šį reglamentą nustatytoms jo pareigoms. Tokiu atveju jis taip pat nedelsdamas informuoja DI tarnybą apie įgaliojimų nutraukimą ir to priežastis.

6. Šiame straipsnyje nustatyta pareiga netaikoma bendrosios paskirties DI modelių, kurie išleidžiami pagal nemokamą ir atvirojo kodo licenciją, kuria suteikiama prieiga prie modelio, leidžiama jį naudoti, keisti ir platinti, tiekėjams, ir kurių parametrai, įskaitant svorius, informaciją apie modelio architektūrą ir informaciją apie modelio naudojimą, skelbiami viešai, išskyrus atvejus, kai bendrosios paskirties DI modeliai kelia sisteminę riziką.

3 SKIRSNIS

SISTEMINĖS RIZIKOS BENDROSIOS PASKIRTIES DI MODELIŲ TIEKĖJŲ PAREIGOS

55 straipsnis

Sisteminės rizikos bendrosios paskirties DI modelių tiekėjų pareigos

1. Be 53 ir 54 straipsniuose išvardytų pareigų, sisteminės rizikos bendrosios paskirties DI modelių tiekėjai:

   a) atlieka modelio vertinimą pagal standartizuotus protokolus ir priemones, atspindinčias pažangiausius metodus, be kita ko, atlieka ir dokumentuoja modelio atsparumo kenksmingiems veiksmams bandymus, kad būtų nustatyta ir sumažinta sisteminė rizika;

   b) įvertina ir sumažina galimą sisteminę riziką Sąjungos lygmeniu, įskaitant jos šaltinius, kuri gali kilti dėl sisteminės rizikos bendrosios paskirties DI modelių kūrimo, pateikimo rinkai arba naudojimo;

   c) stebi, dokumentuoja ir nepagrįstai nedelsdami praneša DI tarnybai ir atitinkamai nacionalinėms kompetentingoms institucijoms atitinkamą informaciją apie rimtus incidentus ir galimas taisomąsias priemones jiems pašalinti;

   d) užtikrina tinkamą sisteminės rizikos bendrosios paskirties DI modelio ir fizinės modelio infrastruktūros apsaugos kibernetinio saugumo atžvilgiu lygį.

2. Sisteminės rizikos bendrosios paskirties DI modelių tiekėjai, siekdami įrodyti, kad laikosi šio straipsnio 1 dalyje nustatytų pareigų, gali remtis praktikos kodeksais, kaip tai suprantama 56 straipsnyje, kol bus paskelbtas darnusis standartas. Atitiktis preziumuojama, jei tiekėjai laikosi Europos darniųjų standartų, tokia apimtimi, kokia tie standartai apima tas pareigas. Sisteminės rizikos bendrosios paskirties DI modelių tiekėjai, kurie nesilaiko patvirtinto praktikos kodekso arba nesilaiko Europos darniojo standarto, privalo įrodyti alternatyvias tinkamas atitikties užtikrinimo priemones, kad jas įvertintų Komisija.

3. Visa pagal šį straipsnį gauta informacija ir dokumentai, įskaitant komercines paslaptis, tvarkomi laikantis 78 straipsnyje nustatytų konfidencialumo pareigų.

4 SKIRSNIS

PRAKTIKOS KODEKSAI

56 straipsnis

Praktikos kodeksai

1. DI tarnyba skatina ir palengvina praktikos kodeksų rengimą Sąjungos lygmeniu, kad būtų prisidedama prie tinkamo šio reglamento taikymo, atsižvelgiant į tarptautinius metodus.

2. DI tarnyba ir Valdyba siekia užtikrinti, kad praktikos kodeksai apimtų bent 53 ir 55 straipsniuose numatytas pareigas, įskaitant šiuos aspektus:

a) priemones, kuriomis užtikrinama, kad 53 straipsnio 1 dalies a ir b punktuose nurodyta informacija būtų nuolat atnaujinama atsižvelgiant į rinkos ir technologinę plėtrą;

b) tinkamą informacijos apie mokymui naudojamą turinį santraukos išsamumą;

c) sisteminės rizikos rūšies ir pobūdžio nustatymą Sąjungos lygmeniu, įskaitant, kai tinkama, jos šaltinius;

d) sisteminės rizikos vertinimo ir valdymo Sąjungos lygmeniu priemones, procedūras ir tvarką, įskaitant jos dokumentavimą, kurie turi būti proporcingi rizikai, kuriuose turi būti atsižvelgiama į jos dydį bei tikimybę ir į konkrečius iššūkius, su kuriais susiduriama šalinant tą riziką, atsižvelgiant į galimus tokios rizikos atsiradimo ir pasireiškimo būdus DI vertės grandinėje.

3. DI tarnyba gali pakviesti visus bendrosios paskirties DI modelių tiekėjus, taip pat atitinkamas nacionalines kompetentingas institucijas dalyvauti rengiant praktikos kodeksus. Prie šio proceso gali prisidėti pilietinės visuomenės organizacijos, pramonė, akademinė bendruomenė ir kiti atitinkami suinteresuotieji subjektai, pavyzdžiui, tolesnės grandies tiekėjai ir nepriklausomi ekspertai.

4. DI tarnyba ir Valdyba siekia užtikrinti, kad praktikos kodeksuose būtų aiškiai nustatyti jų konkretūs tikslai ir į juos būtų įtraukti įsipareigojimai ar priemonės, įskaitant, atitinkamai pagrindinius veiklos efektyvumo rezultatų rodiklius, siekiant užtikrinti, kad tie tikslai būtų pasiekti, ir kad juose būtų tinkamai atsižvelgta į visų suinteresuotųjų subjektų, įskaitant asmenis, kuriems daromas poveikis, poreikius ir interesus Sąjungos lygmeniu.

5. DI tarnyba siekia užtikrinti, kad praktikos kodeksuose dalyvaujantys subjektai reguliariai teiktų DI tarnybai ataskaitas apie įsipareigojimų ir priemonių, kurių buvo imtasi, įgyvendinimą ir jų rezultatus, be kita ko, atitinkamai įvertintus pagal pagrindinius veiklos efektyvumo rezultatų rodiklius. Pagrindiniuose veiklos rezultatų rodikliuose ir ataskaitų teikimo įsipareigojimuose atspindimi įvairių kodeksuose dalyvaujančių subjektų dydžio ir pajėgumų skirtumai.

6. DI tarnyba ir Valdyba reguliariai stebi ir vertina, kaip dalyvaujantys subjektai siekia praktikos kodeksų tikslų ir kaip jie prisideda prie tinkamo šio reglamento taikymo. DI tarnyba ir Valdyba įvertina, ar praktikos kodeksai apima 53 ir 55 straipsniuose numatytas pareigas, ir reguliariai stebi bei vertina, kaip įgyvendinami jų tikslai. Jos paskelbia praktikos kodeksų tinkamumo vertinimus.

   Komisija gali, priimdama įgyvendinimo aktą, patvirtinti praktikos kodeksą ir paskelbti jį galiojančiu visoje Sąjungoje. Tas įgyvendinimo aktas priimamas laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

7. DI tarnyba gali paraginti visus bendrosios paskirties DI modelių tiekėjus laikytis praktikos kodeksų. Bendrosios paskirties DI modelių, nekeliančių sisteminės rizikos, tiekėjai gali laikytis tik 53 straipsnyje numatytų pareigų, išskyrus atvejus, kai jie aiškiai pareiškia norą prisijungti prie viso kodekso.

8. DI tarnyba taip pat atitinkamai skatina ir palengvina praktikos kodeksų peržiūrą ir pritaikymą, visų pirma atsižvelgiant į naujus standartus. DI tarnyba padeda vertinti esamus standartus.

9. Praktikos kodeksai parengiami ne vėliau kaip … [devyni mėnesiai nuo šio reglamento įsigaliojimo dienos]. DI tarnyba imasi būtinų veiksmų, be kita ko, paragina tiekėjus pagal 7 dalį.

   Jei ne vėliau kaip … [12 mėnesių nuo įsigaliojimo dienos] praktikos kodeksas negali būti užbaigtas arba, jei DI tarnyba, atlikusi vertinimą pagal šio straipsnio 6 dalį, mano, kad jis netinkamas, Komisija gali įgyvendinimo aktais nustatyti bendras 53 ir 55 straipsniuose numatytų pareigų, įskaitant šio straipsnio 2 dalyje išdėstytus aspektus, įgyvendinimo taisykles. Tie įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

VI skyrius
Inovacijų rėmimo priemonės

57 straipsnis

Apribotos bandomosios DI reglamentavimo aplinkos

1. Valstybės narės užtikrina, kad jų kompetentingos institucijos nacionaliniu lygmeniu sukurtų bent vieną apribotą bandomąją DI reglamentavimo aplinką, kuri pradėtų veikti ne vėliau kaip … [24 mėnesiai nuo šio reglamento įsigaliojimo dienos]. Ta apribota bandomoji aplinka taip pat gali būti sukuriama kartu su kitų valstybių narių kompetentingomis institucijomis. Komisija gali teikti techninę paramą, konsultacijas ir priemones, kad būtų sukurtos ir veiktų apribotos bandomosios DI reglamentavimo aplinkos.

   Pirmoje pastraipoje nustatyta pareiga taip pat gali būti įvykdyta dalyvaujant esamoje apribotoje bandomojoje reglamentavimo aplinkoje, jei tokiu dalyvavimu dalyvaujančioms valstybėms narėms užtikrinama lygiavertė nacionalinė aprėptis.

2. Be to, regioniniu ar vietos lygmeniu arba kartu su kitomis valstybėmis narėmis gali būti sukurtos papildomos apribotos bandomosios DI reglamentavimo aplinkos.

3. Europos duomenų apsaugos priežiūros pareigūnas taip pat gali sukurti Sąjungos institucijoms, įstaigoms, organams ir agentūroms skirtą apribotą bandomąją DI reglamentavimo aplinką ir atlikti nacionalinių kompetentingų institucijų funkcijas ir užduotis pagal šį skyrių.

4. Valstybės narės užtikrina, kad 1 ir 2 dalyse nurodytos kompetentingos institucijos skirtų pakankamai išteklių, kad būtų veiksmingai ir laiku laikomasi šio straipsnio. Kai tinkama, nacionalinės kompetentingos institucijos bendradarbiauja su kitomis atitinkamomis institucijomis ir gali leisti dalyvauti kitiems DI ekosistemos subjektams. Šiuo straipsniu nedaromas poveikis kitoms apribotoms bandomosioms reglamentavimo aplinkoms, sukurtoms pagal Sąjungos arba nacionalinę teisę. Valstybės narės užtikrina tinkamą institucijų, prižiūrinčių tas kitas apribotas bandomąsias reglamentavimo aplinkas, ir nacionalinių kompetentingų institucijų bendradarbiavimą.

5. Apribotose bandomosiose DI reglamentavimo aplinkose, sukurtose pagal 1 dalį, numatoma kontroliuojama aplinka, kuria skatinamos inovacijos ir sudaromos palankesnės sąlygos kurti, mokyti, bandyti ir patvirtinti novatoriškas DI sistemas ribotą laiką prieš jas pateikiant rinkai arba pradedant naudoti laikantis konkretaus apribotos bandomosios reglamentavimo aplinkos plano, dėl kurio susitaria tiekėjai arba galimi tiekėjai ir kompetentinga institucija. Tokios apribotos bandomosios aplinkos gali apimti ir bandymą realiomis sąlygomis, prižiūrimą joje.

6. Kompetentingos institucijos apribotoje bandomojoje DI reglamentavimo aplinkoje atitinkamai teikia gaires, vykdo priežiūrą ir teikia paramą, kad būtų nustatyta rizika, visų pirma kylanti pagrindinėms teisėms, sveikatai ir saugai, bandymams, rizikos mažinimo priemonėms ir jų veiksmingumui, kiek tai susiję su šiame reglamente nustatytomis pareigomis ir reikalavimais ir, kai aktualu, kitais Sąjungos ir nacionalinės teisės aktais, kurių priežiūra vykdoma apribotoje bandomojoje reglamentavimo aplinkoje.

7. Kompetentingos institucijos tiekėjams ir galimiems tiekėjams, kurie dalyvauja apribotoje bandomojoje DI reglamentavimo aplinkoje, pateikia gaires dėl reglamentavimo lūkesčių ir dėl to, kaip vykdyti šiame reglamente nustatytus reikalavimus ir pareigas.

DI sistemos tiekėjo arba galimo tiekėjo prašymu kompetentinga institucija pateikia apribotoje bandomojoje reglamentavimo aplinkoje sėkmingai įvykdytos veiklos rašytinį įrodymą. Kompetentinga institucija taip pat pateikia pasitraukimo ataskaitą, kurioje išsamiai aprašoma apribotoje bandomojoje reglamentavimo aplinkoje vykdyta veikla ir susiję rezultatai bei mokymosi rezultatai. Tiekėjai gali naudoti tokius dokumentus, kad įrodytų, jog laikosi šio reglamento, atlikdami atitikties vertinimo procesą arba vykdydami atitinkamą rinkos priežiūros veiklą. Šiuo atžvilgiu rinkos priežiūros institucijos ir notifikuotosios įstaigos palankiai atsižvelgia į nacionalinės kompetentingos institucijos pateiktas pasitraukimo ataskaitas ir rašytinius įrodymus, kad būtų pakankamai paspartintos atitikties vertinimo procedūros.

8. Atsižvelgiant į 78 straipsnyje nustatytas konfidencialumo nuostatas ir gavus tiekėjo arba galimo tiekėjo sutikimą, Komisijai ir Valdybai suteikiama teisė susipažinti su pasitraukimo ataskaitomis ir atitinkamai į jas atsižvelgti vykdant savo užduotis pagal šį reglamentą. Jei tiekėjas arba galimas tiekėjas ir nacionalinė kompetentinga institucija tam aiškiai pritaria, pasitraukimo ataskaita gali būti paskelbta viešai šiame straipsnyje nurodytoje bendroje informacinėje platformoje.

9. Sukuriant apribotas bandomąsias DI reglamentavimo aplinkas siekiama prisidėti prie šių tikslų:

   a) didinti teisinį tikrumą, kad būtų užtikrinta atitiktis šio reglamento nuostatoms arba, kai aktualu, kitiems taikytiniems Sąjungos ir nacionalinės teisės aktams;

   b) remti dalijimąsi geriausios praktikos pavyzdžiais bendradarbiaujant su institucijomis, dalyvaujančiomis apribotoje bandomojoje DI reglamentavimo aplinkoje;

c) skatinti inovacijas bei konkurencingumą ir palengvinti DI ekosistemos plėtojimą;

d) prisidėti prie faktiniais duomenimis grindžiamo mokymosi reglamentavimo srityje.

e) palengvinti ir paspartinti DI sistemų patekimą į Sąjungos rinką, visų pirma kai jas teikia MVĮ, įskaitant startuolius.

10. Nacionalinės kompetentingos institucijos užtikrina, kad jei 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 arba tos kitos nacionalinės ar kompetentingos institucijos būtų įtrauktos į apribotos bandomosios DI reglamentavimo aplinkos veiklą ir vykdytų tų aspektų priežiūrą, kiek tai susiję su jų atitinkamomis užduotimis ir įgaliojimais.

11. Apribotos bandomosios DI reglamentavimo aplinkos nedaro poveikio šias aplinkas prižiūrinčių kompetentingų institucijų su priežiūra ir taisomaisiais veiksmais susijusiems įgaliojimams, be kita ko, regioniniu ar vietos lygmeniu. Kuriant ir bandant tokias DI sistemas nustatyta didelė rizika sveikatai, saugai ir pagrindinėms teisėms turi būti tinkamai sumažinta. Nacionalinės kompetentingos institucijos turi įgaliojimus laikinai arba visam laikui sustabdyti bandymų procesą arba dalyvavimą apribotoje bandomojoje reglamentavimo aplinkoje, jei rizikos neįmanoma veiksmingai sumažinti, ir apie tokį sprendimą informuoja DI tarnybą. Siekdamos remti DI inovacijas Sąjungoje, nacionalinės kompetentingos institucijos savo priežiūros įgaliojimais naudojasi laikydamosi atitinkamuose teisės aktuose nustatytų ribų, naudodamosi diskrecija įgyvendinant teisines nuostatas konkretaus apribotos bandomosios DI reglamentavimo aplinkos projekto atžvilgiu.

12. Tiekėjai ir galimi tiekėjai, dalyvaujantys apribotose bandomosiose DI reglamentavimo aplinkose, pagal taikytinus Sąjungos ir nacionalinės teisės aktus, kuriais reglamentuojama atsakomybė, išlieka atsakingi už žalą, padarytą trečiosioms šalims dėl apribotoje bandomojoje reglamentavimo aplinkoje vykdomo eksperimentavimo. Tačiau jei būsimas tiekėjas laikosi konkretaus plano bei dalyvavimo sąlygų, taip pat sąžiningai vadovaujasi nacionalinės kompetentingos institucijos pateiktomis gairėmis, už šio reglamento pažeidimus valdžios institucijos neskiria jokių administracinių baudų. Tais atvejais, kai kitos kompetentingos institucijos, atsakingos už kitus Sąjungos ir nacionalinės teisės aktus, aktyviai dalyvavo prižiūrint DI sistemą apribotoje bandomojoje reglamentavimo aplinkoje ir pateikė atitikties gaires, pagal tuos teisės aktus administracinės baudos neskiriamos.

13. Apribotos bandomosios DI reglamentavimo aplinkos projektuojamos ir įgyvendinamos taip, kad, kai aktualu, jomis būtų palengvintas tarpvalstybinis nacionalinių kompetentingų institucijų bendradarbiavimas.

14. Nacionalinės kompetentingos institucijos koordinuoja savo veiklą ir bendradarbiauja Valdyboje.

15. Nacionalinės kompetentingos institucijos informuoja DI tarnybą ir Valdybą apie apribotos bandomosios reglamentavimo aplinkos sukūrimą ir gali prašyti jų paramos bei gairių. DI tarnyba viešai skelbia planuojamų ir esamų apribotų bandomųjų aplinkų sąrašą ir nuolat jį atnaujina, kad būtų skatinama didesnė sąveika apribotose bandomosiose DI reglamentavimo aplinkose ir tarpvalstybinis bendradarbiavimas.

16. Nacionalinės kompetentingos institucijos DI tarnybai ir Valdybai teikia metines ataskaitas praėjus vieniems metams nuo apribotos bandomosios DI reglamentavimo aplinkos sukūrimo, o vėliau - kasmet iki jos taikymo nutraukimo, taip pat galutinę ataskaitą. Tose ataskaitose pateikiama informacija apie tų apribotų bandomųjų reglamentavimo aplinkų įgyvendinimo pažangą ir rezultatus, įskaitant geriausios praktikos pavyzdžius, incidentus, įgytą patirtį ir rekomendacijas dėl jų struktūros ir, kai aktualu, apie šio reglamento, įskaitant jo deleguotuosius ir įgyvendinimo aktus, taikymą ir galimą peržiūrą, taip pat apie kitų Sąjungos teisės aktų, kuriuos kompetentingos institucijos prižiūri apribotoje bandomojoje reglamentavimo aplinkoje, taikymą. Nacionalinės kompetentingos institucijos viešai paskelbia šias metines ataskaitas ar jų santraukas internete. Kai tinkama, Komisija atsižvelgia į metines ataskaitas vykdydama savo užduotis pagal šį reglamentą.

17. Komisija sukuria bendrą specialią sąsają, kurioje pateikiama visa aktuali informacija, susijusi su apribotomis bandomosiomis DI reglamentavimo aplinkomis, kad suinteresuotieji subjektai galėtų sąveikauti su apribotomis bandomosiomis DI reglamentavimo aplinkomis ir teikti užklausas kompetentingoms institucijoms, taip pat prašyti neprivalomų gairių dėl novatoriškų produktų, paslaugų, verslo modelių, kuriuose įdiegtos DI technologijos, atitikties pagal 62 straipsnio 1 dalies c punktą. Komisija, kai aktualu, proaktyviai koordinuoja veiksmus su nacionalinėmis kompetentingomis institucijomis.

58 straipsnis

Išsami apribotoms bandomosioms DI reglamentavimo aplinkoms taikoma tvarka ir jų veikimas

1. Siekdama išvengti susiskaidymo visoje Sąjungoje, Komisija priima įgyvendinimo aktus, kuriais nustatoma išsami apribotų bandomųjų DI reglamentavimo aplinkų kūrimo, plėtojimo, įgyvendinimo, veikimo ir priežiūros tvarka. Į tuos įgyvendinimo aktus įtraukiami bendri principai, susiję su šiais aspektais:

   a) tinkamumo ir atrankos kriterijais dalyvauti apribotoje bandomojoje DI reglamentavimo aplinkoje;

   b) prašymų dalyvauti apribotoje bandomojoje DI reglamentavimo aplinkoje teikimo, dalyvavimo joje, stebėsenos, pasitraukimo iš tokios aplinkos ir jos taikymo nutraukimo procedūromis, įskaitant apribotos bandomosios reglamentavimo aplinkos planą ir pasitraukimo ataskaitą;

   c) dalyviams taikomomis sąlygomis.

   Tie įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

2. 1 dalyje nurodytais įgyvendinimo aktais užtikrinama, kad:

   a) apribotose bandomosiose DI reglamentavimo aplinkose galėtų dalyvauti visi prašymus pateikę DI sistemų tiekėjai ar galimi tiekėjai, atitinkantys tinkamumo ir atrankos kriterijus, kurie būtų skaidrūs ir sąžiningi, ir kad nacionalinės kompetentingos institucijos per tris mėnesius nuo paraiškos pateikimo informuotų pareiškėjus apie savo sprendimą;

b) apribotos bandomosios DI reglamentavimo aplinkos suteiktų plačią bei vienodą prieigą ir tenkintų dalyvavimo paklausą, o tiekėjai ir galimi tiekėjai paraiškas taip pat galėtų teikti kartu su diegėjais ar kitomis atitinkamomis trečiosiomis šalimis;

c) išsamia apribotoms bandomosioms DI reglamentavimo aplinkoms taikoma tvarka ir sąlygomis būtų kuo labiau remiamas nacionalinių kompetentingų institucijų lankstumas kurti ir naudoti savo apribotas bandomąsias DI reglamentavimo aplinkas;

d) MVĮ ir startuoliams prieiga prie apribotų bandomųjų DI reglamentavimo aplinkų būtų suteikiama nemokamai, nedarant poveikio išimtinėms išlaidoms, kurias nacionalinės kompetentingos institucijos galėtų susigrąžinti sąžiningai ir proporcingai;

e) jais tiekėjams ir galimiems tiekėjams būtų sudarytos palankesnės sąlygos pasinaudojant apribotose bandomosiose DI reglamentavimo aplinkose gautais mokymosi rezultatais, vykdyti šiame reglamente nustatytas atitikties vertinimo pareigas ir savanoriškai taikyti 95 straipsnyje nurodytus elgesio kodeksus;

f) apribotomis bandomosiomis DI reglamentavimo aplinkomis būtų sudarytos palankesnės sąlygos dalyvauti kitiems atitinkamiems DI ekosistemos subjektams, pavyzdžiui, notifikuotosioms įstaigoms ir standartizacijos organizacijoms, MVĮ, įskaitant startuolius, įmonėms, novatoriams, bandymų ir eksperimentavimo priemonėms, mokslinių tyrimų ir eksperimentavimo laboratorijoms, Europos skaitmeninių inovacijų centrams, kompetencijos centrams, atskiriems tyrėjams, kad būtų sudarytos sąlygos bendradarbiavimui su viešuoju bei privačiuoju sektoriais ir jis būtų palengvintas;

g) paraiškų teikimo, atrankos, dalyvavimo ir pasitraukimo iš apribotos bandomosios DI reglamentavimo aplinkos procedūros, procesai ir administraciniai reikalavimai būtų paprasti, lengvai suprantami, aiškiai nurodyti siekiant palengvinti MVĮ, įskaitant startuolius, turinčių ribotus teisinius ir administracinius pajėgumus, dalyvavimą ir jie būtų supaprastinti visoje Sąjungoje, kad būtų išvengta susiskaidymo, o dalyvavimas valstybės narės arba Europos duomenų apsaugos priežiūros pareigūno sukurtoje apribotoje bandomojoje DI reglamentavimo aplinkoje būtų abipusiai ir vienodai pripažįstamas ir turėtų vienodą teisinį poveikį visoje Sąjungoje;

h) dalyvavimas apribotoje bandomojoje DI reglamentavimo aplinkoje truktų laikotarpį, kuris būtų tinkamas atsižvelgiant į projekto sudėtingumą ir mastą, ir kurį nacionalinė kompetentinga institucija gali pratęsti;

i) apribotos bandomosios DI reglamentavimo aplinkos padėtų kurti priemones ir infrastruktūrą, skirtas DI sistemų bandymams, jų lyginamųjų parametrų nustatymui, vertinimui ir mokymuisi reglamentavimo srityje aktualių DI sistemų aspektų (pavyzdžiui, tikslumo, patvarumo ir kibernetinio saugumo) paaiškinimui, taip pat priemones, kuriomis būtų sumažinta rizika pagrindinėms teisėms, aplinkai ir visai visuomenei.

3. Galimi tiekėjai, dalyvaujantys apribotose bandomosiose DI reglamentavimo aplinkose, visų pirma MVĮ ir startuoliai, kai aktualu, nukreipiami pasinaudoti pasirengimo diegimui paslaugomis, pavyzdžiui, patarimais dėl šio reglamento įgyvendinimo, kitomis pridėtinės vertės paslaugomis, pavyzdžiui, pagalba dėl standartizacijos dokumentų ir sertifikavimo, bandymų ir eksperimentavimo priemonių, Europos skaitmeninių inovacijų centrų ir kompetencijos centrų.

4. Kai nacionalinės kompetentingos institucijos svarsto galimybę leisti atlikti bandymą realiomis sąlygomis, prižiūrimą pagal šį straipsnį sukurtinoje apribotoje bandomojoje DI reglamentavimo aplinkoje, jos konkrečiai susitaria su dalyviais dėl tokio bandymo sąlygų, visų pirma dėl tinkamų apsaugos priemonių, kad būtų apsaugotos pagrindinės teisės, sveikata ir sauga. Kai tinkama, jos bendradarbiauja su kitomis nacionalinėmis kompetentingomis institucijomis, kad visoje Sąjungoje būtų užtikrinta nuosekli praktika.

59 straipsnis

Tolesnis asmens duomenų tvarkymas apribotoje bandomojoje DI reglamentavimo aplinkoje siekiant sukurti tam tikras su viešuoju interesu susijusias DI sistemas

1. Apribotoje bandomojoje DI reglamentavimo aplinkoje kitais tikslais teisėtai surinkti asmens duomenys gali būti tvarkomi tik tam tikrų DI sistemų kūrimo, mokymo ir bandymo apribotoje bandomojoje reglamentavimo aplinkoje tikslais, jei tenkinamos visos šios sąlygos:

   a) DI sistemas valdžios institucija arba kitas fizinis arba juridinis asmuo sukuria siekdami apsaugoti svarbų viešąjį interesą vienoje ar daugiau iš šių sričių:

      i) visuomenės saugumo ir visuomenės sveikatos, įskaitant ligų nustatymą, diagnozę, prevenciją, kontrolę ir gydymą, taip pat sveikatos priežiūros sistemų tobulinimo;

      ii) aukšto aplinkos apsaugos lygio užtikrinimo ir aplinkos kokybės gerinimo, biologinės įvairovės apsaugos, apsaugos nuo taršos, žaliosios pertvarkos priemonių, klimato kaitos švelninimo ir prisitaikymo prie jos priemonių;

iii) energetinio tvarumo;

iv) transporto sistemų ir judumo, ypatingos svarbos infrastruktūros ir tinklų saugos ir atsparumo;

v) viešojo administravimo ir viešųjų paslaugų veiksmingumo ir kokybės;

b) duomenų tvarkymas yra būtinas siekiant laikytis vieno ar daugiau iš III skyriaus 2 skirsnyje nurodytų reikalavimų, kai tų reikalavimų neįmanoma veiksmingai įvykdyti tvarkant anoniminius, sintetinius ar kitus ne asmens duomenis;

c) taikomi veiksmingi stebėsenos mechanizmai, skirti nustatyti, ar eksperimentuojant apribotoje bandomojoje reglamentavimo aplinkoje gali kilti didelė rizika duomenų subjektų teisėms ir laisvėms, kaip nurodyta Reglamento (ES) 2016/679 35 straipsnyje ir Reglamento (ES) 2018/1725 39 straipsnyje, taip pat atsako mechanizmai, skirti tai rizikai greitai sumažinti ir, prireikus, duomenų tvarkymui sustabdyti;

d) visi apribotoje bandomojoje reglamentavimo aplinkoje tvarkytini asmens duomenys saugomi funkciniu požiūriu atskirtoje, izoliuotoje ir apsaugotoje galimo tiekėjo kontroliuojamoje duomenų tvarkymo aplinkoje ir prieigą prie tų duomenų turi tik įgalioti asmenys;

e) tiekėjai iš pradžių surinktais duomenimis gali toliau dalytis tik laikydamiesi Sąjungos duomenų apsaugos teisės aktų; apribotoje bandomojoje reglamentavimo aplinkoje sukurtais asmens duomenimis už tos aplinkos ribų dalytis negalima;

f) dėl asmens duomenų tvarkymo apribotos bandomosios reglamentavimo aplinkos kontekste nepriimama jokių priemonių ar sprendimų, kurie darytų poveikį duomenų subjektams ar jų naudojimuisi teisėmis, nustatytomis Sąjungos teisės aktuose dėl asmens duomenų apsaugos;

g) visi apribotos bandomosios reglamentavimo aplinkos kontekste tvarkomi asmens duomenys apsaugomi tinkamomis techninėmis bei organizacinėmis priemonėmis, o pasibaigus dalyvavimui apribotoje bandomojoje reglamentavimo aplinkoje arba asmens duomenų saugojimo laikotarpiui – ištrinami;

h) asmens duomenų tvarkymo apribotos bandomosios reglamentavimo aplinkos kontekste registracijos žurnalai saugomi visą dalyvavimo apribotoje bandomojoje reglamentavimo aplinkoje laikotarpį, nebent Sąjungos arba nacionalinės teisės aktuose nustatyta kitaip;

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

j) kompetentingų institucijų svetainėje yra paskelbtas glaustas apribotoje bandomojoje reglamentavimo aplinkoje įgyvendinamo DI projekto, jo tikslų ir numatomų rezultatų aprašas; ši pareiga netaikoma neskelbtiniems operatyviniams duomenims, susijusiems su teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijų veikla.

2. Nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, kontroliuojant teisėsaugos institucijoms ir jų atsakomybe, asmens duomenų tvarkymas apribotose bandomosiose DI reglamentavimo aplinkose grindžiamas konkrečiu arba Sąjungos, arba valstybės narės teisės aktu ir jam taikomos visos tos pačios 1 dalyje nurodytos sąlygos.

3. 1 dalimi nedaromas poveikis Sąjungos ar nacionalinės teisės aktams, kuriais draudžiama tvarkyti asmens duomenis kitais tikslais, nei aiškiai nurodyta tuose teisės aktuose, taip pat Sąjungos ar nacionalinės teisės aktuose, kuriuose nustatomas asmens duomenų tvarkymo novatoriškų DI sistemų kūrimo, bandymo ar mokymo tikslais pagrindas arba kitas teisinis pagrindas, laikantis Sąjungos teisės aktų dėl asmens duomenų apsaugos.

60 straipsnis

Didelės rizikos DI sistemų bandymas realiomis sąlygomis už apribotų bandomųjų DI reglamentavimo aplinkų ribų

1. Nedarant poveikio 5 straipsnyje nustatytiems draudimams, III priede išvardytų didelės rizikos DI sistemų tiekėjai arba galimi tiekėjai, laikydamiesi šio straipsnio ir šiame straipsnyje nurodyto bandymo realiomis sąlygomis plano, gali atlikti didelės rizikos DI sistemų bandymą realiomis sąlygomis už apribotų bandomųjų DI reglamentavimo aplinkų ribų.

   Komisija įgyvendinimo aktais nurodo išsamius bandymo realiomis sąlygomis plano elementus. Tie įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Šia dalimi nedaromas poveikis Sąjungos ar nacionalinės teisės aktams dėl didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi I priede išvardyti teisės aktai, bandymo realiomis sąlygomis.

2. Tiekėjai arba galimi tiekėjai, patys vieni arba kartu su vienu ar daugiau diegėjų ar galimų diegėjų, III priede nurodytų didelės rizikos DI sistemų bandymą realiomis sąlygomis gali atlikti bet kuriuo metu prieš pateikdami DI sistemą rinkai arba prieš pradedant ją naudoti.

3. Didelės rizikos DI sistemų bandymas realiomis sąlygomis pagal šį straipsnį nedaro poveikio etikos aspektų vertinimui, kurio reikalaujama pagal Sąjungos ar nacionalinę teisę.

4. Tiekėjai arba galimi tiekėjai bandymą realiomis sąlygomis gali atlikti tik tuo atveju, jei tenkinamos visos šios sąlygos:

a) tiekėjas arba galimas tiekėjas yra parengęs bandymo realiomis sąlygomis planą ir jį yra pateikęs valstybės narės, kurioje turi būti atliekamas bandymas realiomis sąlygomis, rinkos priežiūros institucijai;

b) valstybės narės, kurioje turi būti atliekamas bandymas realiomis sąlygomis, rinkos priežiūros institucija yra patvirtinusi bandymą realiomis sąlygomis ir bandymo realiomis sąlygomis planą; jeigu rinkos priežiūros institucija per 30 dienų nepateikia atsakymo, laikoma, kad bandymas realiomis sąlygomis ir bandymo realiomis sąlygomis planas yra patvirtinti; jei nacionalinės teisės aktuose nėra numatytas tylus pritarimas, bandymui realiomis sąlygomis turi būti gautas leidimas;

c) tiekėjas arba galimas tiekėjas, išskyrus III priedo 1, 6 ir 7 punktuose nurodytų didelės rizikos DI sistemų teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo srityse ir didelės rizikos DI sistemų, nurodytų III priedo 2 punkte, tiekėjus ar galimus tiekėjus, bandymą realiomis sąlygomis yra užregistravęs pagal 71 straipsnio 4 dalį su Sąjungos masto unikaliu identifikaciniu numeriu ir su IX priede nurodyta informacija; III priedo 1, 6 ir 7 punktuose nurodytų didelės rizikos DI sistemų teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo srityse tiekėjas arba galimas tiekėjas bandymą realiomis sąlygomis yra užregistravęs ES duomenų bazės neviešoje dalyje pagal 49 straipsnio 4 dalies d punktą su Sąjungos masto unikaliu identifikaciniu numeriu ir su ten nurodyta informacija; didelės rizikos DI sistemų, nurodytų III priedo 2 punkte, tiekėjus ar galimus tiekėjus, bandymą realiomis sąlygomis yra užregistravęs pagal 49 straipsnio 5 dalį;

d) tiekėjas arba galimas tiekėjas, atliekantis bandymą realiomis sąlygomis, yra įsisteigęs Sąjungoje arba bandymo realiomis sąlygomis tikslais yra paskyręs Sąjungoje įsisteigusį teisinį atstovą;

e) duomenys, surinkti ir tvarkomi bandymo realiomis sąlygomis tikslais, trečiosioms valstybėms perduodami tik tuo atveju, jei įgyvendinamos tinkamos ir taikytinos apsaugos priemonės pagal Sąjungos teisę;

f) bandymas realiomis sąlygomis trunka ne ilgiau, nei būtina jo tikslams pasiekti, ir bet kuriuo atveju ne ilgiau kaip šešis mėnesius; šis laikotarpis gali būti pratęstas dar šešių mėnesių laikotarpiu, jei tiekėjas ar galimas tiekėjas apie tai iš anksto praneša rinkos priežiūros institucijai ir pateikia tokio pratęsimo poreikio paaiškinimą;

g) bandymo realiomis sąlygomis subjektai, kurie yra asmenys dėl savo amžiaus, fizinės ar psichinės negalios priskiriami pažeidžiamoms grupėms, yra tinkamai apsaugoti;

h) jeigu tiekėjas arba galimas tiekėjas bandymą realiomis sąlygomis organizuoja bendradarbiaudamas su vienu ar daugiau diegėjų arba galimų diegėjų, pastarieji yra informuoti apie visus bandymo aspektus, kurie yra aktualūs jų sprendimui dalyvauti, ir jiems yra pateikti 13 straipsnyje nurodyti atitinkami nurodymai dėl DI sistemos naudojimo; tiekėjas arba galimas tiekėjas ir diegėjas ar galimas diegėjas sudaro susitarimą, kuriame nurodomi jų vaidmenys ir atsakomybė siekiant užtikrinti, kad būtų laikomasi nuostatų dėl bandymo realiomis sąlygomis pagal šį reglamentą ir kitus taikytinus Sąjungos ir nacionalinės teisės aktus;

i) bandymo realiomis sąlygomis subjektai yra davę informuoto asmens sutikimą pagal 61 straipsnį arba, teisėsaugos atveju, kai prašant informuoto asmens sutikimo būtų užkirstas kelias DI sistemos bandymui, pats bandymas ir bandymo realiomis sąlygomis rezultatai nedaro neigiamo poveikio subjektams, o jų asmens duomenys užbaigus bandymą yra ištrinami;

j) bandymą realiomis sąlygomis tiekėjas arba galimas tiekėjas, taip pat diegėjai arba galimi diegėjai veiksmingai prižiūri, pasitelkdami asmenis, kurie turi tinkamą kvalifikaciją atitinkamoje srityje ir turi savo užduotims atlikti reikiamų gebėjimų, yra tam parengti ir turi atitinkamus įgaliojimus;

k) DI sistemos sugeneruotos predikcijos, rekomendacijos ar sprendimai gali būti veiksmingai atšaukti arba į juos gali būti neatsižvelgiama.

5. Bandymo realiomis sąlygomis subjektai arba atitinkamai jų teisėtai paskirtai atstovai, nepatirdami jokios žalos ir neprivalėdami pateikti jokio pagrindimo, gali bet kuriuo metu pasitraukti iš bandymo atšaukdami savo informuoto asmens sutikimą ir gali reikalauti, kad jų asmens duomenys būtų nedelsiant ištrinti. Informuoto asmens sutikimo atšaukimas neturi įtakos jau atliktai veiklai.

6. Pagal 75 straipsnį valstybės narės savo rinkos priežiūros institucijoms suteikia įgaliojimus reikalauti, kad tiekėjai ir galimi tiekėjai pateiktų informaciją, atlikti nuotolinius neplaninius patikrinimus arba patikrinimus vietoje ir patikrinimus, kaip vyksta bandymas realiomis sąlygomis, taip pat patikrinti susijusias didelės rizikos DI sistemas. Rinkos priežiūros institucijos naudojasi tais įgaliojimais, kad užtikrintų saugų bandymų realiomis sąlygomis plėtojimą.

7. Apie visus rimtus incidentus, nustatytus atliekant bandymą realiomis sąlygomis, pagal šio reglamento 73 straipsnį pranešama nacionalinei rinkos priežiūros institucijai. Tiekėjas arba galimas tiekėjas imasi neatidėliotinų rizikos sumažinimo priemonių arba, kai tai neįmanoma, sustabdo bandymą realiomis sąlygomis, kol tokia rizika bus sumažinta, arba kitu atveju jį nutraukia. Tiekėjas arba galimas tiekėjas nustato procedūrą, pagal kurią DI sistema būtų nedelsiant atšaukta, jei toks bandymas realiomis sąlygomis būtų nutrauktas.

8. Tiekėjai arba galimi tiekėjai valstybės narės, kurioje turi būti atliekamas bandymas realiomis sąlygomis, nacionalinei rinkos priežiūros institucijai praneša apie bandymo realiomis sąlygomis sustabdymą arba nutraukimą ir galutinius rezultatus.

9. Tiekėjai arba galimi tiekėjai pagal taikytinus Sąjungos ir nacionalinės teisės aktus, kuriais reglamentuojama atsakomybė, yra atsakingi už žalą, padarytą jų atliekamo bandymo realiomis sąlygomis metu.

61 straipsnis

Informuoto asmens sutikimas dalyvauti bandyme realiomis sąlygomis už apribotų bandomųjų DI reglamentavimo aplinkų ribų

1. Bandymo realiomis sąlygomis pagal 60 straipsnį tikslais laisva valia duodamas informuoto asmens sutikimas iš subjektų turi būti gautas prieš jiems pradedant dalyvauti tokiame bandyme ir tik juos tinkamai informavus pateikiant glaustą, aiškią, aktualią ir suprantamą informaciją apie:

   a) bandymo realiomis sąlygomis pobūdį ir tikslus bei galimus nepatogumus, kurie gali būti susiję su jų dalyvavimu;

   b) sąlygas, kuriomis turi būti atliekamas bandymas realiomis sąlygomis, įskaitant numatomą subjekto (-ų) dalyvavimo trukmę;

   c) subjektų teises ir garantijas, susijusias su jų dalyvavimu, visų pirma jų teisę atsisakyti dalyvauti ir teisę bet kuriuo metu pasitraukti iš bandymo realiomis sąlygomis nepatiriant jokios žalos ir neprivalant pateikti pagrindimo;

   d) prašymo atšaukti DI sistemos predikcijas, rekomendacijas ar sprendimus arba į juos neatsižvelgti pateikimo tvarką;

   e) bandymo realiomis sąlygomis visoje Sąjungoje taikomą vienintelį unikalųjį identifikacinį numerį pagal 60 straipsnio 4 dalies c punktą ir tiekėjo arba jo teisinio atstovo, iš kurio galima gauti papildomos informacijos, kontaktinius duomenis.

2. Informuoto asmens sutikime turi būti nurodyta data ir jis įforminamas dokumentu, o subjektams arba jų teisiniams atstovams pateikiama šio dokumento kopija.

62 straipsnis

Tiekėjams ir diegėjams, ypač MVĮ, įskaitant startuolius, taikomos priemonės

1. Valstybės narės imasi šių veiksmų:

a) suteikia MVĮ, įskaitant startuolius, kurios Sąjungoje turi registruotą buveinę arba filialą, pirmenybę dalyvauti apribotose bandomosiose DI reglamentavimo aplinkose, jei jos tenkina tinkamumo sąlygas ir atrankos kriterijus; ši pirmenybė dalyvauti nekliudo kitoms MVĮ, įskaitant startuolius, kurios nėra šioje dalyje nurodytos įmonės, taip pat dalyvauti apribotoje bandomojoje DI reglamentavimo aplinkoje, jei jos taip pat atitinka tinkamumo sąlygas ir atrankos kriterijus;

b) organizuoja specialią informuotumo apie šio reglamento taikymą didinimo ir mokymo šia tema veiklą, specialiai pritaikytą MVĮ, įskaitant startuolius, diegėjų ir atitinkamai vietos valdžios institucijų poreikiams;

c) naudoja esamus specialius kanalus ir, kai tinkama, sukuria naujus kanalus ryšiams su MVĮ, įskaitant startuolius, diegėjais, kitais novatoriais ir atitinkamai vietos valdžios institucijomis, kad būtų teikiamos konsultacijos ir atsakoma į užklausas dėl šio reglamento įgyvendinimo, be kita ko, dėl dalyvavimo apribotose bandomosiose DI reglamentavimo aplinkose;

d) sudaro palankesnes sąlygas MVĮ ir kitiems atitinkamiems suinteresuotiesiems subjektams dalyvauti standartų rengimo procese.

2. Nustatant rinkliavas už 43 straipsnyje nurodytą atitikties vertinimą atsižvelgiama į konkrečius tiekėjų, kurie yra MVĮ, įskaitant startuolius, interesus ir poreikius; šios rinkliavos proporcingai sumažinamos atsižvelgiant į jų dydį, rinkos dydį ir kitus atitinkamus rodiklius.

3. DI tarnyba imasi šių veiksmų:

a) pateikia standartinius šablonus, skirtus sritims, kurioms taikomas šis reglamentas, kaip savo prašyme nurodė Valdyba;

b) sukuria ir tvarko bendrą informacinę platformą, kurioje visiems veiklos vykdytojams visoje Sąjungoje būtų teikiama lengvai naudojama su šiuo reglamentu susijusi informacija;

c) rengia atitinkamas komunikacijos kampanijas, skirtas informuotumui apie iš šio reglamento kylančias pareigas didinti;

d) vertina ir skatina su DI sistemomis susijusių viešųjų pirkimų procedūrų geriausios praktikos konvergenciją.

63 straipsnis

Konkretiems veiklos vykdytojams taikomos nukrypti leidžiančios nuostatos

1. Labai mažos įmonės, kaip tai suprantama Rekomendacijoje 2003/361/EB, tam tikrų kokybės valdymo sistemos, kurios reikalaujama pagal šio reglamento 17 straipsnį, elementų gali laikytis supaprastintai, su sąlyga, kad jos neturi įmonių partnerių arba susijusių įmonių, kaip tai suprantama toje rekomendacijoje. Tuo tikslu Komisija parengia gaires dėl kokybės valdymo sistemos elementų, kurių gali būti laikomasi supaprastintai, atsižvelgiant į labai mažų įmonių poreikius, nedarant poveikio apsaugos lygiui ar poreikiui laikytis reikalavimų, susijusių su didelės rizikos DI sistemomis.

2. Šio straipsnio 1 dalis negali būti suprantama taip, kad tie veiklos vykdytojai atleidžiami nuo kitų šiame reglamente nustatytų reikalavimų ir pareigų vykdymo, įskaitant 9, 10, 11, 12, 13, 14, 15, 72 ir 73 straipsniuose nustatytus reikalavimus ir pareigas.

VII skyrius
Valdymas

1 SKIRSNIS
VALDYMAS SĄJUNGOS LYGMENIU

64 straipsnis

DI tarnyba

1. Komisija per DI tarnybą plėtoja Sąjungos ekspertines žinias ir pajėgumus DI srityje.

2. Valstybės narės sudaro palankesnes sąlygas vykdyti DI tarnybai pavestas užduotis, kaip nurodyta šiame reglamente.

65 straipsnis

Europos dirbtinio intelekto valdybos įsteigimas ir struktūra

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

2. Valdybą sudaro po vieną kiekvienos valstybės narės atstovą. Stebėtojo teisėmis joje dalyvauja Europos duomenų apsaugos priežiūros pareigūnas. Valdybos posėdžiuose taip pat dalyvauja DI tarnyba, tačiau ji nedalyvauja balsuojant. Į Valdybos posėdžius kiekvienu konkrečiu atveju gali būti kviečiamos kitos nacionalinės ir Sąjungos institucijos, įstaigos ar ekspertai, jei aptariami klausimai yra jiems aktualūs.

3. Kiekvieną atstovą valstybė narė skiria trejų metų laikotarpiui, kuris gali būti pratęstas vieną kartą.

4. Valstybės narės užtikrina, kad jų atstovai Valdyboje:

   a) savo valstybėje narėje turėtų atitinkamą kompetenciją ir įgaliojimus, kad galėtų aktyviai prisidėti prie 66 straipsnyje nurodytų Valdybos užduočių vykdymo;

   b) būtų paskirti ryšių su Valdyba palaikymo vienu bendru kontaktiniu punktu ir, kai tinkama, atsižvelgiant į valstybių narių poreikius, ryšių su suinteresuotaisiais subjektais palaikymo vienu bendru kontaktiniu punktu;

   c) būtų įgalioti palengvinti savo valstybės narės nacionalinių kompetentingų institucijų veiklos nuoseklumo ir koordinavimo užtikrinimą, kiek tai susiję su šio reglamento įgyvendinimu, be kita ko, rinktų atitinkamus duomenis ir informaciją, kad galėtų vykdyti savo užduotis Valdyboje.

5. Paskirti valstybių narių atstovai Valdybos darbo tvarkos taisykles priima dviejų trečdalių balsų dauguma. Darbo tvarkos taisyklėse visų pirma nustatoma atrankos proceso tvarka, įgaliojimų trukmė ir pirmininko užduočių specifikacijos, išsami balsavimo tvarka ir Valdybos bei jos pogrupių veiklos organizavimas.

6. Valdyba įsteigia du nuolatinius pogrupius, kad būtų suteikta platforma rinkos priežiūros institucijų bendradarbiavimui ir keitimuisi informacija, o notifikuojančioms institucijoms būtų pranešama apie klausimus, susijusius su atitinkamai rinkos priežiūros ir notifikuotosiomis įstaigomis.

Nuolatinis rinkos priežiūros pogrupis turėtų veikti kaip administracinio bendradarbiavimo šio reglamento tikslais grupė, kaip tai suprantama Reglamento (ES) 2019/1020 30 straipsnyje.

Valdyba atitinkamai gali sudaryti kitus nuolatinius ar laikinuosius pogrupius konkretiems klausimams nagrinėti. Kai tinkama, į tokius pogrupius arba į konkrečius tų pogrupių posėdžius stebėtojų teisėmis gali būti kviečiami 67 straipsnyje nurodyto patariamojo forumo atstovai.

7. Valdybos veikla organizuojama ir ji veikia taip, kad būtų užtikrintas jos veiklos objektyvumas ir nešališkumas.

8. Valdybai pirmininkauja vienas iš valstybių narių atstovų. DI tarnyba teikia Valdybai sekretoriato paslaugas, pirmininko prašymu sušaukia posėdžius ir parengia darbotvarkę atsižvelgdama į Valdybos užduotis pagal šį reglamentą ir jos darbo tvarkos taisykles.

66 straipsnis

Valdybos užduotys

Valdyba konsultuoja Komisiją ir valstybes nares ir joms padeda, kad būtų palengvintas nuoseklus ir veiksmingas šio reglamento taikymas. Tuo tikslu Valdyba visų pirma gali:

a) prisidėti prie nacionalinių kompetentingų institucijų, atsakingų už šio reglamento taikymą, veiklos koordinavimo ir, bendradarbiaudama su atitinkamomis rinkos priežiūros institucijomis ir gavusi jų sutikimą, remti 74 straipsnio 11 dalyje nurodytą bendrą rinkos priežiūros institucijų veiklą;

b) rinkti technines ir su reglamentavimu susijusias ekspertines žinias bei geriausios praktikos pavyzdžius ir jais dalytis su valstybėmis narėmis;

c) teikti konsultacijas dėl šio reglamento įgyvendinimo, visų pirma dėl bendrosios paskirties DI modeliams skirtų taisyklių vykdymo užtikrinimo;

d) prisidėti derinant valstybių narių administracinę praktiką, be kita ko, susijusią su nukrypti nuo 46 straipsnyje nurodytų atitikties vertinimo procedūrų leidžiančia nuostata,
DI apribotų bandomųjų reglamentavimo aplinkų veikimu ir bandymu realiomis sąlygomis, kaip nurodyta 57, 59 ir 60 straipsniuose;

e) Komisijos prašymu arba savo iniciatyva skelbti rekomendacijas ir rašytines nuomones dėl visų aktualių klausimų, susijusių su šio reglamento įgyvendinimu ir nuosekliu bei veiksmingu jo taikymu, be kita ko:

i) dėl elgesio kodeksų ir praktikos kodeksų, taip pat Komisijos gairių rengimo ir taikymo pagal šį reglamentą;

ii) dėl šio reglamento vertinimo ir peržiūros pagal 112 straipsnį, be kita ko, kiek tai susiję su 73 straipsnyje nurodytais pranešimais apie rimtus incidentus, ir dėl 71 straipsnyje nurodytos ES duomenų bazės veikimo, deleguotųjų arba įgyvendinimo aktų rengimo ir dėl galimo šio reglamento suderinimo su I priede išvardytais Sąjungos derinimo teisės aktais;

iii) dėl techninių specifikacijų arba esamų standartų, susijusių su III skyriaus 2 skirsnyje nustatytais reikalavimais;

iv) dėl 40 ir 41 straipsniuose nurodytų darniųjų standartų arba bendrųjų specifikacijų naudojimo;

v) dėl tendencijų, pavyzdžiui, Europos pasaulinio konkurencingumo DI srityje, DI diegimo Sąjungoje ir skaitmeninių įgūdžių ugdymo;

vi) dėl tendencijų, susijusių su kintančia DI vertės grandinių tipologija, visų pirma dėl su tuo susijusių pasekmių atsakomybei;

vii) dėl galimo poreikio pagal 7 straipsnį iš dalies pakeisti III priedą ir dėl galimo poreikio laikantis 112 straipsnio galimai peržiūrėti 5 straipsnį, atsižvelgiant į atitinkamus turimus faktinius duomenis ir naujausius technologinius pokyčius;

f) remti Komisiją skatinant visuomenės informuotumą ir supratimą apie DI sistemų naudojimo naudą, jų riziką, su jomis susijusias apsaugos priemones ir teises bei pareigas;

g) sudaryti palankesnes sąlygas parengti bendrus kriterijus ir plėtoti bendrą rinkos dalyvių ir kompetentingų institucijų supratimą apie atitinkamas šiame reglamente numatytas sąvokas, be kita, prisidėti prie lyginamųjų parametrų rengimo;

h) atitinkamai bendradarbiauti su kitomis Sąjungos institucijomis, įstaigomis, organais ir agentūromis, taip pat atitinkamomis Sąjungos ekspertų grupėmis ir tinklais, visų pirma gaminių saugos, kibernetinio saugumo, konkurencijos, skaitmeninių ir žiniasklaidos paslaugų, finansinių paslaugų, vartotojų apsaugos, duomenų ir pagrindinių teisių apsaugos srityse;

i) prisidėti prie veiksmingo bendradarbiavimo su trečiųjų valstybių kompetentingomis institucijomis ir tarptautinėmis organizacijomis;

j) padėti nacionalinėms kompetentingoms institucijoms ir Komisijai plėtoti organizacines ir technines ekspertines žinias, reikalingas šiam reglamentui įgyvendinti, be kita ko, prisidėti vertinant valstybių narių darbuotojų, dalyvaujančių įgyvendinant šį reglamentą, mokymo poreikius;

k) padėti DI tarnybai remti nacionalines kompetentingas institucijas kuriant ir plėtojant DI apribotas bandomąsias reglamentavimo aplinkas ir sudaryti palankesnes sąlygas bendradarbiavimui ir dalijimuisi informacija tokiose aplinkose;

l) prisidėti prie rekomendacinių dokumentų rengimo ir teikti atitinkamas konsultacijas šiuo klausimu;

m) konsultuoti Komisiją tarptautiniais su DI susijusiais klausimais;

n) teikti nuomones Komisijai dėl kvalifikuotų perspėjimų dėl bendrosios paskirties DI modelių;

o) gauti valstybių narių nuomones apie kvalifikuotus perspėjimus dėl bendrosios paskirties DI modelių ir apie nacionalinę patirtį bei praktiką DI sistemų, visų pirma sistemų, į kuriais yra integruota bendrosios paskirties DI modelių, stebėsenos ir joms taikomų reikalavimų vykdymo užtikrinimo srityse.

67 straipsnis

Patariamasis forumas

1. Įsteigiamas patariamasis forumas, kurio paskirtis – teikti technines ekspertines žinias ir konsultuoti Valdybą bei Komisiją ir prisidėti prie jų užduočių pagal šį reglamentą vykdymo.

2. Patariamojo forumo nariais yra subalansuotai atrinkta suinteresuotųjų subjektų, įskaitant pramonės atstovus, startuolius, MVĮ, pilietinės visuomenės ir akademinės bendruomenės atstovus, grupė. Patariamajame forume subalansuotai atstovaujama komerciniams ir nekomerciniams interesams, o komercinių interesų kategorijoje – MVĮ ir kitoms įmonėms.

3. Komisija, laikydamasi 2 dalyje nustatytų kriterijų, skiria patariamojo forumo narius iš pripažintų ekspertinių žinių DI srityje turinčių suinteresuotųjų subjektų.

4. Patariamojo forumo nariai skiriami dvejų metų kadencijai, kuri gali būti pratęsta ne ilgesniam kaip ketverių metų laikotarpiui.

5. Pagrindinių teisių agentūra, ENISA, Europos standartizacijos komitetas (CEN), Europos elektrotechnikos standartizacijos komitetas (CENELEC) ir Europos telekomunikacijų standartų institutas (ETSI) yra nuolatiniai patariamojo forumo nariai.

6. Patariamasis forumas parengia savo darbo tvarkos taisykles. Jis iš savo narių išrenka du bendrapirmininkius pagal 2 dalyje nustatytus kriterijus. Bendrapirmininkiai skiriami dvejų metų kadencijai, kuri gali būti pratęsta vieną kartą.

7. Patariamasis forumas rengia posėdžius bent du kartus per metus. Patariamasis forumas į savo posėdžius gali kviesti ekspertus ir kitus suinteresuotuosius subjektus.

8. Valdybos arba Komisijos prašymu patariamasis forumas gali rengti nuomones, rekomendacijas ir rašytines pastabas.

9. Patariamasis forumas atitinkamai gali sudaryti nuolatinius arba laikinuosius pogrupius konkretiems su šio reglamento tikslais susijusiems klausimams nagrinėti.

10. Patariamasis forumas parengia metinę savo veiklos ataskaitą. Ši ataskaita skelbiama viešai.

68 straipsnis

Nepriklausomų ekspertų mokslinė komisija

1. Komisija įgyvendinimo aktu priima nuostatas dėl nepriklausomų ekspertų mokslinės komisijos (toliau – mokslinė komisija), kuriai pavesta remti vykdymo užtikrinimo veiklą pagal šį reglamentą, įsteigimo. Tas įgyvendinimo aktas priimamas laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

2. Mokslinę komisiją sudaro ekspertai, kuriuos Komisija atrenka remdamasi jų naujausiomis mokslinėmis ar techninėmis ekspertinėmis žiniomis DI srityje, kurių reikia 3 dalyje nustatytoms užduotims atlikti, ir kurie gali įrodyti, kad atitinka visas šias sąlygas:

   a) turi specialių ekspertinių žinių ir kompetencijos ir mokslinių ar techninių ekspertinių žinių DI srityje;

   b) yra nepriklausomi nuo DI sistemų ar bendrosios paskirties DI modelių tiekėjų;

   c) sugeba savo veiklą vykdyti kruopščiai, tiksliai ir objektyviai.

   Komisija, konsultuodamasi su Valdyba, nustato ekspertų skaičių komisijoje, atsižvelgdama į būtinus poreikius, ir užtikrina teisingą lyčių ir geografinį atstovavimą.

3. Mokslinė komisija konsultuoja ir remia DI tarnybą ir jai padeda, visų pirma vykdant šias užduotis:

a) remiant šio reglamento įgyvendinimą ir vykdymo užtikrinimą, kiek tai susiję su bendrosios paskirties DI modeliais ir sistemomis, visų pirma:

i) pagal 90 straipsnį teikia perspėjimus DI tarnybai apie galimą bendrosios paskirties DI modelių Sąjungos lygmens sisteminę riziką;

ii) prisideda prie priemonių ir metodikų, skirtų bendrosios paskirties DI modelių ir sistemų pajėgumams vertinti (be kita ko, panaudojant lyginamuosius parametrus), rengimo;

iii) teikia konsultacijas dėl sisteminės rizikos bendrosios paskirties DI modelių klasifikavimo;

iv) teikia konsultacijas dėl įvairių bendrosios paskirties DI modelių ir sistemų klasifikavimo;

v) prisideda prie priemonių ir šablonų kūrimo;

b) rinkos priežiūros institucijų prašymu remiant jų darbą;

c) remiant tarpvalstybinę rinkos priežiūros veiklą, nurodytą 74 straipsnio 11 dalyje, nedarant poveikio rinkos priežiūros institucijų įgaliojimams;

d) remiant DI tarnybą, jai vykdant savo pareigas pagal 81 straipsnį nustatytos Sąjungos apsaugos procedūros kontekste.

4. Mokslinės komisijos ekspertai savo užduotis vykdo nešališkai bei objektyviai ir užtikrina informacijos ir duomenų, gautų vykdant savo užduotis ir veiklą, konfidencialumą. Vykdydami savo užduotis pagal 3 dalį, jie nesiekia gauti ir nepriima jokių nurodymų. Kiekvienas ekspertas parengia interesų deklaraciją, kuri paskelbiama viešai. DI tarnyba nustato sistemas ir procedūras, kuriomis būtų aktyviai valdomi galimi interesų konfliktai ir jiems užkertamas kelias.

5. Į 1 dalyje nurodytą įgyvendinimo aktą įtraukiamos nuostatos dėl sąlygų, procedūrų ir išsamios tvarkos, pagal kurias mokslinė komisija ir jos nariai skelbia perspėjimus ir prašo DI tarnybos pagalbos mokslinės komisijos užduočių vykdymui.

69 straipsnis

Valstybių narių galimybės naudotis ekspertų rezervu

1. Valstybės narės gali kreiptis į mokslinės komisijos ekspertus, kad jie padėtų užtikrinti veiklos pagal šį reglamentą vykdymą.

2. Gali būti reikalaujama, kad valstybės narės mokėtų rinkliavas už ekspertų teikiamas konsultacijas ir paramą. Rinkliavų struktūra ir dydis, taip pat atlygintinų išlaidų dydis ir struktūra nustatomi 68 straipsnio 1 dalyje nurodytame įgyvendinimo akte, atsižvelgiant į tinkamo šio reglamento įgyvendinimo tikslus, išlaidų efektyvumą ir būtinybę užtikrinti, kad visos valstybės narės galėtų veiksmingai naudotis ekspertų paslaugomis.

3. Komisija sudaro palankesnes sąlygas valstybėms narėms prireikus laiku pasinaudoti ekspertų paslaugomis ir užtikrina, kad Sąjungos DI bandymų pagalbinių struktūrų pagal 84 straipsnį ir ekspertų pagal šį straipsnį vykdomos paramos veiklos derinimas būtų organizuojamas veiksmingai ir suteiktų kuo didesnės pridėtinės vertės.

2 SKIRSNIS

NACIONALINĖS KOMPETENTINGOS INSTITUCIJOS

70 straipsnis

Nacionalinių kompetentingų institucijų ir vieno bendro kontaktinio punkto skyrimas

1. Kiekviena valstybė narė šio reglamento tikslais įsteigia arba paskiria nacionalinėmis kompetentingomis institucijomis bent vieną notifikuojančiąją instituciją ir bent vieną rinkos priežiūros instituciją. Tos nacionalinės kompetentingos institucijos naudojasi savo įgaliojimais nepriklausomai, nešališkai ir netendencingai, kad apsaugotų savo veiklos bei užduočių objektyvumą ir užtikrintų šio reglamento taikymą ir įgyvendinimą. Tų institucijų nariai susilaiko nuo bet kokių su jų pareigomis nesuderinamų veiksmų. Su sąlyga, kad laikomasi šių principų, atsižvelgiant į valstybės narės organizacinius poreikius tokią veiklą ir užduotis gali vykdyti viena ar daugiau paskirtųjų institucijų.

2. Valstybės narės praneša Komisijai notifikuojančiųjų institucijų ir rinkos priežiūros institucijų pavadinimus ir tų institucijų užduotis, taip pat visus vėlesnius jų pakeitimus. Valstybės narės ne vėliau kaip … [12 mėnesių nuo šio reglamento įsigaliojimo dienos] elektroninėmis ryšio priemonėmis viešai paskelbia informaciją apie tai, kaip galima susisiekti su kompetentingomis institucijomis ir bendrais kontaktiniais punktais. Valstybės narės šio reglamento tikslais vieną rinkos priežiūros instituciją paskiria vienu bendru kontaktiniu punktu ir praneša Komisijai to vieno bendro kontaktinio punkto pavadinimą. Komisija tokių bendrų kontaktinių punktų sąrašą paskelbia viešai.

3. Valstybės narės užtikrina, kad jų nacionalinėms kompetentingoms institucijoms būtų suteikta pakankamai techninių, finansinių ir žmogiškųjų išteklių ir būtų suteikta infrastruktūra jų užduotims pagal šį reglamentą veiksmingai vykdyti. Visų pirma, nacionalinės kompetentingos institucijos turi nuolat turėti pakankamai darbuotojų, kurių kompetencija ir ekspertinės žinios apimtų išsamų DI technologijų, duomenų ir duomenų kompiuterijos, asmens duomenų apsaugos, kibernetinio saugumo, pagrindinių teisių, rizikos sveikatai ir saugai, taip pat esamų standartų bei teisinių reikalavimų išmanymą. Valstybės narės kasmet įvertina ir, prireikus, atnaujina šioje dalyje nurodytus su kompetencija ir ištekliais susijusius reikalavimus.

4. Nacionalinės kompetentingos institucijos imasi tinkamų priemonių užtikrinti tinkamam kibernetinio saugumo lygiui.

5. Vykdydamos savo užduotis, nacionalinės kompetentingos institucijos laikosi 78 straipsnyje nustatytų konfidencialumo pareigų.

6. Ne vėliau kaip … [vieni metai nuo šio reglamento įsigaliojimo dienos], o vėliau – kartą per dvejus metus valstybės narės praneša Komisijai apie nacionalinių kompetentingų institucijų finansinių ir žmogiškųjų išteklių būklę ir pateikia jų tinkamumo įvertinimą. Komisija šią informaciją perduoda Valdybai aptarti ir galimoms rekomendacijoms pateikti.

7. Komisija padeda nacionalinėms kompetentingoms institucijoms keistis patirtimi.

8. Nacionalinės kompetentingos institucijos gali teikti gaires ir patarimus dėl šio reglamento įgyvendinimo, visų pirma MVĮ, įskaitant startuolius, atitinkamai atsižvelgdamos į Valdybos ir Komisijos gaires ir patarimus. Kai nacionalinės kompetentingos institucijos ketina DI sistemos atžvilgiu pateikti gairių ir patarimų srityse, kurioms taikoma kiti Sąjungos teisės aktai, atitinkamai pagal tuos Sąjungos teisės aktus konsultuojamasi su nacionalinėmis kompetentingomis institucijomis.

9. Kai šis reglamentas taikomas Sąjungos institucijoms, įstaigoms, organams ar agentūroms, jų priežiūros tikslu kompetentingos institucijos funkcijas vykdo Europos duomenų apsaugos priežiūros pareigūnas.

VIII skyrius

Didelės rizikos DI sistemų ES duomenų bazė

71 straipsnis

III priede išvardytų didelės rizikos DI sistemų ES duomenų bazė

1. Komisija, bendradarbiaudama su valstybėmis narėmis, sukuria ir tvarko ES duomenų bazę, kurioje saugoma šio straipsnio 2 ir 3 dalyse nurodyta informacija, susijusi su 6 straipsnio 2 dalyje nurodytomis pagal 49 ir 60 straipsnius užregistruotomis didelės rizikos DI sistemomis ir DI sistemomis, kurios pagal 6 straipsnio 3 dalį nelaikomos didelės rizikos DI sistemomis ir kurios yra užregistruotos pagal 6 straipsnio 4 dalį ir 49 straipsnį. Nustatydama tokios duomenų bazės funkcines specifikacijas, Komisija konsultuojasi su atitinkamais ekspertais, o atnaujindama tokios duomenų bazės funkcines specifikacijas – su Valdyba.

2. VIII priedo A ir B skirsniuose išvardytus duomenis į ES duomenų bazę įveda tiekėjas arba, kai taikytina, įgaliotas atstovas.

3. VIII priedo C skirsnyje išvardytus duomenis į ES duomenų bazę įveda diegėjas, kuris yra valdžios institucija, agentūra ar įstaiga arba kuris veikia jų vardu, pagal 49 straipsnio 3 ir 4 dalis.

4. Išskyrus 49 straipsnio 4 dalyje ir 60 straipsnio 4 dalies c punkte nurodytą skirsnį, su ES duomenų bazėje saugoma informacija, užregistruota pagal 49 straipsnį, turi būti galima vartotojui patogiu būdu susipažinti ir ji turi būti skelbiama viešai. Informacija turėtų būti lengvai naršoma ir kompiuterio nuskaitoma. Pagal 60 straipsnį užregistruota informacija yra prieinama tik rinkos priežiūros institucijoms ir Komisijai, išskyrus atvejus, kai galimas tiekėjas ar tiekėjas yra davęs sutikimą, kad ši informacija būtų prieinama viešai.

5. ES duomenų bazėje saugomi tik tie 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 atitinkamai tiekėjui arba diegėjui, vardus bei pavardes ir kontaktinius duomenis.

6. Komisija yra ES duomenų bazės valdytoja. Ji teikia tiekėjams, galimiems tiekėjams ir diegėjams tinkamą techninę ir administracinę paramą. ES duomenų bazė turi atitikti taikomus prieinamumo reikalavimus.

IX skyrius
Priežiūra po pateikimo rinkai, dalijimasis informacija ir rinkos priežiūra

1 SKIRSNIS
PRIEŽIŪRA PO PATEIKIMO RINKAI

72 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 jos duomenis dokumentuoja tokiu būdu, kuris yra proporcingas DI technologijų pobūdžiui ir didelės rizikos DI sistemos keliamai rizikai.

2. Naudojantis priežiūros po pateikimo rinkai sistema aktyviai ir sistemingai renkami, dokumentuojami ir analizuojami atitinkami duomenys, kuriuos gali teikti diegėjai arba kurie gali būti renkami naudojantis kitais informacijos apie didelės rizikos DI sistemų veikimo efektyvumą šaltiniais visą jų gyvavimo laikotarpį ir kurie sudaro sąlygas tiekėjui įvertinti, ar DI sistemos nuolat atitinka III skyriaus 2 skirsnyje nustatytus reikalavimus. Kai aktualu, stebėsena po pateikimo rinkai apima sąveikos su kitomis DI sistemomis analizę. Ši pareiga netaikoma diegėjų, kurie yra teisėsaugos institucijos, neskelbtiniems operatyviniams duomenims.

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 ne vėliau kaip … [18 mėnesių nuo šio reglamento įsigaliojimo dienos] priima įgyvendinimo aktą, kuriame nustatomos išsamios nuostatos dėl priežiūros po pateikimo rinkai plano šablono ir į planą įtrauktinų elementų sąrašo. Tas įgyvendinimo aktas priimamas laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

4. Didelės rizikos DI sistemų, kurioms taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, atveju, jeigu pagal tuos teisės aktus priežiūros po pateikimo rinkai sistema jau yra įdiegta, o planas jau yra parengtas, siekiant užtikrinti nuoseklumą, išvengti veiksmų dubliavimosi ir kuo labiau sumažinti papildomą naštą, tiekėjai, naudodamiesi 3 dalyje nurodytą šablonu, gali pasirinkti į pagal tuos teisės aktus jau sukurtas sistemas ir parengtus planus atitinkamai integruoti 1, 2 ir 3 dalyse apibūdintus būtinus elementus, su sąlyga, kad taip bus užtikrintas lygiavertis apsaugos lygis.

Pirma šios dalies pastraipa taip pat taikoma III priedo 5 punkte nurodytoms didelės rizikos DI sistemoms, kurias rinkai pateikė arba pradėjo naudoti finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi reikalavimai, susiję su jų vidaus valdymu, tvarka ar procesais.

2 SKIRSNIS

DALIJIMASIS INFORMACIJA APIE RIMTUS INCIDENTUS

73 straipsnis

Pranešimas apie rimtus incidentus

1. DI sistemas Sąjungos rinkai pateikiantys tiekėjai valstybių narių, kuriose įvyko rimtas incidentas, rinkos priežiūros institucijoms praneša apie visus tokius incidentus.

2. 1 dalyje nurodytas pranešimas pateikiamas iškart po to, kai tiekėjas nustato priežastinį ryšį tarp DI sistemos ir rimto incidento arba pagrįstą tokio ryšio tikimybę, ir bet kuriuo atveju ne vėliau kaip per 15 dienų po to, kai tiekėjas arba, kai taikytina, diegėjas sužino apie rimtą incidentą.

   Nustatant pirmoje pastraipoje nurodytą pranešimo laikotarpį atsižvelgiama į rimto incidento sunkumą.

3. Nepaisant šio straipsnio 2 dalies, plačiai paplitusio pažeidimo arba rimto incidento, kaip apibrėžta 3 straipsnio 49 punkto b papunktyje, atveju šio straipsnio 1 dalyje nurodyta ataskaita pateikiama iškart, ir ne vėliau kaip dvi dienos nuo tada, kai tiekėjas arba, kai taikoma, diegėjas sužino apie incidentą.

4. Nepaisant 2 dalies, asmens mirties atveju pranešimas pateikiamas iš karto po to, kai tiekėjas arba diegėjas nustato arba įtaria didelės rizikos DI sistemos ir rimto incidento priežastinį ryšį, tai padaroma ne vėliau kaip per 10 dienų nuo tos dienos, kai tiekėjas arba, kai taikytina, diegėjas sužino apie rimtą incidentą.

5. Kai tai būtina siekiant užtikrinti, kad pranešimai būtų pateikiami laiku, tiekėjas arba, kai taikytina, diegėjas gali pateikti pradinį neišsamų pranešimą, o vėliau – išsamų pranešimą.

6. Pranešęs apie rimtą incidentą pagal 1 dalį, tiekėjas nedelsdamas atlieka būtinus tyrimus, susijusius su rimtu incidentu ir atitinkama DI sistema. Tai apima incidento rizikos vertinimą ir taisomuosius veiksmus.

   Atlikdamas pirmoje pastraipoje nurodytus tyrimus tiekėjas bendradarbiauja su kompetentingomis institucijomis ir, kai aktualu, su atitinkama notifikuotąja įstaiga ir, prieš tai neinformavęs kompetentingų institucijų apie tokius veiksmus, neatlieka jokių tyrimų, kurių metu atitinkama DI sistema būtų pakeista taip, kad tai galėtų turėti įtakos vėlesniam incidento priežasčių vertinimui.

7. Gavusi pranešimą, susijusį su 3 straipsnio 49 punkto c papunktyje nurodytu rimtu incidentu, atitinkama rinkos priežiūros institucija informuoja 77 straipsnio 1 dalyje nurodytas nacionalines valdžios institucijas ar įstaigas. Siekdama palengvinti šio straipsnio 1 dalyje nustatytų pareigų vykdymą Komisija parengia specialias gaires. Tos gairės priimamos ne vėliau kaip … [12 mėnesių nuo šio reglamento įsigaliojimo dienos] ir reguliariai vertinamos.

8. Rinkos priežiūros institucija per septynias dienas nuo šio straipsnio 1 dalyje nurodyto pranešimo gavimo dienos imasi tinkamų priemonių, kaip numatyta Reglamento (ES) 2019/1020 19 straipsnyje, ir laikosi tame reglamente nustatytų pranešimo procedūrų.

9. III priede nurodytų didelės rizikos DI sistemų, kurias rinkai pateikė arba pradėjo naudoti tiekėjai, kuriems taikomi Sąjungos teisė aktai, nustatantys pranešimo pareigas, lygiavertes nustatytoms šiame reglamente , atveju pranešama tik apie 3 straipsnio 49 punkto c papunktyje nurodytus rimtus incidentus.

10. Didelės rizikos DI sistemų, kurios yra prietaisų saugos komponentai arba kurios pačios yra prietaisai, kurioms taikomi reglamentai (ES) 2017/745 ir (ES) 2017/746, atveju pranešama tik apie šio reglamento 3 straipsnio 49 punkto c papunktyje nurodytus rimtus incidentus ir apie juos pranešama valstybių narių, kuriose įvyko incidentas, tuo tikslu pasirinktai nacionalinei kompetentingai institucijai.

11. Nacionalinės kompetentingos institucijos pagal Reglamento (ES) 2019/1020 20 straipsnį nedelsdamos praneša Komisijai apie kiekvieną rimtą incidentą nepriklausomai nuo to, ar jos ėmėsi veiksmų jo atžvilgiu.

3 SKIRSNIS

VYKDYMO UŽTIKRINIMAS

74 straipsnis

Sąjungos rinkoje esančių DI sistemų rinkos priežiūra ir kontrolė

1. DI sistemoms, kurios patenka į šio reglamento taikymo sritį, taikomas Reglamentas (ES) 2019/1020. Šio reglamento veiksmingo vykdymo užtikrinimo tikslais:

   a) visos nuorodos į ekonominės veiklos vykdytoją pagal Reglamentą (ES) 2019/1020 suprantamos kaip apimančios visus šio reglamento 2 straipsnio 1 dalyje nurodytus veiklos vykdytojus;

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

2. Vykdydamos savo pareigas pranešti pagal Reglamento (ES) 2019/1020 34 straipsnio 4 dalį, rinkos priežiūros institucijos kasmet praneša Komisijai ir atitinkamoms nacionalinėms konkurencijos institucijoms visą vykdant rinkos priežiūros veiklą nustatytą informaciją, kuri gali būti svarbi konkurencijos taisykles reglamentuojančių Sąjungos teisės aktų taikymui. Jos taip pat kasmet praneša Komisijai apie tais metais vykdytos draudžiamos praktikos atvejus ir apie priemones, kurių buvo imtasi.

3. Didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, atveju šio reglamento tikslais rinkos priežiūros institucija yra pagal tuos teisės aktus paskirta institucija, atsakinga už rinkos priežiūros veiklą.

Nukrypstant nuo pirmos pastraipos, esant tinkamoms aplinkybėms valstybės narės gali paskirti kitą atitinkamą instituciją veikti kaip rinkos priežiūros institucija, su sąlyga, kad jos užtikrins veiklos koordinavimą su atitinkamomis sektorių rinkos priežiūros institucijomis, atsakingomis už I priede išvardytų Sąjungos derinimo teisės aktų vykdymo užtikrinimą.

4. Šio reglamento 79–83 straipsniuose nurodytos procedūros netaikomos DI sistemoms, susijusioms su gaminiais, kuriems taikomi I priedo A skirsnyje išvardyti Sąjungos derinamieji teisės aktai, kai tokiuose teisės aktuose jau numatytos procedūros, kuriomis užtikrinamas lygiavertis apsaugos lygis arba kuriomis siekiama tokio paties tikslo. Tokiais atvejais taikomos atitinkamos sektorių procedūros.

5. Nedarant poveikio rinkos priežiūros institucijų įgaliojimams pagal Reglamento (ES) 2019/1020 14 straipsnį, veiksmingo šio reglamento vykdymo užtikrinimo tikslais rinkos priežiūros institucijos atitinkamai to reglamento 14 straipsnio 4 dalies d ir j punktuose nurodytais įgaliojimais gali naudotis nuotoliniu būdu.

6. Didelės rizikos DI sistemų, kurias rinkai pateikia, pradeda naudoti arba naudoja finansų įstaigos, kurias reglamentuoja Sąjungos finansinių paslaugų teisės aktai, atveju šio reglamento tikslais rinkos priežiūros institucija yra atitinkama nacionalinė institucija, atsakinga už tų įstaigų finansinę priežiūrą pagal tuos teisės aktus, tiek, kiek DI sistemos pateikimas rinkai, pradėjimas naudoti arba naudojimas yra tiesiogiai susijęs su tų finansinių paslaugų teikimu.

7. Nukrypstant nuo 6 dalies, atitinkamomis aplinkybėmis ir su sąlyga, kad bus užtikrinta veiklos koordinavimas, šio reglamento tikslais valstybė narė gali rinkos priežiūros institucija paskirti kitą atitinkamą instituciją.

Nacionalinės rinkos priežiūros institucijos, prižiūrinčios reguliuojamas kredito įstaigas, reglamentuojamas pagal Direktyvą 2013/36/ES, kurios dalyvauja bendrame priežiūros mechanizme, nustatytame Reglamentu (ES) Nr. 1024/2013, turėtų nedelsdamos pateikti Europos Centriniam Bankui visą vykdant rinkos priežiūros veiklą nustatytą informaciją, kuri gali būti svarbi Europos Centrinio Banko prudencinės priežiūros užduotims, nurodytoms tame reglamente.

8. Didelės rizikos DI sistemų, išvardytų šio reglamento III priedo 1 punkte atveju, tiek, kiek tos sistemos naudojamos teisėsaugos, sienų valdymo ir teisingumo ir demokratijos tikslais, taip pat didelės rizikos DI sistemų, išvardytų šio reglamento III priedo 6, 7 ir 8 punktuose, atveju valstybės narės šio reglamento tikslais rinkos priežiūros institucijomis paskiria kompetentingas duomenų apsaugos priežiūros institucijas pagal Reglamentą (ES) 2016/679 ar Direktyvą (ES) 2016/680 arba kitas institucijas, paskiriamos laikantis tų pačių sąlygų, kurios yra nustatytos Direktyvos (ES) 2016/680 41–44 straipsniuose. Rinkos priežiūros veikla jokiu būdu nedaro poveikio teisminių institucijų nepriklausomumui ar ja kitaip nesikišama į jų veiklą, kai jos vykdo teismines funkcijas.

9. Kai šis reglamentas taikomas Sąjungos institucijoms, įstaigoms, organams ar agentūroms, jų atžvilgiu rinkos priežiūros institucijos funkcijas vykdo Europos duomenų apsaugos priežiūros pareigūnas, išskyrus Europos Sąjungos Teisingumo Teismo, vykdančio savo teismines funkcijas, atvejį.

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

11. Rinkos priežiūros institucijos ir Komisija turi turėti galimybę pagal Reglamento (ES) 2019/1020 9 straipsnį pasiūlyti bendrą veiklą, įskaitant bendrus tyrimus, kurią vykdytų pačios rinkos priežiūros institucijos arba rinkos priežiūros institucijos kartu su Komisija ir kuria būtų siekiama skatinti atitiktį, nustatyti neatitikties atvejus, didinti informuotumą arba teikti su šiuo reglamentu susijusias gaires dėl konkrečių kategorijų didelės rizikos DI sistemų, kurios, kaip nustatyta, kelia didelę riziką dviejose ar daugiau valstybių narių. DI tarnyba padeda koordinuoti bendrus tyrimus.

12. Nedarant poveikio pagal Reglamentą (ES) 2019/1020 numatytiems įgaliojimams, kai aktualu, ir neviršijant to, kas būtina rinkos priežiūros institucijų užduotims atlikti, tiekėjai šioms institucijoms turi suteikti visapusišką prieigą prie dokumentų, taip pat didelės rizikos DI sistemų plėtojimui naudojamų mokymo, validavimo ir bandymo duomenų rinkinių, įskaitant, kai tinkama, ir taikant apsaugos priemones, taikomųjų programų sąsajas (API) arba kitas atitinkamas technines priemones ir įrankius, kurie sudaro sąlygas nuotolinei prieigai.

13. Prieigą prie didelės rizikos DI sistemos pirminio kodo rinkos priežiūros institucijoms tiekėjai suteikia gavę jų motyvuotą prašymą ir tik tada, kai tenkinamos abi šios sąlygos:

    a) prieiga prie pirminio kodo yra būtina siekiant įvertinti didelės rizikos DI sistemos atitiktį III skyriaus 2 skirsnyje nustatytiems reikalavimams ir

    b) nebeįmanoma atlikti kitų bandymo ir audito procedūrų ir patikrinimų, pagrįstų tiekėjo pateiktais duomenimis ir dokumentais, arba paaiškėjo, kad tokių procedūrų ir patikrinimų nepakanka.

14. Visa rinkos priežiūros institucijų gauta informacija ar dokumentai tvarkomi laikantis 78 straipsnyje nustatytų konfidencialumo pareigų.

75 straipsnis

Savitarpio pagalba, rinkos priežiūra ir bendrosios paskirties DI sistemų kontrolė

1. Kai DI sistema grindžiama bendrosios paskirties DI modeliu, o modelį bei sistemą yra sukūręs tas pats tiekėjas, DI tarnyba turi įgaliojimus stebėti ir prižiūrėti, kaip tos DI sistemos atžvilgiu laikomasi šiame reglamente nustatytų pareigų. Kad galėtų vykdyti savo stebėsenos ir priežiūros užduotis, DI tarnyba turi visus rinkos priežiūros institucijos įgaliojimus, numatytus šiame skirsnyje ir Reglamente (ES) 2019/1020.

2. Jei atitinkamos rinkos priežiūros institucijos turi pakankamą pagrindą manyti, kad bendrosios paskirties DI sistemos, kurias diegėjai gali tiesiogiai naudoti bent vienai paskirčiai, kuri pagal šį reglamentą priskiriama didelės rizikos kategorijai, neatitinka šiame reglamente nustatytų reikalavimų, jos bendradarbiauja su DI tarnyba, kad atliktų atitikties vertinimus, ir atitinkamai informuoja Valdybą ir kitas rinkos priežiūros institucijas.

3. Tais atvejais, kai rinkos priežiūros institucija negali užbaigti didelės rizikos DI sistemos tyrimo, nes negavo prieigos prie tam tikros su bendrosios paskirties DI modeliu susijusios informacijos, nors ir dėjo visas tinkamas pastangas tai informacijai gauti, ji gali pateikti DI tarnybai pagrįstą prašymą, kuriuo būtų užtikrinta prieiga prie tos informacijos. Tokiu atveju DI tarnyba nedelsdama ir bet kuriuo atveju per 30 dienų pateikia prašančiajai institucijai visą informaciją, kurią DI tarnyba laiko svarbia siekiant nustatyti, ar didelės rizikos DI sistema neatitinka reikalavimų. Rinkos priežiūros institucijos pagal šio reglamento 78 straipsnį užtikrina gautos informacijos konfidencialumą. *Mutatis mutandis* taikoma Reglamento (ES) 2019/1020 VI skyriuje numatyta procedūra.

76 straipsnis

Rinkos priežiūros institucijų vykdoma bandymo realiomis sąlygomis priežiūra

1. Rinkos priežiūros institucijos yra kompetentingos ir turi įgaliojimus užtikrinti, kad bandymas realiomis sąlygomis atitiktų šį reglamentą.

2. Kai bandymas realiomis sąlygomis atliekamas DI sistemų, kurios prižiūrimos apribotoje bandomojoje DI reglamentavimo aplinkoje pagal 58 straipsnį, atžvilgiu, rinkos priežiūros institucijos, vykdydamos apribotos bandomosios DI reglamentavimo aplinkos priežiūros funkciją, patikrina, ar laikomasi 60 straipsnio. Tos institucijos gali atitinkamai leisti, kad tiekėjas arba galimas tiekėjas bandymą realiomis sąlygomis atliktų nukrypdamas nuo 60 straipsnio 4 dalies f ir g punktuose nustatytų sąlygų.

3. Jei galimas tiekėjas, tiekėjas arba trečioji šalis rinkos priežiūros instituciją yra informavę apie rimtą incidentą arba jei ta institucija turi kitų motyvų manyti, kad nevykdomos 60 ir 61 straipsniuose nustatytos sąlygos, ji gali atitinkamai savo teritorijoje priimti bet kurį iš šių sprendimų:

   a) sustabdyti arba nutraukti bandymą realiomis sąlygomis;

   b) reikalauti, kad tiekėjas arba galimas tiekėjas ir diegėjas arba galimas diegėjas pakeistų bet kurį bandymo realiomis sąlygomis aspektą.

4. Jeigu rinkos priežiūros institucija yra priėmusi šio straipsnio 3 dalyje nurodytą sprendimą arba yra pareiškusi prieštaravimą, kaip tai suprantama 60 straipsnio 4 dalies b punkte, tame sprendime arba prieštaravime nurodomi motyvai ir tai, kaip tiekėjas arba galimas tiekėjas gali tą sprendimą arba prieštaravimą užginčyti.

5. Kai taikytina, kai rinkos priežiūros institucija priima 3 dalyje nurodytą sprendimą, ji praneša to sprendimo motyvus kitų valstybių narių, kuriose ta DI sistema buvo bandoma pagal bandymų planą, rinkos priežiūros institucijoms.

77 straipsnis

Pagrindines teises ginančių institucijų įgaliojimai

1. Nacionalinės valdžios institucijos arba įstaigos, prižiūrinčios, kaip vykdomos pareigos pagal Sąjungos teisės aktus dėl pagrindinių teisių, įskaitant teisę nebūti diskriminuojamiems, apsaugos, kai naudojamos III priede nurodytos didelės rizikos DI sistemos, arba užtikrinančios tų pareigų vykdymą, turi įgaliojimus prašyti prieigos prie visų pagal šį reglamentą parengtų ar saugomų dokumentų ir juos gauti suprantama kalba ir prieinamu formatu, kai prieiga prie tų dokumentų yra būtina jų įgaliojimams veiksmingai įgyvendinti laikantis jų jurisdikcijos ribų. Atitinkama valdžios institucija ar įstaiga apie tokį prašymą informuoja atitinkamos valstybės narės rinkos priežiūros instituciją.

2. Ne vėliau kaip … [trys mėnesiai nuo šio reglamento įsigaliojimo dienos] kiekviena valstybė narė identifikuoja 1 dalyje nurodytas valdžios institucijas ar įstaigas ir jų sąrašą paskelbia viešai . Valstybės narės pateikia sąrašą Komisijai bei kitoms valstybėms narėms ir nuolat jį atnaujina.

3. Jeigu 1 dalyje nurodytų dokumentų nepakanka, kad būtų galima įsitikinti, ar buvo nesilaikyta Sąjungos teisės aktuose, kuriais saugomos pagrindinės teisės, nustatytų pareigų, 1 dalyje nurodyta valdžios institucija arba įstaiga gali pateikti rinkos priežiūros institucijai motyvuotą prašymą organizuoti didelės rizikos DI sistemos bandymą techninėmis priemonėmis. Rinkos priežiūros institucija per pagrįstą laikotarpį po prašymo pateikimo suorganizuoja bandymą glaudžiai bendradarbiaudama su prašančiąja valdžios institucija ar įstaiga.

4. Visa informacija ar dokumentai, kuriuos šio straipsnio 1 dalyje nurodytos nacionalinės valdžios institucijos ar įstaigos gavo pagal šio straipsnio nuostatas, tvarkomi laikantis 78 straipsnyje nustatytų konfidencialumo pareigų.

78 straipsnis

Konfidencialumas

1. Komisija, rinkos priežiūros institucijos ir notifikuotosios įstaigos ir visi kiti fiziniai ar juridiniai asmenys, dalyvaujantys taikant šį reglamentą, pagal Sąjungos ar nacionalinės teisės aktus užtikrina informacijos ir duomenų, gautų vykdant jų užduotis ir veiklą, konfidencialumą, kad visų pirma būtų apsaugotos:

   a) intelektinės nuosavybės teisės ir fizinio ar juridinio asmens konfidenciali verslo informacija ar komercinės paslaptys, įskaitant pirminį kodą, išskyrus atvejus, nurodytus Europos Parlamento ir Tarybos direktyvos (ES) 2016/943[57] 5 straipsnyje;

   b) veiksmingas šio reglamento įgyvendinimas, visų pirma patikrinimų, tyrimų arba auditų tikslais;

   c) visuomenės ir nacionalinio saugumo interesai;

   d) baudžiamojo ar administracinio proceso vykdymas;

[57] 2016 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/943 dėl neatskleistos praktinės patirties ir verslo informacijos (komercinių paslapčių) apsaugos nuo neteisėto jų gavimo, naudojimo ir atskleidimo (OL L 157, 2016 6 15, p. 1).

e) pagal Sąjungos arba nacionalinės teisės aktus įslaptinta informacija.

2. Institucijos, dalyvaujančios taikant šį reglamentą pagal 1 dalį, prašo tik tų duomenų, kurie yra tikrai būtini DI sistemų keliamai rizikai įvertinti ir jų įgaliojimams vykdyti laikantis šio reglamento ir Reglamento (ES) 2019/1020. Jos įdiegia tinkamas ir veiksmingas kibernetinio saugumo priemones, kad būtų apsaugotas gautos informacijos bei duomenų saugumas ir konfidencialumas, o surinktus duomenis ištrina iškart, kai tik jie yra nebereikalingi tikslui, kuriuo jie buvo gauti, pagal taikytinus Sąjungos ar nacionalinės teisės aktus.

3. Nedarant poveikio 1 ir 2 dalims, informacija, kuria konfidencialiai keičiasi nacionalinės kompetentingos institucijos tarpusavyje arba su Komisija, neatskleidžiama iš anksto nepasikonsultavus su ją pateikusia nacionaline kompetentinga institucija ir diegėju, kai III priedo 1, 6 arba 7 punkte nurodytas didelės rizikos DI sistemas naudoja teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijos ir jei toks atskleidimas keltų grėsmę visuomenės ir nacionalinio saugumo interesams. Šis keitimasis informacija neapima neskelbtinų operatyvinių duomenų, susijusių su teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijų veikla.

Kai teisėsaugos, imigracijos ar prieglobsčio institucijos yra didelės rizikos DI sistemų, nurodytų III priedo 1, 6 ar 7 punkte, tiekėjos, IV priede nurodyti techniniai dokumentai turi likti tų institucijų patalpose. Tos institucijos užtikrina, kad, pateikusios prašymą, atitinkamai 74 straipsnio 8 ir 9 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.

4. 1, 2 ir 3 dalimis nedaromas poveikis Komisijos, valstybių narių ir atitinkamų jų institucijų, taip pat notifikuotųjų įstaigų teisėms ir pareigoms keistis informacija ir platinti įspėjimus, be kita ko, tarpvalstybinio bendradarbiavimo kontekste, taip pat nedaro poveikio atitinkamų šalių pareigoms teikti informaciją pagal valstybių narių baudžiamąją teisę.

5. Komisija ir valstybės narės, kai tai būtina, laikydamosi atitinkamų tarptautinių ir prekybos susitarimų nuostatų, gali keistis konfidencialia informacija su trečiųjų valstybių, su kuriomis jos yra sudariusios dvišalius arba daugiašalius konfidencialumo susitarimus, kuriais užtikrinamas reikiamas konfidencialumo lygis, reguliavimo institucijomis.

79 straipsnis

Nacionalinio lygmens procedūra, taikoma riziką keliančioms DI sistemoms

1. Riziką keliančios DI sistemos laikomos pavojų keliančiu gaminiu, kaip apibrėžta Reglamento (ES) 2019/1020 3 straipsnio 19 punkte, tiek, kiek jos kelia riziką asmenų sveikatai ar saugai arba pagrindinėms teisėms.

2. Jeigu valstybės narės rinkos priežiūros institucija turi pakankamo pagrindo manyti, kad DI sistema kelia 1 dalyje nurodytą riziką, ji atlieka atitinkamą DI sistemos vertinimą, kad nustatytų ar jos atžvilgiu laikomasi visų šiame reglamente nustatytų reikalavimų ir pareigų. Ypatingas dėmesys skiriamas DI sistemoms, keliančioms riziką pažeidžiamoms grupėms. Kai nustatoma rizika pagrindinėms teisėms, rinkos priežiūros institucija taip pat nedelsdama informuoja atitinkamas 77 straipsnio 1 dalyje nurodytas nacionalines valdžios institucijas ar įstaigas ir su jomis visapusiškai bendradarbiauja. Atitinkami veiklos vykdytojai prireikus bendradarbiauja su rinkos priežiūros institucija ir 77 straipsnio 1 dalyje nurodytomis kitomis nacionalinėmis valdžios institucijomis ar įstaigomis.

Jeigu atlikdama tą vertinimą rinkos priežiūros institucija arba, kai taikytina, rinkos priežiūros institucija, bendradarbiaudama su 77 straipsnio 1 dalyje nurodyta nacionaline valdžios institucija, nustato, kad DI sistemos atžvilgiu nesilaikoma šiame reglamente nustatytų reikalavimų ir pareigų, ji nepagrįstai nedelsdama pareikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų reikiamų taisomųjų veiksmų, kad būtų užtikrinta DI sistemos atitiktis, DI sistema būtų pašalinta iš rinkos arba ji būtų atšaukta per laikotarpį, kurį rinkos priežiūros institucija gali nustatyti, ir bet kuriuo atveju per trumpesnį nei 15 darbo dienų laikotarpį arba kaip numatyta atitinkamuose Sąjungos derinamuosiuose teisės aktuose.

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

3. Jei rinkos priežiūros institucija mano, kad reikalavimų nesilaikoma ne tik jos nacionalinėje teritorijoje, ji nepagrįstai nedelsdama informuoja Komisiją ir kitas valstybes nares apie vertinimo rezultatus ir veiksmus, kurių ji nurodė imtis veiklos vykdytojui.

4. Veiklos vykdytojas užtikrina, kad visų reikiamų taisomųjų veiksmų būtų imtasi visų atitinkamų DI sistemų, kurias jis pateikė Sąjungos rinkai, atžvilgiu.

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 pateikimas jos nacionalinei rinkai arba pradėjimas naudoti, gaminys arba atskira DI sistema būtų pašalinti iš rinkos arba atšaukti. Apie tokias priemones ta institucija nepagrįstai nedelsdama praneša Komisijai ir kitoms valstybėms narėms.

6. 5 dalyje nurodytame pranešime pateikiami visi turimi duomenys, visų pirma informacija, kurios reikia reikalavimų neatitinkančiai DI sistemai identifikuoti, DI sistemos ir vertės grandinės kilmė, įtariamo reikalavimų nesilaikymo ir keliamos rizikos pobūdis, nacionalinių priemonių, kurių imtasi, pobūdis ir trukmė, taip pat atitinkamo veiklos vykdytojo pateikti argumentai. Visų pirma rinkos priežiūros institucijos nurodo, ar reikalavimų nesilaikymas sietinas su viena ar daugiau iš šių priežasčių:

   a) nesilaikoma 5 straipsnyje nurodyto su DI susijusios praktikos draudimo;

   b) didelės rizikos DI sistema neatitinka III skyriaus 2 skirsnyje nustatytų reikalavimų;

c) 40 ir 41 straipsniuose nurodyti darnieji standartai arba bendrosios specifikacijos, kuriais remiantis daryta atitikties prezumpcija, turi trūkumų;

d) nesilaikoma 50 straipsnio.

7. Kitos rinkos priežiūros institucijos nei procedūrą inicijavusios valstybės narės rinkos priežiūros institucija nedelsdamos informuoja Komisiją ir kitas valstybes nares apie visas priemones, kurių ėmėsi, ir pateikia visą turimą papildomą informaciją, susijusią su atitinkamai DI sistemai taikomų reikalavimų nesilaikymu, o jei nesutinka su nacionaline priemone, apie kurią pranešta, – savo prieštaravimus.

8. Jeigu per tris mėnesius nuo šio straipsnio 5 dalyje nurodyto pranešimo gavimo nei valstybės narės rinkos priežiūros institucija, nei Komisija nepareiškia prieštaravimo dėl laikinosios priemonės, kurios ėmėsi kitos valstybės narės rinkos priežiūros institucija, ta priemonė laikoma pagrįsta. Tai nedaro poveikio atitinkamo veiklos vykdytojo procesinėms teisėms pagal Reglamento (ES) 2019/1020 18 straipsnį. Tuo atveju, kai nesilaikoma šio reglamento 5 straipsnyje nurodyto su DI susijusios praktikos draudimo, šioje dalyje nurodytas trijų mėnesių laikotarpis sutrumpinamas iki 30 dienų.

9. Rinkos priežiūros institucijos užtikrina, kad atitinkamo gaminio arba DI sistemos atžvilgiu nepagrįstai nedelsiant būtų taikomos tinkamos ribojamosios priemonės, pavyzdžiui, gaminys arba DI sistema būtų pašalinti iš jų rinkos.

80 straipsnis

Procedūra, taikoma DI sistemoms,

kurias tiekėjas pagal III priedą priskiria nedidelės rizikos sistemoms

1. Jeigu rinkos priežiūros institucija turi pakankamą pagrindą manyti, kad DI sistema, kurią tiekėjas pagal 6 straipsnio 3 dalį priskiria nedidelės rizikos sistemoms, iš tikrųjų yra didelės rizikos sistema, rinkos priežiūros institucija atlieka atitinkamos DI sistemos vertinimą, susijusį su jos priskyrimu didelės rizikos DI sistemoms, remdamasi 6 straipsnio 3 dalyje nustatytomis sąlygomis ir Komisijos gairėmis.

2. Jeigu atlikdama tą vertinimą rinkos priežiūros institucija nustato, kad atitinkama DI sistema kelia didelę riziką, ji nepagrįstai nedelsdama pareikalauja, kad atitinkamas tiekėjas imtųsi visų reikiamų veiksmų, kad būtų užtikrintas tos DI sistemos atžvilgiu taikomų šiame reglamente nustatytų reikalavimų ir pareigų laikymasis, taip pat per laikotarpį, kurį rinkos priežiūros institucija gali nustatyti, būtų imtasi tinkamų taisomųjų veiksmų.

3. Jeigu rinkos priežiūros institucija mano, kad atitinkama DI sistema naudojama ne tik jos nacionalinėje teritorijoje, ji nepagrįstai nedelsdama informuoja Komisiją ir kitas valstybes nares apie vertinimo rezultatus ir veiksmus, kurių ji nurodė imtis tiekėjui.

4. Tiekėjas užtikrina, kad būtų imtasi visų reikiamų veiksmų, kad DI sistemos atžvilgiu būtų laikomasi šiame reglamente nustatytų reikalavimų ir pareigų. Jei atitinkamas DI sistemos tiekėjas per šio straipsnio 2 dalyje nurodytą laikotarpį neužtikrina, kad DI sistemos atžvilgiu būtų laikomasi tų reikalavimų ir pareigų, tiekėjui skiriamos baudos pagal 99 straipsnį.

5. Tiekėjas užtikrina, kad visų reikiamų taisomųjų veiksmų būtų imtasi visų atitinkamų DI sistemų, kurias jis pateikė Sąjungos rinkai, atžvilgiu.

6. Jeigu per šio straipsnio 2 dalyje nurodytą laikotarpį atitinkamos DI sistemos tiekėjas nesiima tinkamų taisomųjų veiksmų, taikomos 79 straipsnio 5–9 dalys.

7. Jeigu atlikdama vertinimą pagal šio straipsnio 1 dalį rinkos priežiūros institucija nustato, kad tiekėjas klaidingai priskyrė DI sistemą nedidelės rizikos sistemoms, kad išvengtų III skyriaus 2 skirsnio reikalavimų taikymo, tiekėjui skiriamos baudos pagal 99 straipsnį.

8. Naudodamosi savo įgaliojimais stebėti, kaip taikomas šis straipsnis, rinkos priežiūros institucijos pagal Reglamento (ES) 2019/1020 11 straipsnį gali atlikti atitinkamus patikrinimus, visų pirma atsižvelgdamos į informaciją, saugomą šio reglamento 71 straipsnyje nurodytoje ES duomenų bazėje.

81 straipsnis

Sąjungos apsaugos procedūra

1. Jeigu per tris mėnesius nuo 79 straipsnio 5 dalyje nurodyto pranešimo gavimo arba per 30 dienų tuo atveju, kai nesilaikoma 5 straipsnyje nurodyto su DI susijusios praktikos draudimo kurios nors valstybės narės rinkos priežiūros institucija pareiškia prieštaravimą dėl priemonės, kurios ėmėsi kita rinkos priežiūros institucija, arba jeigu Komisija mano, kad priemonė prieštarauja Sąjungos teisei, Komisija nepagrįstai nedelsdama pradeda konsultacijas su atitinkamos valstybės narės rinkos priežiūros institucija ir veiklos vykdytoju ar vykdytojais ir tą nacionalinę priemonę įvertina. Remdamasi to vertinimo rezultatais, Komisija per šešis mėnesius arba per 60 dienų, jei nesilaikoma 5 straipsnyje nurodyto su DI susijusios praktikos draudimo, nuo 79 straipsnio 5 dalyje nurodyto pranešimo gavimo dienos nusprendžia, ar nacionalinė priemonė yra pagrįsta, ir apie savo sprendimą praneša atitinkamos valstybės narės rinkos priežiūros institucijai. Apie tokį sprendimą Komisija taip pat informuoja visas kitas rinkos priežiūros institucijas.

2. Jei Komisija mano, kad priemonė, kurios ėmėsi atitinkama valstybė narė, yra pagrįsta, visos valstybės narės užtikrina, kad būtų imtasi tinkamų ribojamųjų priemonių dėl atitinkamos DI sistemos, pavyzdžiui, būtų pareikalauta nepagrįstai nedelsiant DI sistemą pašalinti iš jų rinkos, ir atitinkamai informuoja Komisiją. Jeigu Komisija nacionalinę priemonę laiko nepagrįsta, atitinkama valstybė narė priemonę atšaukia ir atitinkamai informuoja Komisiją.

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.

82 straipsnis

Riziką keliančios reikalavimus atitinkančios DI sistemos

1. Jeigu, atlikusi vertinimą pagal 79 straipsnį ir pasikonsultavusi su 77 straipsnio 1 dalyje nurodyta atitinkama nacionaline valdžios institucija, valstybės narės rinkos priežiūros institucija nustato, kad, nors didelės rizikos DI sistema atitinka šio reglamento reikalavimus, tačiau ji vis tiek kelia riziką asmenų sveikatai ar saugai, pagrindinėms teisėms arba kitiems visuomenės intereso apsaugos aspektams, ji pareikalauja, kad atitinkamas veiklos vykdytojas nepagrįstai nedelsdamas, per laikotarpį , kurį ji gali nustatyti, imtųsi visų tinkamų priemonių užtikrinti, kad atitinkama DI sistema, kai ji pateikiama rinkai ar pradedama naudoti, nebekeltų tokios rizikos.

2. Tiekėjas arba kitas atitinkamas veiklos vykdytojas užtikrina, kad taisomųjų veiksmų dėl visų susijusių DI sistemų, kurias jie patiekė Sąjungos rinkai, būtų imtasi per 1 dalyje nurodytos valstybės narės rinkos priežiūros institucijos nustatytą terminą.

3. Valstybės narės nedelsdamos informuoja Komisiją ir kitas valstybes nares apie pagal 1 dalį padarytas išvadas. 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 nacionalinių priemonių, kurių imtasi, pobūdis ir trukmė.

4. Komisija nepagrįstai nedelsdama pradeda konsultacijas su atitinkamomis valstybėmis narėmis ir atitinkamais veiklos vykdytojais ir įvertina nacionalines priemones, kurių imtasi. Remdamasi to vertinimo rezultatais Komisija nusprendžia, ar priemonė pagrįsta, ir prireikus pasiūlo kitų tinkamų priemonių.

5. Apie savo sprendimą Komisija tuojau pat praneša atitinkamai valstybei narei ir atitinkamiems veiklos vykdytojams. Ji taip pat informuoja kitas valstybes nares.

83 straipsnis

Oficiali neatitiktis

1. Jeigu valstybės narės rinkos priežiūros institucija padaro vieną iš toliau nurodytų išvadų, ji reikalauja, kad atitinkamas tiekėjas pašalintų nustatytą neatitiktį per laikotarpį, kurį ji gali nustatyti:

   a) CE ženklu paženklinta pažeidžiant 48 straipsnį;

   b) nepaženklinta CE ženklu;

   c) neparengta 47 straipsnyje nurodyta ES atitikties deklaracija;

d) 47 straipsnyje nurodyta ES atitikties deklaracija parengta netinkamai;

e) neatlikta registracija 71 straipsnyje nurodytoje ES duomenų bazėje;

f) kai taikytina, nepaskirtas įgaliotasis atstovas;

g) nepateikta techninių dokumentų.

2. Jeigu 1 dalyje nurodyta neatitiktis nepašalinama, atitinkamos valstybės narės rinkos priežiūros institucija imasi tinkamų ir proporcingų priemonių, kad būtų apribotas ar uždraustas didelės rizikos DI sistemos tiekimas rinkai arba užtikrinama, kad ji būtų nedelsiant atšaukta arba pašalinta iš rinkos.

84 straipsnis

Sąjungos DI bandymų pagalbinės struktūros

1. Komisija paskiria vieną ar daugiau Sąjungos DI bandymų pagalbinių struktūrų, kad būtų atliktos Reglamento (ES) 2019/1020 21 straipsnio 6 dalyje išvardytos užduotys DI srityje.

2. Nedarant poveikio 1 dalyje nurodytoms užduotims, Sąjungos DI bandymų pagalbinės struktūros taip pat teikia nepriklausomas technines ar mokslines konsultacijas Valdybos, Komisijos arba rinkos priežiūros institucijų prašymu.

4 SKIRSNIS

TEISIŲ GYNIMO PRIEMONĖS

85 straipsnis

Teisė pateikti skundą rinkos priežiūros institucijai

Nedarant poveikio kitoms administracinėms ar teisminėms teisių gynimo priemonėms, bet kuris fizinis ar juridinis asmuo, turintis pagrindo manyti, kad buvo pažeistos šio reglamento nuostatos, gali atitinkamai rinkos priežiūros institucijai pateikti skundus.

Pagal Reglamentą (ES) 2019/1020 į tokius skundus atsižvelgiama rinkos priežiūros veiklos tikslu ir jie nagrinėjami laikantis rinkos priežiūros institucijų tuo tikslu nustatytų specialių procedūrų.

86 straipsnis

Teisė gauti priimtų individualių sprendimų paaiškinimą

1. Bet kuris asmuo, paveiktas sprendimo, kurį diegėjas priima remdamasis III priede nurodytos didelės rizikos DI sistemos, išskyrus jo 2 punkte išvardytas sistemas, išvediniu, ir kuris tam asmeniui sukelia teisinių padarinių arba daro panašų didelį poveikį taip, kad, to asmens nuomone, tai daro neigiamą poveikį jo sveikatai, saugai ar pagrindinėms teisėms, turi teisę iš diegėjo gauti aiškius ir prasmingus paaiškinimus apie DI sistemos vaidmenį sprendimų priėmimo procedūroje ir pagrindinius priimto sprendimo elementus.

2. 1 dalis netaikoma DI sistemų, kurioms taikomos toje dalyje nustatytos pareigos išimtys ar apribojimai, kylantys iš Sąjungos ar nacionalinės teisės laikantis Sąjungos teisės, naudojimui.

3. Šis straipsnis taikomas tik tokiu mastu, kokiu 1 dalyje nurodyta teisė nenumatyta kitaip pagal Sąjungos teisę.

87 straipsnis

Pranešimai apie pažeidimus ir pranešėjų apsauga

Pranešimams apie šio reglamento pažeidimus ir asmenų, pranešančių apie tokius pažeidimus, apsaugai taikoma Direktyva (ES) 2019/1937.

5 SKIRSNIS

BENDROSIOS PASKIRTIES DI MODELIŲ TIEKĖJŲ ATŽVILGIU TAIKOMA PRIEŽIŪRA, TYRIMAS, VYKDYMO UŽTIKRINIMAS IR STEBĖSENA

88 straipsnis

Bendrosios paskirties DI modelių tiekėjų pareigų vykdymo užtikrinimas

1. Komisija turi išimtinius įgaliojimus prižiūrėti ir užtikrinti V skyriaus vykdymą, atsižvelgiant į procedūrines garantijas pagal 94 straipsnį. Šias užduotis Komisija paveda įgyvendinti DI tarnybai, nedarant poveikio Komisijos organizaciniams įgaliojimams ir Sutartimis grindžiamam valstybių narių ir Sąjungos kompetencijos pasidalijimui.

2. Nedarant poveikio 75 straipsnio 3 daliai, rinkos priežiūros institucijos gali prašyti Komisijos naudotis šiame skirsnyje nustatytais įgaliojimais, kai tai būtina ir proporcinga siekiant padėti joms vykdyti užduotis pagal šį reglamentą.

89 straipsnis

Stebėsenos veiksmai

1. DI tarnyba, siekdama vykdyti pagal šį skirsnį jai pavestas užduotis, gali imtis būtinų veiksmų, kad stebėtų, ar bendrosios paskirties DI modelių tiekėjai veiksmingai įgyvendina šį reglamentą ir ar jo laikosi, be kita ko, kaip jie laikosi patvirtintų praktikos kodeksų.

2. Tolesnės grandies tiekėjai turi teisę pateikti skundą dėl įtariamo šio reglamento pažeidimo. Skundas turi būti tinkamai pagrįstas ir jame nurodoma bent:

   a) atitinkamo bendrosios paskirties DI modelio tiekėjo kontaktinis punktas;

   b) atitinkamų faktų aprašymas, atitinkamos šio reglamento nuostatos ir priežastis, kodėl tolesnės grandies tiekėjas mano, kad atitinkamo bendrosios paskirties DI modelio tiekėjas pažeidė šį reglamentą;

   c) visa kita informacija, kuri prašymą išsiuntusio tolesnės grandies tiekėjo nuomone, yra svarbi, įskaitant, kai tinkama, jo iniciatyva surinktą informaciją.

90 straipsnis

Mokslinės komisijos perspėjimai apie sisteminę riziką

1. Mokslinė komisija DI tarnybai gali pateikti kvalifikuotą perspėjimą, jei turi pagrindo įtarti, kad:

   a) bendrosios paskirties DI modelis Sąjungos lygmeniu kelia konkrečią nustatomą riziką, arba

   b) bendrosios paskirties DI modelis atitinka 51 straipsnyje nurodytas sąlygas.

2. Gavusi tokį kvalifikuotą perspėjimą, Komisija per DI tarnybą ir informavusi Valdybą, siekdama tai įvertinti, gali pasinaudoti šiame skirsnyje nustatytais įgaliojimais. DI tarnyba informuoja Valdybą apie visas priemones pagal 91–94 straipsnius.

3. Kvalifikuotas perspėjimas turi būti tinkamai pagrįstas ir jame nurodoma bent:

   a) atitinkamo sisteminės rizikos bendrosios paskirties DI modelio tiekėjo kontaktinis punktas;

   b) atitinkamų faktų aprašymas ir priežastys, dėl kurių mokslinė komisija pateikė perspėjimą;

   c) visa kita informacija, kuri, mokslinės komisijos nuomone, yra svarbi, įskaitant, kai tinkama, jos iniciatyva surinktą informaciją.

91 straipsnis

Įgaliojimai prašyti dokumentų ir informacijos

1. Komisija gali paprašyti atitinkamo bendrosios paskirties DI modelio tiekėjo pateikti pagal 53 ir 55 straipsnius tiekėjo parengtus dokumentus arba bet kokią papildomą informaciją, kurios reikia siekiant įvertinti, ar tiekėjas laikosi šio reglamento.

2. Prieš išsiųsdama prašymą pateikti informaciją, DI tarnyba gali pradėti struktūrinį dialogą su bendrosios paskirties DI modelio tiekėju.

3. Gavusi tinkamai pagrįstą mokslinės komisijos prašymą, Komisija gali bendrosios paskirties DI modelio tiekėjui pateikti prašymą dėl informacijos, jei prieiga prie informacijos yra būtina ir proporcinga mokslinės komisijos užduotims pagal 68 straipsnio 2 dalį vykdyti.

4. Prašyme pateikti informaciją nurodomas prašymo teisinis pagrindas ir tikslas, nurodoma, kokios informacijos reikia, nustatomas laikotarpis, per kurį informacija turi būti pateikta ir nurodomos 101 straipsnyje numatytos baudos už neteisingos, neišsamios ar klaidinančios informacijos pateikimą.

5. Prašomą informaciją pateikia atitinkamo bendrosios paskirties DI modelio tiekėjas arba jo atstovas. Juridinių asmenų, bendrovių ar įmonių atveju arba tais atvejais, kai tiekėjas neturi juridinio asmens statuso, prašomą informaciją atitinkamo bendrosios paskirties DI modelio tiekėjo vardu pateikia asmenys, teisės aktais arba jo įstatais įgalioti jam atstovauti. Tinkamai įgalioti teisininkai gali teikti informaciją savo klientų vardu. Vis dėlto klientai lieka visiškai atsakingi, jei pateikta informacija yra neišsami, neteisinga ar klaidinanti.

92 straipsnis

Įgaliojimai atlikti vertinimus

1. DI tarnyba, pasikonsultavusi su Valdyba, gali atlikti atitinkamo bendrosios paskirties DI modelio vertinimus:

   a) kad įvertintų, kaip tiekėjas vykdo pareigas pagal šį reglamentą, kai pagal 91 straipsnį surinkta informacija yra nepakankama, arba

   b) kad ištirtų sisteminę riziką Sąjungos lygmeniu, susijusią su sisteminės rizikos bendrosios paskirties DI modeliais, visų pirma remiantis mokslinės komisijos kvalifikuotu perspėjimu pagal 90 straipsnio 1 dalies a punktą.

2. Komisija gali nuspręsti paskirti nepriklausomus ekspertus vertinimams atlikti jos vardu, įskaitant ekspertus iš mokslinės komisijos, sudarytos pagal 68 straipsnį. Šiai užduočiai atlikti paskirti nepriklausomi ekspertai turi atitikti 68 straipsnio 2 dalyje išdėstytus kriterijus.

3. 1 dalies tikslais Komisija gali prašyti prieigos prie atitinkamo bendrosios paskirties DI modelio per API arba kitas tinkamas technines priemones ir įrankius, įskaitant pirminį kodą.

4. Prašyme suteikti prieigą prie informacijos nurodomas prašymo teisinis pagrindas, tikslas bei priežastys ir nustatomas laikotarpis, per kurį prieiga turi būti suteikta, taip pat nurodomos 101 straipsnyje numatytos baudos už prieigos nesuteikimą.

5. Atitinkamo bendrosios paskirties DI modelio tiekėjai arba jo atstovas suteikia prašomą informaciją. Juridinių asmenų, bendrovių ar įmonių atveju arba tais atvejais, kai tiekėjas neturi juridinio asmens statuso, prašomą prieigą atitinkamo bendrosios paskirties DI modelio tiekėjo vardu suteikia asmenys, teisės aktais arba jų nuostatais įgalioti jiems atstovauti.

6. Komisija priima įgyvendinimo aktus, kuriais nustatoma išsami vertinimų tvarka ir sąlygos, įskaitant išsamią nepriklausomų ekspertų įtraukimo tvarką ir jų atrankos procedūrą. Tie įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

7. Prieš prašydama prieigos prie atitinkamo bendrosios paskirties DI modelio, DI tarnyba gali pradėti struktūrinį dialogą su bendrosios paskirties DI modelio tiekėju, kad surinktų daugiau informacijos apie modelio vidaus bandymus, sisteminės rizikos prevencijai skirtas vidaus apsaugos priemones ir kitas vidaus procedūras bei priemones, kurių tiekėjas ėmėsi tokiai rizikai sumažinti.

93 straipsnis

Įgaliojimai prašyti imtis priemonių

1. Kai būtina ir tikslinga, Komisija gali prašyti, kad tiekėjai:

   a) imtųsi tinkamų priemonių 53 ir 54 straipsniuose nustatytoms pareigoms vykdyti;

   b) įgyvendintų rizikos mažinimo priemones, kai pagal 92 straipsnį atlikus vertinimą kyla rimtas ir pagrįstas susirūpinimas dėl sisteminės rizikos Sąjungos lygmeniu;

   c) apribotų modelio tiekimą rinkai, jį pašalintų arba atšauktų.

2. Prieš paprašydama imtis priemonės, DI tarnyba gali pradėti struktūrinį dialogą su bendrosios paskirties DI modelio tiekėju.

3. Jei per 2 dalyje nurodytą struktūrinį dialogą sisteminės rizikos bendrosios paskirties DI modelio tiekėjas pasiūlo įsipareigoti įgyvendinti rizikos mažinimo priemones, kad būtų šalinama sisteminė rizika Sąjungos lygmeniu, Komisija gali priimti sprendimą, kuriuo tie įsipareigojimai taptų privalomi, ir paskelbti, kad nėra pagrindo imtis tolesnių veiksmų.

94 straipsnis

Bendrosios paskirties DI modelio ekonominės veiklos vykdytojų procesinės teisės

Reglamento (ES) 2019/1020 18 straipsnis *mutatis mutandis* taikomas bendrosios paskirties DI modelio tiekėjams, nedarant poveikio konkretesnėms šiame reglamente numatytoms procesinėms teisėms.

X skyrius

Elgesio kodeksai ir gairės

95 straipsnis

Savanoriško konkrečių reikalavimų taikymo elgesio kodeksai

1. DI tarnyba ir valstybės narės skatina ir padeda rengti elgesio kodeksus, įskaitant susijusius valdymo mechanizmus, kuriais siekiama skatinti DI sistemoms, išskyrus didelės rizikos DI sistemas, savanoriškai taikyti kelis ar visus III skyriaus 2 skirsnyje nustatytus reikalavimus, atsižvelgiant į turimus techninius sprendimus ir sektoriaus geriausią praktiką, kuriais sudaromos sąlygos taikyti tokius reikalavimus.

2. DI tarnyba ir valstybės narės padeda rengti elgesio kodeksus, susijusius su savanorišku konkrečių reikalavimų taikymu, įskaitant diegėjų vykdomą taikymą, visoms DI sistemoms, remiantis aiškiais tikslais ir tų tikslų pasiekimui įvertinti skirtais pagrindiniais veikimo rodikliais, įskaitant, pavyzdžiui, toliau nurodytus elementus (bet jais neapsiribojant):

a) taikytini elementai, numatyti Sąjungos patikimo DI etikos gairėse;

b) DI sistemų poveikio aplinkosauginiam tvarumui įvertinimas, be kita ko, kiek tai susiję su efektyviu energijos vartojimu grindžiamu programavimu ir veiksmingo DI projektavimo, mokymo ir naudojimo metodais, ir kuo didesnis to poveikio sumažinimas;

c) raštingumo DI srityje, visų pirma asmenų, susijusių su DI kūrimu, veikimu ir naudojimu, raštingumo skatinimas;

d) palankesnių sąlygų įtraukiam ir įvairove grindžiamam DI sistemų projektavimui sudarymas, be kita ko, sudarant įtraukias ir įvairove grindžiamas kūrimo grupes ir skatinant suinteresuotuosius subjektus dalyvauti tame procese;

e) neigiamo DI sistemų poveikio pažeidžiamiems asmenims ar pažeidžiamų asmenų grupėms, be kita ko, kiek tai susiję su prieinamumu asmenims su negalia, taip pat lyčių lygybei vertinimas ir prevencija.

3. Elgesio kodeksus gali rengti individualūs DI sistemų tiekėjai ar diegėjai arba jiems atstovaujančios organizacijos, arba ir vieni, ir kiti, be kita ko, dalyvaujant visiems suinteresuotiesiems subjektams, taip pat jiems atstovaujančioms organizacijoms, įskaitant pilietinės visuomenės organizacijas ir akademinę bendruomenę. Elgesio kodeksai gali būti taikomi vienai ar daugiau DI sistemų, atsižvelgiant į atitinkamų sistemų numatytosios paskirties panašumą.

4. DI tarnyba ir valstybės narės, skatindamos ir padėdamos rengti elgesio kodeksus, atsižvelgia į konkrečius MVĮ, įskaitant startuolius, interesus ir poreikius.

96 straipsnis

Komisijos gairės dėl šio reglamento įgyvendinimo

1. Komisija parengia šio reglamento praktinio įgyvendinimo gaires, visų pirma dėl:

   a) 8–15 straipsniuose ir 25 straipsnyje nurodytų reikalavimų taikymo ir pareigų vykdymo;

   b) 5 straipsnyje nurodytos draudžiamos praktikos;

   c) nuostatų, susijusių su esminiais pakeitimais, praktinio įgyvendinimo;

   d) 50 straipsnyje nustatytų skaidrumo pareigų praktinio įgyvendinimo;

e) išsamios informacijos apie šio reglamento ryšį su I priede išvardytais Sąjungos derinamaisiais teisės aktais, taip pat su kitais atitinkamais Sąjungos teisės aktais, be kita ko, kiek tai susiję su jų vykdymo užtikrinimo nuoseklumu;

f) 3 straipsnio 1 punkte pateiktos DI sistemos apibrėžties taikymo.

Priimdama tokias gaires, Komisija ypač daug dėmesio skiria MVĮ, įskaitant startuolius, vietos valdžios institucijų ir sektorių, kuriems šio reglamento poveikis yra labiausiai tikėtinas, poreikiams.

Šios dalies pirmoje pastraipoje nurodytose gairėse tinkamai atsižvelgiama į visuotinai pripažintus pažangiausius DI srities metodus, taip pat į atitinkamus darniuosius standartus ir bendrąsias specifikacijas, nurodytus 40 ir 41 straipsniuose, arba į darniuosius standartus ar technines specifikacijas, nustatytus pagal Sąjungos derinamuosius teisės aktus.

2. Anksčiau priimtas gaires Komisija, jeigu tai laiko reikalinga, atnaujina valstybių narių arba DI tarnybos prašymu arba savo iniciatyva.

XI skyrius
Deleguotieji įgaliojimai ir komiteto procedūra

97 straipsnis

Įgaliojimų delegavimas

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

2. 6 straipsnio 6 ir 7 dalyse, 7 straipsnio 1 ir 3 dalyse, 11 straipsnio 3 dalyje, 43 straipsnio 5 ir 6 dalyse, 47 straipsnio 5 dalyje, 51 straipsnio 3 dalyje, 52 straipsnio 4 dalyje ir 53 straipsnio 5 ir 6 dalyse nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo … [šio reglamento įsigaliojimo diena]. Likus ne mažiau kaip devyniems mėnesiams iki penkerių metų laikotarpio pabaigos Komisija parengia naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno laikotarpio pabaigos.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 6 straipsnio 6 ir 7 dalyse, 7 straipsnio 1 ir 3 dalyse, 11 straipsnio 3 dalyje, 43 straipsnio 5 ir 6 dalyse, 47 straipsnio 5 dalyje, 51 straipsnio 3 dalyje, 52 straipsnio 4 dalyje ir 53 straipsnio 5 ir 6 dalyse 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. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.

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

6. Pagal 6 straipsnio 6 arba 7 dalį, 7 straipsnio 1 arba 3 dalį, 11 straipsnio 3 dalį, 43 straipsnio 5 ir 6 dalį, 47 straipsnio 5 dalį, 51 straipsnio 3 dalį, 52 straipsnio 4 dalį arba 53 straipsnio 5 arba 6 dalį priimti deleguotieji aktai įsigalioja tik tuo atveju, jeigu per tris mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie tą 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.

98 straipsnis

Komiteto procedūra

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

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

XII skyrius
Sankcijos

99 straipsnis

Sankcijos

1. Laikydamosi šiame reglamente nustatytų sąlygų, valstybės narės nustato taisykles dėl sankcijų ir kitų vykdymo užtikrinimo priemonių, kurios taip pat gali apimti įspėjimus ir nepinigines priemones, taikytinų už veiklos vykdytojų padarytus šio reglamento pažeidimus, ir imasi visų būtinų priemonių užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendinamos, taip atsižvelgdamos į Komisijos pagal 96 straipsnį paskelbtas gaires. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Jomis visų pirma atsižvelgiama į MVĮ, įskaitant startuolius, interesus ir jų ekonominį gyvybingumą.

2. Valstybės narės nedelsdamos ir ne vėliau kaip iki taikymo pradžios dienos praneša Komisijai apie taisykles dėl sankcijų ir kitų vykdymo užtikrinimo priemonių, nurodytų 1 dalyje, ir nedelsdamos praneša jai apie visus vėlesnius jų pakeitimus.

3. Už 5 straipsnyje nurodytų su DI susijusios praktikos draudimų nesilaikymą skiriamos iki 35 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra įmonė, iki 7 % jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos, atsižvelgiant į tai, kuri yra didesnė.

4. Iki 15 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra įmonė, iki 3 % jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos, atsižvelgiant į tai, kuri yra didesnė, skiriamos, jei nesilaikoma kurios nors iš toliau nurodytų nuostatų, susijusių su veiklos vykdytojais ar notifikuotosiomis įstaigomis, išskyrus 5 straipsnyje išdėstytas nuostatas:

a) tiekėjų pareigų pagal 16 straipsnį;

b) įgaliotųjų atstovų pareigų pagal 22 straipsnį;

c) importuotojų pareigų pagal 23 straipsnį;

d) platintojų pareigų pagal 24 straipsnį;

e) diegėjų pareigų pagal 26 straipsnį;

f) notifikuotosioms įstaigoms taikomų reikalavimų ir pareigų pagal 31 straipsnį, 33 straipsnio 1 dalį, 33 straipsnio 3 dalį, 33 straipsnio 4 dalį arba 34 straipsnį;

g) tiekėjams ir diegėjams taikomų skaidrumo pareigų pagal 50 straipsnį.

5. Už neteisingos, neišsamios ar klaidinančios informacijos pateikimą notifikuotosioms įstaigoms arba nacionalinėms kompetentingoms institucijoms atsakant į jų prašymą taikomos iki 7 500 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra įmonė – iki 1 % jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos, atsižvelgiant į tai, kuri yra didesnė.

6. MVĮ, įskaitant startuolius, atveju kiekviena šiame straipsnyje nurodyta bauda neviršija 3, 4 ir 5 dalyse nurodytų procentų arba sumos, atsižvelgiant į tai, kuri yra mažesnė.

7. Sprendžiant, ar skirti administracinę baudą, ir sprendžiant, koks turėtų būti jos dydis kiekvienu konkrečiu atveju, atitinkamai atsižvelgiama į visas reikšmingas konkrečios situacijos aplinkybes ir į šiuos dalykus:

a) pažeidimo pobūdį, sunkumą, trukmę ir jo pasekmes, atsižvelgiant į atitinkamos DI sistemos paskirtį, taip pat, kai tikslinga, į paveiktų asmenų skaičių ir jų patirtos žalos dydį;

b) tai, ar kitos rinkos priežiūros institucijos jau yra skyrusios administracines baudas tam pačiam veiklos vykdytojui už tą patį pažeidimą;

c) tai, ar kitos institucijos jau yra skyrusios administracines baudas tam pačiam veiklos vykdytojui už kitų Sąjungos ar nacionalinės teisės aktų pažeidimus, kai tokie pažeidimai padaryti dėl tos pačios veiklos arba neveikimo, kurie yra svarbus šio reglamento pažeidimas;

d) pažeidimą padariusio veiklos vykdytojo dydį, metinę apyvartą ir rinkos dalį;

e) kitas atsakomybę sunkinančias ar švelninančias aplinkybes, susijusias su konkrečiu atveju, pavyzdžiui, gautą finansinę naudą arba nuostolius, kurių buvo tiesiogiai ar netiesiogiai išvengta dėl pažeidimo;

f) bendradarbiavimo su nacionaline kompetentinga institucija lygį siekiant atitaisyti pažeidimą ir sumažinti galimą neigiamą jo poveikį;

g) veiklos vykdytojo atsakomybės laipsnį, atsižvelgiant į jo įgyvendintas technines ir organizacines priemones;

h) tai, kokiu būdu nacionalinė kompetentinga institucija sužinojo apie pažeidimą, visų pirma tai, ar veiklos vykdytojas pranešė apie pažeidimą, jei taip – kokia apimtimi;

i) tai, ar pažeidimas padarytas tyčia ar dėl aplaidumo;

j) visus veiklos vykdytojo atliktus veiksmus siekiant sumažinti asmenų, kuriems padarytas poveikis, patirtą žalą.

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

9. 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.

10. Naudojimuisi įgaliojimais pagal šį straipsnį taikomos atitinkamos procedūrinės garantijos laikantis Sąjungos ir nacionalinės teisės, įskaitant veiksmingas teismines teisių gynimo priemones ir tinkamą procesą.

11. Valstybės narės kasmet praneša Komisijai apie administracines baudas, kurias jos skyrė tais metais pagal šį straipsnį, ir apie visus susijusius ginčų nagrinėjimo ar teismo procesus.

100 straipsnis

Administracinės baudos Sąjungos institucijoms, įstaigoms, organams ir agentūroms

1. Europos duomenų apsaugos priežiūros pareigūnas gali skirti administracines baudas Sąjungos institucijoms, įstaigoms, organams ir agentūroms, kurie patenka į šio reglamento taikymo sritį. 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, atsižvelgiant į atitinkamos DI sistemos paskirtį, taip pat, kai tinkama, į asmenų, kuriems padarytas poveikis, skaičių ir jų patirtos žalos dydį;

   b) Sąjungos institucijos, įstaigos, organo ar agentūros atsakomybės laipsnį, atsižvelgiant į jų įgyvendintas technines ir organizacines priemones;

   c) bet kokius veiksmus, kurių ėmėsi Sąjungos institucija, įstaiga, organas ar agentūra, kad sumažintų asmenų, kuriems padarytas poveikis, patirtą žalą;

   d) bendradarbiavimo su Europos duomenų apsaugos priežiūros pareigūnu lygį siekiant ištaisyti pažeidimą ir sumažinti galimą neigiamą pažeidimo poveikį, įskaitant visų priemonių, kurias Europos duomenų apsaugos priežiūros pareigūnas anksčiau nurodė taikyti atitinkamai Sąjungos institucijai, įstaigai, organui ar agentūrai dėl to paties dalyko, taikymą;

e) bet kokius anksčiau Sąjungos institucijos, įstaigos, organo ar agentūros padarytus panašius pažeidimus;

f) tai, kokiu būdu Europos duomenų apsaugos priežiūros pareigūnas sužinojo apie pažeidimą, visų pirma, ar Sąjungos institucija, įstaiga, organas ar agentūra pranešė apie pažeidimą, jei taip – kokia apimtimi;

g) Sąjungos institucijos, įstaigos, organo ar agentūros metinį biudžetą.

2. Už 5 straipsnyje nurodyto su DI susijusios praktikos draudimo nesilaikymą skiriamos iki 1 500 000 EUR dydžio administracinės baudos.

3. Už DI sistemos neatitiktį bet kuriems pagal šį reglamentą nustatytiems reikalavimams ar pareigoms, išskyrus nustatytus 5 straipsnyje, skiriamos iki 750 000 EUR dydžio administracinės baudos.

4. Prieš priimdamas sprendimus pagal šį straipsnį, Europos duomenų apsaugos priežiūros pareigūnas suteikia Sąjungos institucijai, įstaigai, organui ar agentūrai, dėl kurių jis pradėjo procesą, galimybę būti išklausytiems su galimu pažeidimu susijusiais klausimais. Europos duomenų apsaugos priežiūros pareigūnas savo sprendimus grindžia tik tais elementais ir aplinkybėmis, dėl kurių atitinkamos šalys galėjo pateikti pastabų. 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 skyrus šiame straipsnyje numatytas baudas, įskaitomos į Sąjungos bendrąjį biudžetą. Baudos nedaro poveikio veiksmingai Sąjungos institucijos, įstaigos, organo ar agentūros, kuriems skirta bauda, veiklai.

7. Europos duomenų apsaugos priežiūros pareigūnas kasmet praneša Komisijai apie administracines baudas, kurias jis skyrė pagal šį straipsnį, ir apie visus savo inicijuotus ginčų nagrinėjimo ar teismo procesus.

101 straipsnis

Baudos bendrosios paskirties DI modelių tiekėjams

1. Komisija bendrosios paskirties DI modelių tiekėjams gali skirti baudas, neviršijančias 3 % jų bendros pasaulinės praėjusių finansinių metų metinės apyvartos arba 15 000 000 EUR sumos, atsižvelgiant į tai, kuri yra didesnė, jei Komisija nustato, kad tiekėjas tyčia ar dėl aplaidumo:

   a) pažeidė atitinkamas šio reglamento nuostatas;

   b) nepatenkino prašymo pateikti dokumentą arba pateikti informaciją pagal 91 straipsnį arba pateikė neteisingą, neišsamią ar klaidinančią informaciją;

c) nesilaikė pagal 93 straipsnį prašomos priemonės;

d) nesuteikė Komisijai prieigos prie bendrosios paskirties DI modelio arba sisteminės rizikos bendrosios paskirties DI modelio, kad būtų galima atlikti vertinimą pagal 92 straipsnį.

Nustatant baudos arba periodinės baudos dydį atsižvelgiama į pažeidimo pobūdį, sunkumą ir trukmę, deramai atsižvelgiant į proporcingumo ir tinkamumo principus. Komisija taip pat atsižvelgia į įsipareigojimus, prisiimtus pagal 93 straipsnio 3 dalį arba prisiimtus atitinkamuose praktikos kodeksuose pagal 56 straipsnį.

2. Prieš priimdama sprendimą pagal 1 dalį, Komisija pateikia preliminarias išvadas bendrosios paskirties DI modelio tiekėjui ir suteikia jam galimybę būti išklausytam.

3. Pagal šį straipsnį skiriamos baudos turi būti veiksmingos, proporcingos ir atgrasomos.

4. Informacija apie pagal šį straipsnį skirtas baudas atitinkamai perduodama ir Valdybai.

5. Europos Sąjungos Teisingumo Teismas turi neribotą jurisdikciją peržiūrėti Komisijos sprendimus, kuriais pagal šį straipsnį nustatoma bauda. Jis gali panaikinti, sumažinti arba padidinti skirtą baudą.

6. Komisija priima įgyvendinimo aktus, kuriuose nustatoma išsami procedūrų tvarka ir procesinės garantijos, kad būtų galima priimti sprendimus pagal šio straipsnio 1 dalį. Tie įgyvendinimo aktai priimami laikantis 98 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

XIII skyrius
Baigiamosios nuostatos

102 straipsnis

Reglamento (EB) Nr. 300/2008 pakeitimas

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

„Priimant išsamias priemones, susijusias su saugumo įrangos patvirtinimo ir naudojimo techninėmis specifikacijomis ir procedūromis, kiek tai susiję su dirbtinio intelekto sistemomis, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

103 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, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

104 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, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas)(OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

105 straipsnis

Direktyvos 2014/90/ES pakeitimas

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

„5. Kiek tai susiję su dirbtinio intelekto sistemomis, kurios yra saugos komponentai, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], vykdydama veiklą pagal 1 dalį ir priimdama technines specifikacijas ir bandymo standartus pagal 2 ir 3 dalis Komisija atsižvelgia į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

106 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, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

107 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, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …)“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

108 straipsnis

Reglamento (ES) 2018/1139 pakeitimai

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, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …).“;

2) 19 straipsnis papildomas šia dalimi:

„4. Priimant deleguotuosius aktus pagal 1 ir 2 dalis dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, kaip tai suprantama Reglamente (ES) 2024/…[++], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.“;

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

[++] OL: prašom įrašyti šio reglamento (2021/0106(COD)) numerį.

3) 43 straipsnis papildomas šia dalimi:

„4. Priimant įgyvendinimo aktus pagal 1 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, kaip tai suprantama Reglamente (ES) 2024/…[+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje 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, kaip tai suprantama Reglamente (ES) 2024/…[+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.“;

5) 57 straipsnis papildomas šia pastraipa:

„Priimant tuos įgyvendinimo aktus dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, kaip tai suprantama Reglamente (ES) 2024/…[+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje 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, kaip tai suprantama Reglamente (ES) 2024/…[+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.“.

[+] OL: prašom įrašyti šio reglamento (2021/0106(COD)) numerį.

109 straipsnis

Reglamento (ES) 2019/2144 pakeitimas

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

„3. Priimant įgyvendinimo aktus pagal 2 dalį dėl dirbtinio intelekto sistemų, kurios yra saugos komponentai, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2024/…[*+], atsižvelgiama į to reglamento III skyriaus 2 skirsnyje nustatytus reikalavimus.

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …).“.

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) numerį ir baigti pildyti atitinkamą išnašą.

110 straipsnis

Direktyvos (ES) 2020/1828 pakeitimas

Europos Parlamento ir Tarybos direktyvos (ES) 2020/1828[58] I priedas papildomas šiuo punktu:

„68. … m. … … d. Europos Parlamento ir Tarybos reglamentas 2024/…[+], kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828) (Dirbtinio intelekto aktas) (OL L, …, ELI: …).“.

111 straipsnis

Rinkai jau pateiktos ar pradėtos naudoti DI sistemos ir rinkai jau pateikti bendrosios paskirties DI modeliai

1. Nedarant poveikio 5 straipsnio taikymui, kaip nurodyta 113 straipsnio 3 dalies a punkte, DI sistemos, kurios yra didelės apimties IT sistemų, sukurtų X priede nurodytais teisės aktais ir pateiktų rinkai arba pradėtų naudoti anksčiau nei … [36 mėnesiai nuo šio reglamento įsigaliojimo dienos], komponentai, ne vėliau kaip 2030 m. gruodžio 31 d. turi atitikti šį reglamentą.

---

[58] 2020 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2020/1828 dėl atstovaujamųjų ieškinių siekiant apsaugoti vartotojų kolektyvinius interesus, kuria panaikinama Direktyva 2009/22/EB (OL L 409, 2020 12 4, p. 1).

[+] OL: prašom tekste įrašyti šio reglamento (2021/0106(COD)) datą ir numerį.

Atliekant kiekvienos X priede nurodytais teisės aktais sukurtos didelės apimties IT sistemos vertinimą, kaip numatyta tuose teisės aktuose ir kai tie teisės aktai pakeičiami arba iš dalies keičiami, atsižvelgiama į šiame reglamente nustatytus reikalavimus.

2. Nedarant poveikio 5 straipsnio taikymui, kaip nurodyta 113 straipsnio 3 dalies a punkte, didelės rizikos DI sistemų, kurios nėra šio straipsnio 1 dalyje nurodytos sistemos ir kurios buvo pateiktos rinkai arba pradėtos naudoti anksčiau nei … [24 mėnesiai nuo šio reglamento įsigaliojimo dienos], operatoriams šis reglamentas taikomas tik tuo atveju, jei nuo tos dienos tų sistemų konstrukcijos reikšmingai pasikeitė. Bet kuriuo atveju didelės rizikos DI sistemų, kurias ketina naudoti valdžios institucijos, tiekėjai ir diegėjai imasi būtinų veiksmų, kad laikytųsi šio reglamento reikalavimų ir pareigų, ne vėliau kaip … [šešeri metai nuo šio reglamento įsigaliojimo dienos].

3. Bendrosios paskirties DI modelių, kurie buvo pateikti rinkai anksčiau nei … [12 mėnesių nuo šio reglamento įsigaliojimo dienos], tiekėjai imasi būtinų veiksmų, kad įvykdytų šiame reglamente nustatytas pareigas ne vėliau kaip… [36 mėnesiai nuo šio reglamento įsigaliojimo dienos].

112 straipsnis

Vertinimas ir peržiūra

1. Komisija kartą per metus po šio reglamento įsigaliojimo ir iki 97 straipsnyje nustatyto įgaliojimų delegavimo laikotarpio pabaigos įvertina poreikį iš dalies pakeisti III priede pateiktą sąrašą ir 5 straipsnyje nustatytą draudžiamos DI praktikos sąrašą. To vertinimo rezultatus Komisija pateikia Europos Parlamentui ir Tarybai.

2. Ne vėliau kaip … [ketveri metai nuo šio reglamento įsigaliojimo dienos], o vėliau - kas ketverius metus Komisija atlieka vertinimą ir Europos Parlamentui ir Tarybai pateikia ataskaitą dėl:

   a) pakeitimų siekiant išplėsti esamas sričių antraštes arba į III priedą įtraukti naujas sričių antraštes poreikio;

   b) 50 straipsnyje pateikto DI sistemų, dėl kurių reikia papildomų skaidrumo priemonių, sąrašo pakeitimų;

   c) pakeitimų, kuriais didinamas priežiūros ir valdymo sistemos veiksmingumas.

3. Ne vėliau kaip … [penkeri metai nuo šio reglamento įsigaliojimo dienos], o vėliau - kas ketverius metus Komisija teikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą. Ataskaitoje pateikiamas vykdymo užtikrinimo struktūros ir galimo poreikio Sąjungos agentūrai pašalinti nustatytus trūkumus vertinimas. Remiantis išvadomis, su ta ataskaita, kai tikslinga, pateikiamas pasiūlymas dėl šio reglamento dalinio pakeitimo. Ataskaitos skelbiamos viešai.

4. 2 dalyje nurodytose ataskaitose ypatingas dėmesys skiriamas šiems dalykams:

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

b) sankcijų, visų pirma 99 straipsnio 1 dalyje nurodytų administracinių baudų, kurias valstybės narės taiko už šio reglamento pažeidimus, padėčiai;

c) priimtiems šiam reglamentui įgyvendinti parengtiems darniesiems standartams ir bendrosioms specifikacijoms;

d) įmonių, kurios patenka į rinką po šio reglamento taikymo pradžios datos, skaičiui ir tam, kiek iš jų yra MVĮ.

5. Ne vėliau kaip … [ketveri metai nuo šio reglamento įsigaliojimo dienos] Komisija įvertina DI tarnybos veikimą, ar jai suteikti pakankami įgaliojimai ir kompetencija, kad ji galėtų vykdyti savo užduotis, ir ar siekiant tinkamai įgyvendinti šį reglamentą ir užtikrinti jo vykdymą būtų tikslinga ir reikalinga plėsti DI tarnybą ir jos vykdymo užtikrinimo kompetenciją ir padidinti jos išteklius. Komisija vertinimo ataskaitą teikia Europos Parlamentui ir Tarybai.

6. Ne vėliau kaip… [ketveri metai nuo šio reglamento įsigaliojimo dienos] ir vėliau kas ketverius metus Komisija pateikia ataskaitą dėl pažangos, padarytos rengiant standartizacijos leidinius, susijusius su efektyviu energijos vartojimu grindžiamu bendrosios paskirties AI modelių kūrimu, peržiūros ir įvertina, ar reikia papildomų priemonių ar veiksmų, įskaitant privalomas priemones ar veiksmus. Ataskaita pateikiama Europos Parlamentui ir Tarybai ir skelbiama viešai.

7. Ne vėliau kaip … [ketveri metai nuo šio reglamento įsigaliojimo dienos], o vėliau - kas trejus metus Komisija įvertina savanoriškų elgesio kodeksų poveikį ir veiksmingumą skatinant III skyriaus 2 skirsnyje nustatytų reikalavimų taikymą DI sistemoms, išskyrus didelės rizikos DI sistemas, ir galbūt kitų papildomų reikalavimų taikymą DI sistemoms, išskyrus didelės rizikos DI sistemas, be kita ko, kiek tai susiję su aplinkosauginiu tvarumu.

8. 1–7 dalių tikslais Valdyba, valstybės narės ir nacionalinės kompetentingos institucijos teikia Komisijai informaciją jos prašymu ir nepagrįstai nedelsdamos.

9. Atlikdama 1–7 dalyse nurodytus vertinimus ir peržiūras, Komisija atsižvelgia į Valdybos, Europos Parlamento, Tarybos, taip pat kitų susijusių įstaigų ar šaltinių nuomones ir išvadas.

10. Prireikus Komisija pateikia tinkamus pasiūlymus iš dalies pakeisti šį reglamentą, visų pirma atsižvelgdama į technologinius pokyčius, DI sistemų poveikį sveikatai, saugai ir pagrindinėms teisėms ir į informacinės visuomenės pažangą.

11. Kad būtų galima vadovautis gairėmis atliekant šio straipsnio 1–7 dalyse nurodytus vertinimus ir peržiūras, DI tarnyba įsipareigoja parengti objektyvią ir dalyvaujamąją rizikos lygių vertinimo metodiką, grindžiamą atitinkamuose straipsniuose išdėstytais kriterijais ir naujų sistemų įtraukimu į:

    a) III priede nustatytą sąrašą, įskaitant esamų sričių antraščių išplėtimą arba naujų sričių antraščių įtraukimą į tą priedą,

    b) 5 straipsnyje nustatytą draudžiamos praktikos sąrašą ir

    c) DI sistemų, dėl kurių reikia papildomų skaidrumo priemonių, sąrašą pagal 50 straipsnį.

12. Bet kokiu šio reglamento pakeitimu pagal 10 dalį arba atitinkamais deleguotaisiais ar įgyvendinimo aktais, susijusiais su I priedo B skirsnyje išvardytais sektorių Sąjungos derinamaisiais teisės aktais, atsižvelgiama į kiekvieno sektoriaus reglamentavimo ypatumus ir esamus valdymo, atitikties vertinimo ir vykdymo užtikrinimo mechanizmus ir tose srityse įsteigtas institucijas.

13. Ne vėliau kaip … [septyneri metai nuo šio reglamento įsigaliojimo dienos] Komisija atlieka šio reglamento vykdymo užtikrinimo vertinimą ir pateikia Europos Parlamentui, Tarybai ir Europos ekonomikos ir socialinių reikalų komitetui ataskaitą šiuo klausimu, atsižvelgdama į pirmuosius šio reglamento taikymo metus. Remiantis išvadomis, kai tikslinga, prie tos ataskaitos pridedamas pasiūlymas iš dalies pakeisti šį reglamentą, kiek tai susiję su vykdymo užtikrinimo struktūra ir poreikiu, kad Sąjungos agentūra pašalintų nustatytus trūkumus.

113 straipsnis

Įsigaliojimas ir taikymas

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

Jis taikomas nuo … [24 mėnesiai nuo šio reglamento įsigaliojimo dienos].

Tačiau:

a) I ir II skyriai taikomi nuo … [šeši mėnesiai nuo šio reglamento įsigaliojimo dienos];

b) III skyriaus 4 skirsnis, V skyrius, VII skyrius ir XII skyrius bei 78 straipsnis taikomi nuo … [12 mėnesių nuo šio reglamento įsigaliojimo dienos], išskyrus 101 straipsnį;

c) 6 straipsnio 1 dalis ir atitinkamos šiame reglamente nustatytos pareigos taikomos nuo … [36 mėnesiai nuo šio reglamento įsigaliojimo dienos].

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta …

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas / Pirmininkė*

I PRIEDAS

Sąjungos derinamųjų teisės aktų sąrašas

A skirsnis. Sąjungos derinamųjų teisės aktų sąrašas, pagrįstas naująja teisės aktų sistema

1. 2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyva 2006/42/EB dėl mašinų, iš dalies keičianti Direktyvą 95/16/EB (OL L 157, 2006 6 9, p. 24) [panaikinta Mašinų reglamentu];

2. 2009 m. birželio 18 d. Europos Parlamento ir Tarybos direktyva 2009/48/EB dėl žaislų saugos (OL L 170, 2009 6 30, p. 1);

3. 2013 m. lapkričio 20 d. Europos Parlamento ir Tarybos direktyva 2013/53/ES dėl pramoginių ir asmeninių laivų, kuria panaikinama Direktyva 94/25/EB (OL L 354, 2013 12 28, p. 90);

4. 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/33/ES dėl valstybių narių įstatymų, susijusių su liftais ir liftų saugos įtaisais, suderinimo (OL L 96, 2014 3 29, p. 251);

5. 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/34/ES dėl valstybių narių įstatymų, susijusių su potencialiai sprogioje aplinkoje naudojama įranga ir apsaugos sistemomis, suderinimo (OL L 96, 2014 3 29, p. 309);

6. 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos direktyva 2014/53/ES dėl valstybių narių įstatymų, susijusių su radijo įrenginių tiekimu rinkai, suderinimo, kuria panaikinama Direktyva 1999/5/EB (OL L 153, 2014 5 22, p. 62);

7. 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/68/ES dėl valstybių narių įstatymų, susijusių su slėginės įrangos tiekimu rinkai, suderinimo (OL L 189, 2014 6 27, p. 164);

8. 2016 m. kovo 9 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/424 dėl lynų kelio įrenginių, kuriuo panaikinama Direktyva 2000/9/EB (OL L 81, 2016 3 31, p. 1);

9. 2016 m. kovo 9 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/425 dėl asmeninių apsaugos priemonių, kuriuo panaikinama Tarybos direktyva 89/686/EEB (OL L 81, 2016 3 31, p. 51);

10. 2016 m. kovo 9 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/426 dėl dujinį kurą deginančių prietaisų, kuriuo panaikinama Direktyva 2009/142/EB (OL L 81, 2016 3 31, p. 99);

11. 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);

12. 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);

B skirsnis. Kitų Sąjungos derinamųjų teisės aktų sąrašas

13. 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);

14. 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);

15. 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);

16. 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);

17. 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);

18. 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);

19. 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);

20. 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), kiek tai susiję su jo 2 straipsnio 1 dalies a ir b punktuose nurodytų orlaivių projektavimu, gamyba ir pateikimu rinkai, bepiločių orlaivių, jų variklių, oro sraigtų, dalių, ir nuotolinio orlaivių valdymo įrangos atveju.

II PRIEDAS

5 straipsnio 1 dalies pirmos pastraipos h punkto iii papunktyje nurodytų nusikalstamų veikų sąrašas

5 straipsnio 1 dalies pirmos pastraipos h punkto iii papunktyje nurodytos nusikalstamos veikos:

– terorizmas,

– prekyba žmonėmis,

– seksualinis vaikų išnaudojimas ir vaikų pornografija,

– neteisėta prekyba narkotinėmis ar psichotropinėmis medžiagomis,

– neteisėta prekyba ginklais, šaudmenimis ar sprogmenimis,

– tyčinis nužudymas, sunkus sužalojimas,

– neteisėta prekyba žmogaus organais ar audiniais,

– neteisėta prekyba branduolinėmis ar radioaktyviosiomis medžiagomis,

– žmonių grobimas, neteisėtas laisvės atėmimas ar įkaitų ėmimas,

– Tarptautinio baudžiamojo teismo jurisdikcijai priklausantys nusikaltimai,

– neteisėtas orlaivių ar laivų užgrobimas,

– iššaginimas,

– nusikaltimas aplinkai,

– organizuotas ar ginkluotas apiplėšimas,

– sabotažas,

– dalyvavimas nusikalstamo susivienijimo veikloje, susijusioje su viena ar keliomis pirmiau išvardytomis nusikalstamomis veikomis.

III PRIEDAS

6 straipsnio 2 dalyje nurodytos didelės rizikos DI sistemos

Didelės rizikos DI sistemos pagal 6 straipsnio 2 dalį yra bet kurioje iš toliau nurodytų sričių išvardytos DI sistemos:

1. Biometrija, jei ją leidžiama naudoti pagal atitinkamus Sąjungos ar nacionalinės teisės aktus:

   a) nuotolinio biometrinio tapatybės nustatymo sistemos.

      Į tai neįtraukiamos DI sistemos, skirtos naudoti biometriniam sutikrinimui, kurių vienintelis tikslas – patvirtinti, kad konkretus fizinis asmuo yra tas asmuo, kuriuo jis prisistato;

   b) DI sistemos, skirtos naudoti biometriniam kategorizavimui pagal neskelbtinus ar saugomus požymius ar ypatumus, remiantis nuspėjamais tais požymiais ar ypatumais;

   c) DI sistemos, skirtos naudoti emocijų atpažinimui.

2. Ypatingos svarbos infrastruktūra: DI sistemos, skirtos naudoti kaip saugos komponentai užtikrinant ypatingos svarbos skaitmeninės infrastruktūros, kelių eismo ar vandens, dujų, šilumos ar elektros energijos tiekimo valdymą ir veikimą.

3. Švietimas ir profesinis mokymas:

a) DI sistemos, skirtos naudoti siekiant nustatyti fizinių asmenų teisę būti svarstomiems dėl priėmimo į švietimo ir profesinio mokymo įstaigas visais lygmenimis ar juos į tas įstaigas priimti arba paskirti;

b) DI sistemos, skirtos naudoti mokymosi rezultatams vertinti, įskaitant atvejus, kai tie rezultatai naudojami siekiant valdyti fizinių asmenų mokymosi procesą švietimo ir profesinio mokymo įstaigose visais lygmenimis;

c) DI sistemos, skirtos naudoti siekiant įvertinti tinkamą švietimo, kurį asmuo gaus arba galės gauti visų lygių švietimo ir profesinio mokymo įstaigose, lygį;

d) DI sistemos, skirtos naudoti siekiant stebėti ir atpažinti draudžiamą mokinių arba studentų elgesį per testus visų lygių švietimo ir profesinio mokymo įstaigose.

4. Užimtumas, darbuotojų valdymas ir galimybė dirbti savarankiškai:

a) DI sistemos, skirtos naudoti fizinių asmenų įdarbinimui arba atrankai, visų pirma siekiant teikti tikslinius darbo skelbimus, analizuoti ir filtruoti darbo prašymus ir vertinti kandidatus;

b) DI sistemos, skirtos naudoti priimant sprendimus, darančius poveikį darbo santykių sąlygoms, paaukštinimui arba darbo santykių nutraukimui, siekiant paskirstyti užduotis remiantis individualiu elgesiu arba asmenybės bruožais ar savybėmis arba stebėti bei įvertinti tokiuose santykiuose dalyvaujančių asmenų rezultatus ir elgesį.

5. Galimybė gauti pagrindines privačiąsias paslaugas ir pagrindines viešąsias paslaugas ir išmokas ir naudojimasis jomis:

a) DI sistemos, skirtos naudoti valdžios institucijose arba jų vardu siekiant įvertinti fizinių asmenų tinkamumą gauti esminės viešosios paramos išmokas ir paslaugas, įskaitant sveikatos priežiūros paslaugas, taip pat siekiant suteikti, sumažinti, panaikinti arba susigrąžinti tokias išmokas;

b) DI sistemos, skirtos naudoti siekiant įvertinti fizinių asmenų kreditingumą arba nustatyti jų kredito reitingą, išskyrus DI sistemas, naudojamas finansinio sukčiavimo atvejų aptikimo tikslu;

c) DI sistemos, skirtos naudoti siekiant įvertinti su fiziniais asmenimis susijusią riziką ir kainodarą gyvybės bei sveikatos draudimo atveju;

d) DI sistemos, skirtos naudoti siekiant įvertinti ir klasifikuoti fizinių asmenų pagalbos skambučius ar teikiant arba nustatant prioritetines teiktinas skubias pirmosios pagalbos paslaugas, įskaitant policijos, ugniagesių ir medicinos pagalbos tarnybų paslaugas, taip pat skubios sveikatos priežiūros pacientų medicininio skirstymo sistemas.

6. Teisėsauga, jei jas leidžiama naudoti pagal atitinkamus Sąjungos ar nacionalinės teisės aktus:

a) DI sistemos, skirtos naudoti teisėsaugos institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti teisėsaugos institucijoms įvertinti riziką, kad fizinis asmuo taps nusikalstamų veikų auka, arba tai darant jų vardu;

b) DI sistemos, skirtos naudoti teisėsaugos institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti teisėsaugos institucijoms, kaip poligrafai ar panašios priemonės;

c) DI sistemos, skirtos naudoti teisėsaugos institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti teisėsaugos institucijoms įvertinti įrodymų patikimumą tiriant nusikalstamas veikas arba vykdant baudžiamąjį persekiojimą už jas;

d) DI sistemos, skirtos naudoti teisėsaugos institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti teisėsaugos institucijoms įvertinti fizinio asmens nusikalstamumo ar pakartotinio nusikalstamumo riziką remiantis ne tik fizinių asmenų profiliavimu, kaip nurodyta Direktyvos (ES) 2016/680 3 straipsnio 4 dalyje, arba įvertinti fizinių asmenų arba grupių asmenybės bruožus ir savybes arba ankstesnį nusikalstamą elgesį;

e) DI sistemos, skirtos naudoti teisėsaugos institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti teisėsaugos institucijoms profiliuoti fizinius asmenis, kaip nurodyta Direktyvos (ES) 2016/680 3 straipsnio 4 dalyje, išaiškinant ar tiriant nusikalstamas veikas arba vykdant baudžiamąjį persekiojimą už jas.

7. Migracija, prieglobstis ir sienų kontrolės valdymas, jei DI sistemas leidžiama naudoti pagal atitinkamus Sąjungos ar nacionalinės teisės aktus:

a) DI sistemos, skirtos naudoti kompetentingose valdžios institucijose arba Sąjungos institucijose, įstaigose, organuose ar agentūrose arba jų vardu kaip poligrafai ar panašios priemonės;

b) DI sistemos, skirtos naudoti kompetentingose valdžios institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant įvertinti riziką, įskaitant saugumo riziką, neteisėtos migracijos riziką arba riziką sveikatai, kurią kelia fizinis asmuo, ketinantis atvykti į valstybės narės teritoriją arba į ją atvykęs;

c) DI sistemos, skirtos naudoti kompetentingose valdžios institucijose ar jų vardu arba Sąjungos institucijose, įstaigose, organuose ar agentūrose, siekiant padėti kompetentingoms valdžios institucijoms išnagrinėti prašymus suteikti prieglobstį, išduoti vizą ar leidimus gyventi ir susijusius skundus dėl fizinių asmenų tinkamumo prašyti suteikti tam tikrą statusą, įskaitant susijusius įrodymų patikimumo vertinimus;

d) DI sistemos, skirtos naudoti kompetentingose valdžios institucijose arba Sąjungos institucijose, įstaigose, organuose ar agentūrose arba jų vardu migracijos, prieglobsčio ar sienų kontrolės valdymo kontekste fizinių asmenų aptikimo, atpažinimo arba identifikavimo tikslu, išskyrus kelionės dokumentų tikrinimą.

8. Teisingumo vykdymas ir demokratiniai procesai:

a) DI sistemos, skirtos naudoti teisminėse institucijose arba jų vardu, siekiant padėti teisminei institucijai tirti ir aiškinti faktus bei įstatymus ir taikyti įstatymus konkretiems faktų rinkiniams, arba skirtas naudoti panašiu būdu alternatyvaus ginčų sprendimo procese;

b) DI sistemos, skirtos naudoti siekiant daryti įtaką rinkimų ar referendumų rezultatams arba fizinių asmenų balsavimo elgsenai, kai jie balsuoja rinkimuose ar referendumuose. Tai neapima DI sistemų, kurių išvediniai fiziniams asmenims neturi tiesioginio poveikio, pavyzdžiui, priemonių, naudojamų politinėms kampanijoms organizuoti, optimizuoti ar struktūrizuoti administraciniu ar logistiniu požiūriu.

IV PRIEDAS

11 straipsnio 1 dalyje nurodyti techniniai dokumentai

11 straipsnio 1 dalyje nurodytuose techniniuose dokumentuose pateikiama bent ši informacija, kuri taikoma atitinkamai DI sistemai:

1. bendras DI sistemos aprašymas, įskaitant:

   a) numatytąją paskirtį, tiekėjo pavadinimą bei sistemos versiją, atspindinčią jos ryšį su ankstesnėmis versijomis;

   b) kai taikytina, tai, kaip DI sistema sąveikauja su aparatine arba programine įranga, be kita ko, su kitomis DI sistemomis, kurios nėra pačios DI sistemos sudedamoji dalis, arba kaip ji gali būti naudojama, kad sąveikautų su tokia įranga;

   c) atitinkamos programinės įrangos arba aparatinės programinės įrangos versijas ir su versijos atnaujinimais susijusius bet kokius reikalavimus;

   d) visų DI sistemos pateikimo rinkai arba pradėjimo naudoti formų, pvz., į aparatinę įrangą instaliuotų programinės įrangos paketų, parsisiuntimų ar API, aprašymą;

   e) aparatinės įrangos, kurią naudojant numatoma naudoti DI sistemą, aprašymą;

   f) jeigu DI sistema yra gaminių komponentas, nuotraukas arba iliustracijas, kuriose matomi tų gaminių išorės požymiai, ženklinimas ir vidaus sandara;

g) diegėjui pateiktos naudotojo sąsajos pagrindinį aprašymą;

h) diegėjui skirtos naudojimo instrukcijos ir, kai taikytina, diegėjui pateiktos naudotojo sąsajos pagrindinį aprašymą;

2. išsamus DI sistemos ir jos kūrimo proceso elementų aprašymas, įskaitant:

a) metodus ir etapus, susijusius su DI sistemos kūrimu, įskaitant, kai aktualu, iš anksto apmokytų sistemų arba įrankių, kuriuos suteikė trečiosios šalys, naudojimą ir tai, kaip tiekėjas juos panaudojo, integravo arba pakeitė;

b) sistemos modelio specifikacijas, būtent bendrą DI sistemos ir algoritmų logiką; pagrindinius projektavimo sprendimus, įskaitant loginį pagrindą ir prielaidas, be kita ko, dėl asmenų ar asmenų grupių, kurių atžvilgiu sistema skirta naudoti; pagrindinius klasifikacijos sprendimus; tai, ką sistema siekiama optimizuoti, ir įvairių parametrų svarbą; numatomo sistemos išvedinio ir išvedinio kokybės aprašymą; sprendimus dėl bet kokių galimų kompromisų, susijusių su techniniais sprendimais, kurie buvo įgyvendinti siekiant laikytis III skyriaus 2 skirsnyje nustatytų reikalavimų;

c) sistemos architektūros aprašymą, kuriame paaiškinama, kaip programinės įrangos komponentai remiasi vienas kitu arba kaip papildo vienas kitą ir kaip jie integruoti į visą apdorojimo procesą; kompiuterinio apdorojimo išteklius, kurie buvo naudojami DI sistemai kurti, mokyti, bandyti ir validuoti;

d) kai aktualu, duomenų reikalavimus, nustatytus duomenų lapuose, kuriuose aprašomos mokymo metodikos ir būdai, ir naudojamus mokymo duomenų rinkinius, įskaitant bendrą šių duomenų rinkinių aprašymą, informaciją apie jų kilmę, taikymo sritį ir pagrindinius ypatumus; tai, kaip duomenys buvo gauti ir atrinkti; ženklinimo procedūras (pvz., prižiūrimojo mokymosi), duomenų valymo metodikas (pvz., išskirčių nustatymas);

e) žmogaus atliekamos priežiūros priemonių, reikalingų pagal 14 straipsnį, vertinimą, įskaitant techninių priemonių, kurios reikalingos siekiant padėti diegėjams interpretuoti DI sistemų išvedinius pagal 13 straipsnio 3 dalies d punktą, vertinimą;

f) kai taikytina, išsamų iš anksto nustatytų DI sistemos ir jos veikimo efektyvumo pakeitimų aprašymą, įskaitant visą atitinkamą informaciją, susijusią su techniniais sprendimais, įgyvendintais siekiant užtikrinti nuolatinę DI sistemos atitiktį atitinkamiems III skyriaus 2 skirsnyje išdėstytiems reikalavimams;

g) naudotas validavimo ir bandymo procedūras, įskaitant informaciją apie naudotus validavimo ir bandymo duomenis ir jų pagrindines charakteristikas; metriką, kuri buvo naudota tikslumui, patvarumui ir atitikčiai kitiems susijusiems reikalavimams, nustatytiems III skyriaus 2 skirsnyje, taip pat galimam diskriminaciniam poveikiui įvertinti; bandymų žurnalus ir visas bandymų ataskaitas, kuriuose nurodoma data ir kuriuos pasirašo atsakingi asmenys, taip pat atsižvelgiant į f punkte nurodytus iš anksto nustatytus pakeitimus;

h) taikomas kibernetinio saugumo priemones;

3. išsami informacija apie DI sistemos stebėseną, veikimą ir kontrolę, visų pirma atsižvelgiant į: jos veikimo efektyvumo pajėgumus ir ribotumus, įskaitant tikslumo laipsnius konkrečių asmenų arba asmenų grupių, kurių atžvilgiu numatoma naudoti sistemą, atveju ir bendrą tikėtiną tikslumo lygį, atsižvelgiant į numatytąją paskirtį; įmanomas numatyti nepageidaujamas pasekmes ir rizikos sveikatai ir saugai, pagrindinėms teisėms ir susijusius su diskriminacija šaltinius, atsižvelgiant į DI sistemos numatytąją paskirtį; žmogaus atliekamos priežiūros priemones, reikalingas pagal 14 straipsnį, įskaitant įdiegtas technines priemones, siekiant padėti diegėjams interpretuoti DI sistemų išvedinius; kai tinkama, įvesties duomenų specifikacijas;

4. konkrečios DI sistemos veikimo efektyvumo metrikos tinkamumo aprašymas;

5. išsamus rizikos valdymo sistemos aprašymas pagal 9 straipsnį;

6. atitinkamų sistemos pakeitimų, padarytų tiekėjo per jos gyvavimo ciklą, aprašymas;

7. darniųjų standartų, taikomų visa apimtimi ar iš dalies, kurių nuorodos buvo paskelbtos *Europos Sąjungos oficialiajame leidinyje*, sąrašas; jeigu tokie darnieji standartai nebuvo taikomi, išsamus sprendimų, įgyvendintų siekiant laikytis III skyriaus 2 skirsnyje nurodytų reikalavimų, aprašymas, įskaitant kitų taikomų susijusių standartų ir techninių specifikacijų sąrašą;

8. 47 straipsnyje nurodytą ES atitikties deklaracijos kopija;

9. išsamus sistemos, taikomos vertinant DI sistemos veikimo efektyvumą priežiūros po pateikimo rinkai etape pagal 72 straipsnį, aprašymas, įskaitant 72 straipsnio 3 dalyje nurodytą priežiūros po pateikimo rinkai planą.

V PRIEDAS

ES atitikties deklaracija

47 straipsnyje nurodytoje ES atitikties deklaracijoje pateikiama visa toliau nurodyta informacija:

1. DI sistemos pavadinimas, tipas ir bet kuri papildoma vienareikšmiška nuoroda, sudaranti sąlygas identifikuoti DI sistemą ir užtikrinti jos atsekamumą;

2. tiekėjo arba, kai taikytina, jo įgaliotojo atstovo pavadinimas (vardas ir pavardė) ir adresas;

3. pareiškimas, kad 47 straipsnyje nurodytą ES atitikties deklaracija parengta tik tiekėjo atsakomybe;

4. pareiškimas, kad DI sistema atitinka šį reglamentą ir, jei taikytina, kitus atitinkamus Sąjungos teisės aktus, pagal kuriuos numatyta išduoti 47 straipsnyje nurodytą ES atitikties deklaraciją;

5. tais atvejais, kai naudojant DI sistemą tvarkomi asmens duomenys, – pareiškimas, kad DI sistema atitinka reglamentus (ES) 2016/679 ir (ES) 2018/1725 bei Direktyvą (ES) 2016/680;

6. nuoroda į bet kuriuos naudojamus susijusius darniuosius standartus arba bet kurią kitą bendrąją specifikaciją, atitiktis kuriems yra deklaruojama;

7. kai taikytina, notifikuotosios įstaigos pavadinimas ir identifikacinis numeris, atliktos atitikties vertinimo procedūros aprašymas ir išduoto sertifikato identifikaciniai duomenys;

8. deklaracijos parengimo vieta ir data, ją pasirašiusio asmens vardas, pavardė ir pareigos, taip pat duomenys apie tai, kieno vardu jis pasirašė, ir parašas.

VI PRIEDAS

Vidaus kontrole pagrįsta atitikties vertinimo procedūra

1. Vidaus kontrole pagrįsta atitikties vertinimo procedūra – tai 2, 3 ir 4 punktais pagrįsta atitikties vertinimo procedūra.

2. Tiekėjas patikrina, ar nustatyta kokybės valdymo sistema atitinka 17 straipsnio reikalavimus.

3. Tiekėjas nagrinėja techniniuose dokumentuose pateiktą informaciją, kad įvertintų DI sistemos atitiktį atitinkamiems III skyriaus 2 skirsnyje išvardytiems esminiams reikalavimams.

4. Tiekėjas taip pat patikrina, ar 72 straipsnyje nurodytas DI sistemos projektavimo ir kūrimo procesas ir DI sistemos priežiūra po pateikimo rinkai atitinka techninius dokumentus.

VII PRIEDAS

Atitiktis, grindžiama kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu

1. Įvadas

Atitiktis, grindžiama kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu, yra atitikties vertinimo procedūra pagal 2–5 punktus.

2. Apžvalga

Patvirtinta kokybės valdymo sistema, skirta DI sistemoms projektuoti, kurti ir bandyti pagal 17 straipsnį, nagrinėjama pagal 3 punktą ir jai taikoma 5 punkte nurodyta priežiūra. DI sistemos techniniai dokumentai nagrinėjami pagal 4 punktą.

3. Kokybės valdymo sistema

3.1. Tiekėjo paraiškoje nurodomas (pateikiamas):

a) tiekėjo pavadinimas (vardas ir pavardė) ir adresas, o jei paraišką pateikia įgaliotasis atstovas – ir to atstovo pavadinimas (vardas ir pavardė) ir adresas;

b) DI sistemų, kurioms taikoma ta pati kokybės valdymo sistema, sąrašas;

c) kiekvienos DI sistemos, kuriai taikoma ta pati kokybės valdymo sistema, techniniai dokumentai;

d) dokumentai, susiję su kokybės valdymo sistema, kurie apima visus 17 straipsnyje išvardytus aspektus;

e) taikomų procedūrų siekiant užtikrinti, kad kokybės valdymo sistema išliktų tinkama ir veiksminga, aprašymas;

f) rašytinis pareiškimas, kad tokia pati paraiška nebuvo pateikta jokiai kitai notifikuotajai įstaigai.

3.2. Kokybės valdymo sistemą įvertina notifikuotoji įstaiga siekdama nustatyti, ar sistema atitinka 17 straipsnyje nurodytus reikalavimus.

Apie sprendimą pranešama tiekėjui arba jo įgaliotajam atstovui.

Pranešime pateikiamos kokybės valdymo sistemos vertinimo išvados ir motyvuotas sprendimas dėl įvertinimo.

3.3. Tiekėjas toliau įgyvendina ir prižiūri patvirtintą kokybės valdymo sistemą, kad ji išliktų tinkama ir veiksminga.

3.4. Apie bet kokį numatytą patvirtintos kokybės valdymo sistemos arba DI sistemų, kurioms taikoma minėta kokybės valdymo sistema, sąrašo pakeitimą tiekėjas praneša notifikuotajai įstaigai.

Notifikuotoji įstaiga išnagrinėja siūlomus pakeitimus ir nusprendžia, ar pakeista kokybės valdymo sistema ir toliau atitinka 3.2 punkte nurodytus reikalavimus, ar kokybės valdymo sistemą reikia įvertinti iš naujo.

Notifikuotoji įstaiga savo sprendimą praneša tiekėjui. Pranešime pateikiamos pakeitimų nagrinėjimo išvados ir motyvuotas sprendimas dėl įvertinimo.

4. Techninių dokumentų kontrolė.

4.1. Be 3 punkte nurodytos paraiškos, tiekėjas teikia pasirinktai notifikuotajai įstaigai paraišką, kad būtų įvertinti techniniai dokumentai, susiję su DI sistema, kurią tiekėjas ketina pateikti rinkai arba pradėti naudoti ir kuriai taikoma 3 punkte nurodyta kokybės valdymo sistema.

4.2. Paraiškoje nurodoma:

a) tiekėjo pavadinimas (vardas ir pavardė) ir adresas;

b) rašytinis pareiškimas, kad tokia pati paraiška nebuvo pateikta jokiai kitai notifikuotajai įstaigai;

c) techniniai dokumentai, nurodyti IV priede.

4.3. Techninius dokumentus nagrinėja notifikuotoji įstaiga. Kai aktualu ir neviršijama to, kas būtina notifikuotosios įstaigos užduotims atlikti, jai suteikiama visapusiška prieiga prie naudojamų mokymo, validavimo ir bandymo duomenų rinkinių, įskaitant, kai tinkama ir taikant apsaugos priemones, API arba kitas atitinkamas technines priemones ir įrankius, kurie sudaro sąlygas nuotolinei prieigai.

4.4. Nagrinėdama techninius dokumentus notifikuotoji įstaiga gali prašyti, kad tiekėjas pateiktų papildomų įrodymų arba atliktų tolesnius bandymus ir taip sudarytų sąlygas tinkamai įvertinti DI sistemos atitiktį III skyriaus 2 skirsnyje nustatytiems reikalavimams. Visais atvejais, kai notifikuotosios įstaigos netenkina tiekėjo atlikti bandymai, notifikuotoji įstaiga, kai tinkama, pati tiesiogiai atlieka tinkamus bandymus.

4.5. Kai būtina įvertinti didelės rizikos DI sistemos atitiktį III skyriaus 2 skirsnyje nustatytiems reikalavimams, išnaudojus visus kitus pagrįstus atitikties tikrinimo būdus ir paaiškėjus, kad jų nepakanka, ir gavus pagrįstą prašymą, notifikuotajai įstaigai taip pat suteikiama prieiga prie DI sistemos mokymo ir išmokytų modelių, įskaitant atitinkamus sistemos parametrus. Tokiai prieigai taikoma galiojanti Sąjungos teisė dėl intelektinės nuosavybės ir komercinių paslapčių apsaugos.

4.6. Apie notifikuotosios įstaigos sprendimą pranešama tiekėjui arba jo įgaliotajam atstovui. Pranešime pateikiamos techninių dokumentų vertinimo išvados ir motyvuotas sprendimas dėl įvertinimo.

Jeigu DI sistema atitinka III skyriaus 2 skirsnyje nustatytus reikalavimus, notifikuotoji įstaiga išduoda Sąjungos techninių dokumentų įvertinimo sertifikatą. Sertifikate nurodomas tiekėjo pavadinimas (vardas ir pavardė) ir adresas, nagrinėjimo išvados, jo galiojimo sąlygos (jei yra) ir DI sistemos identifikavimui būtini duomenys.

Sertifikate ir jo prieduose pateikiama visa atitinkama informacija, kad būtų sudarytos sąlygos DI sistemos atitikčiai įvertinti ir, kai taikytina, DI sistemai kontroliuoti tuo metu, kai ji naudojama.

Jeigu DI sistema neatitinka III skyriaus 2 skirsnyje nustatytų reikalavimų, notifikuotoji įstaiga atsisako išduoti Sąjungos techninių dokumentų įvertinimo sertifikatą ir atitinkamai informuoja pareiškėją, nurodydama išsamias atsisakymo priežastis.

Jeigu DI sistema neatitinka reikalavimo, susijusio su jos mokymui naudotais duomenimis, prieš pateikiant paraišką dėl naujo DI sistemos atitikties vertinimo, sistema turės būti pakartotinai mokoma. Šiuo atveju notifikuotosios įstaigos pagrįstame sprendime dėl vertinimo, kuriuo atsisakoma išduoti Sąjungos techninių dokumentų įvertinimo sertifikatą, nurodomos konkrečios aplinkybės, susijusios su duomenų, naudotų mokant DI sistemą, kokybe, visų pirma su neatitikties priežastimis.

4.7. Bet kurį DI sistemos pakeitimą, kuris galėtų turėti įtakos DI sistemos atitikčiai reikalavimams arba jos numatytajai paskirčiai, įvertina Sąjungos techninių dokumentų įvertinimo sertifikatą išdavusi notifikuotoji įstaiga. Tiekėjas informuoja tokią notifikuotąją įstaigą apie savo ketinimą atlikti bet kurį iš pirmiau minėtų pakeitimų arba jeigu jis kitais būdais sužino apie tokius pakeitimus. Notifikuotoji įstaiga įvertina numatomus pakeitimus ir nusprendžia, ar dėl tų pakeitimų reikia atlikti naują atitikties vertinimą pagal 43 straipsnio 4 dalį, ar dėl jų galima išduoti Sąjungos techninių dokumentų įvertinimo sertifikato papildymą. Pastaruoju atveju notifikuotoji įstaiga įvertina pakeitimus, praneša tiekėjui apie savo sprendimą ir, jei pakeitimai patvirtinami, pateikia jam Sąjungos techninių dokumentų įvertinimo sertifikato papildymą.

5. Patvirtintos kokybės valdymo sistemos priežiūra.

5.1. Notifikuotosios įstaigos atliekamos priežiūros pagal 3 punktą tikslas – užtikrinti, kad tiekėjas tinkamai laikytųsi patvirtintos kokybės valdymo sistemos sąlygų.

5.2. Vertinimo tikslais tiekėjas leidžia notifikuotajai įstaigai patekti į patalpas, kuriose kuriamos, plėtojamos ir bandomos DI sistemos. Tiekėjas su notifikuotąja įstaiga toliau dalijasi visa būtina informacija.

5.3. Siekdama užtikrinti, kad tiekėjas nuolat taikytų kokybės valdymo sistemą, notifikuotoji įstaiga periodiškai vykdo auditą ir tiekėjui pateikia audito ataskaitas. Šių auditų kontekste notifikuotoji įstaiga gali atlikti papildomus DI sistemos, dėl kurios buvo išduotas Sąjungos techninių dokumentų įvertinimo sertifikatas, bandymus.

VIII PRIEDAS

Informacija, kurią reikia pateikti užregistravus didelės rizikos
DI sistemas pagal 49 straipsnį

A skirsnis. Informacija, kurią didelės rizikos DI sistemų tiekėjai turi pateikti pagal 49 straipsnio 1 dalį

Toliau nurodyta informacija dėl didelės rizikos DI sistemų, kurias reikia užregistruoti pagal 49 straipsnio 1 dalį, turi būti pateikiama ir paskui nuolat atnaujinama:

1. tiekėjo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

2. kai informaciją pateikia kitas asmuo tiekėjo vardu – to asmens (vardas ir pavardė), adresas ir kontaktiniai duomenys;

3. kai taikytina, įgaliotojo atstovo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

4. DI sistemos prekybinis pavadinimas ir bet kuri papildoma vienareikšmiška nuoroda, sudaranti sąlygas identifikuoti DI sistemą ir užtikrinti jos atsekamumą;

5. DI sistemos numatytosios paskirties ir naudojant šią DI sistemą palaikomų komponentų bei funkcijų aprašymas;

6. būtiniausias glaustas sistemos naudojamos informacijos (duomenų, įvedinių) ir jos veikimo logikos aprašymas;

7. DI sistemos statusas (pateikta rinkai arba naudojama; nebeteikiama rinkai / nebenaudojama, atšaukta);

8. notifikuotosios įstaigos išduoto sertifikato rūšis, numeris ir galiojimo pabaigos data ir, kai taikytina, tos notifikuotosios įstaigos pavadinimas arba identifikacinis numeris;

9. kai taikytina, 8 punkte nurodyto sertifikato skenuota kopija;

10. valstybės narės, kuriose DI sistema buvo pateikta rinkai, pradėta naudoti arba yra patiekta Sąjungoje;

11. 47 straipsnyje nurodytos ES atitikties deklaracijos kopija;

12. elektroninės naudojimo instrukcijos. Ši informacija neteikiama dėl didelės rizikos DI sistemų, naudojamų teisėsaugos ar migracijos, prieglobsčio ir sienų kontrolės valdymo, kaip nurodyta III priedo 1, 6 ir 7 punktuose, srityse;

13. URL, kaip papildoma informacija (neprivaloma).

B skirsnis. Informacija dėl didelės rizikos DI sistemų,
kurią tiekėjai turi pateikti pagal 49 straipsnį

Toliau nurodyta informacija dėl DI sistemų, kurias reikia užregistruoti pagal 49 straipsnio 2 dalį, turi būti pateikiama ir paskui nuolat atnaujinama:

1. tiekėjo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

2. kai informaciją pateikia kitas asmuo tiekėjo vardu – to asmens pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys,

3. kai taikytina, įgaliotojo atstovo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

4. DI sistemos prekybinis pavadinimas ir bet kuri papildoma vienareikšmiška nuoroda, sudaranti sąlygas identifikuoti DI sistemą ir užtikrinti jos atsekamumą;

5. DI sistemos numatytosios paskirties aprašymas;

6. 6 straipsnio 3 dalyje nustatyta sąlyga ar sąlygos, kuriomis remiantis DI sistema laikoma ne didelės rizikos sistema;

7. trumpa pagrindų, kuriais remiantis DI sistema laikoma ne didelės rizikos sistema taikant procedūrą pagal 6 straipsnio 3 dalį, santrauka;

8. DI sistemos statusas (pateikta rinkai arba naudojama; nebeteikiama rinkai / nebenaudojama, atšaukta);

9. valstybės narės, kuriose DI sistema yra pateikta rinkai, pradedama arba yra pradėta naudoti arba tiekiama arba yra patiekta Sąjungoje.

C skirsnis. Informacija dėl didelės rizikos DI sistemų, kurią diegėjai turi pateikti pagal 49 straipsnio 3 dalį

Toliau nurodyta informacija dėl didelės rizikos DI sistemų, kurias reikia užregistruoti pagal 49 straipsnį, turi būti pateikiama ir paskui nuolat atnaujinama:

1. diegėjo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

2. diegėjo vardu informaciją teikiančio asmens (vardas ir pavardė), adresas ir kontaktiniai duomenys;

3. DI sistemos ES duomenų bazėje URL, kurį pateikia jos tiekėjas;

4. poveikio pagrindinėms teisėms vertinimo, atlikto pagal 27 straipsnį, išvadų santrauka;

5. jei taikytina, poveikio duomenų apsaugai vertinimo, atlikto pagal Reglamento (ES) 2016/679 35 straipsnį arba Direktyvos (ES) 2016/680 27 straipsnį, kaip nurodyta šio reglamento 26 straipsnio 8 dalyje, santrauka.

IX PRIEDAS

Informacija, kurią reikia pateikti registruojant III priede išvardytas didelės rizikos DI sistemas, kiek tai susiję su bandymu realiomis sąlygomis pagal 60 straipsnį

Turi būti pateikiama ir po to nuolat atnaujinama toliau nurodyta informacija, susijusi su bandymu realiomis sąlygomis, kuris turi būti užregistruotas pagal 60 straipsnį:

1. visoje Sąjungoje taikomas vienintelis unikalusis bandymo realiomis sąlygomis identifikacinis numeris;

2. tiekėjo arba galimo tiekėjo ir diegėjų, dalyvaujančių bandyme realiomis sąlygomis, pavadinimas (vardas ir pavardė) ir kontaktiniai duomenys;

3. trumpas DI sistemos bei jos numatytosios paskirties aprašymas ir kita informacija, būtina sistemai identifikuoti;

4. bandymo realiomis sąlygomis plano pagrindinių charakteristikų santrauka;

5. informacija apie bandymo realiomis sąlygomis sustabdymą arba nutraukimą.

X PRIEDAS

Sąjungos teisėkūros procedūra priimami aktai dėl didelės apimties IT sistemų laisvės, saugumo ir teisingumo srityse

1. Šengeno informacinė sistema

   a) 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1860 dėl Šengeno informacinės sistemos naudojimo neteisėtai esančių trečiųjų šalių piliečių grąžinimui (OL L 312, 2018 12 7, p. 1);

   b) 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1861 dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo patikrinimams kertant sieną, kuriuo iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir iš dalies keičiamas bei panaikinamas Reglamentas (EB) Nr. 1987/2006 (OL L 312, 2018 12 7, p. 14);

   c) 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1862 dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo policijos bendradarbiavimui ir teisminiam bendradarbiavimui baudžiamosiose bylose, kuriuo iš dalies keičiamas ir panaikinamas Tarybos sprendimas 2007/533/TVR ir panaikinamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1986/2006 ir Komisijos sprendimas 2010/261/ES (OL L 312, 2018 12 7, p. 56).

2. Vizų informacinė sistema

a) 2021 m. liepos 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/1133, kuriuo iš dalies keičiami reglamentai (ES) Nr. 603/2013, (ES) 2016/794, (ES) 2018/1862, (ES) 2019/816 ir (ES) 2019/818, kiek tai susiję su prieigos prie kitų ES informacinių sistemų Vizų informacinės sistemos tikslais sąlygų nustatymu (OL L 248, 2021 7 13, p. 1);

b) 2021 m. liepos 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/1134, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 767/2008, (EB) Nr. 810/2009, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1860, (ES) 2018/1861, (ES) 2019/817 ir (ES) 2019/1896 ir panaikinami Tarybos sprendimai 2004/512/EB ir 2008/633/TVR siekiant reformuoti Vizų informacinę sistemą (OL L 248, 2021 7 13, p. 11).

3. Sistema EURODAC

… m. … … d. Europos Parlamento ir Tarybos reglamento (ES) 2024/… dėl biometrinių duomenų lyginimo sistemos EURODAC sukūrimo siekiant veiksmingai taikyti Europos Parlamento ir Tarybos reglamentus (ES) 2024/… bei (ES) 2024/… ir Tarybos direktyvą 2001/55/EB ir nustatyti neteisėtai esančius trečiųjų šalių piliečius ar asmenis be pilietybės ir dėl valstybių narių teisėsaugos institucijų bei Europolo teisėsaugos tikslais teikiamų prašymų palyginti duomenis su sistemos EURODAC duomenimis, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (ES) 2018/1240 ir (ES) 2019/818 ir panaikinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 603/2013[+].

4. Atvykimo ir išvykimo sistema

2017 m. lapkričio 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2226, kuriuo sukuriama atvykimo ir išvykimo sistema (AIS), kurioje registruojami trečiųjų šalių piliečių, kertančių valstybių narių išorės sienas, atvykimo ir išvykimo bei atsisakymo leisti jiems atvykti duomenys, nustatomos prieigos prie AIS teisėsaugos tikslais sąlygos ir iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir reglamentai (EB) Nr. 767/2008 ir (ES) Nr. 1077/2011 (OL L 327, 2017 12 9, p. 20).

[+] OL: prašom tekste įrašyti dokumente PE-CONS 15/24 (2016/0132 (COD)) pateikiamo reglamento numerį, o išnašoje – to reglamento numerį, datą, pavadinimą ir OL nuorodą.

5. Europos kelionių informacijos ir leidimų sistema

a) 2018 m. rugsėjo 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1240, kuriuo sukuriama Europos kelionių informacijos ir leidimų sistema (ETIAS) ir iš dalies keičiami reglamentai (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 ir (ES) 2017/2226 (OL L 236, 2018 9 19, p. 1);

b) 2018 m. rugsėjo 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1241, kuriuo iš dalies keičiamas Reglamentas (ES) 2016/794 siekiant sukurti Europos kelionių informacijos ir leidimų sistemą (ETIAS) (OL L 236, 2018 9 19, p. 72).

6. Europos nuosprendžių registrų informacinė sistema trečiųjų šalių piliečiams ir asmenims be pilietybės

2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/816, kuriuo Europos nuosprendžių registrų informacinei sistemai papildyti sukuriama centralizuota valstybių narių, turinčių informacijos apie priimtus trečiųjų šalių piliečių ir asmenų be pilietybės apkaltinamuosius nuosprendžius, nustatymo sistema (ECRIS-TCN) ir kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726 (OL L 135, 2019 5 22, p. 1).

7. Sąveikumas

a) 2019 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/817 dėl ES informacinių sistemų sienų ir vizų srityje sąveikumo sistemos sukūrimo, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 ir (ES) 2018/1861 ir Tarybos sprendimai 2004/512/EB ir 2008/633/TVR (OL L 135, 2019 5 22, p. 27);

b) 2019 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/818 dėl ES informacinių sistemų policijos ir teisminio bendradarbiavimo, prieglobsčio ir migracijos srityje sąveikumo sistemos sukūrimo, kuriuo iš dalies keičiami reglamentai (ES) 2018/1726, (ES) 2018/1862 ir (ES) 2019/816 (OL L 135, 2019 5 22, p. 85).

XI PRIEDAS

53 straipsnio 1 dalies a punkte nurodyti techniniai dokumentai:
bendrosios paskirties DI modelių tiekėjams skirti techniniai dokumentai

1 skirsnis
Informacija, kurią turi pateikti visi bendrosios paskirties DI modelių tiekėjai

53 straipsnio 1 dalies a punkte nurodytuose techniniuose dokumentuose pateikiama bent ši informacija atitinkamai pagal modelio dydį ir rizikos profilį:

1. bendras bendrosios paskirties DI sistemos aprašymas, be kita ko:

   a) užduotys, kurias turėtų atlikti modelis, ir DI sistemų, į kurias jis gali būti integruojamas, tipas ir pobūdis;

   b) taikytinos priimtinos naudojimo taisyklės;

   c) išleidimo data ir platinimo būdai;

   d) architektūra ir parametrų skaičius;

   e) įvedinių ir išvedinių būdai (pvz., tekstas, vaizdas) ir formatas;

   f) licencija;

2. išsamus 1 punkte nurodyto modelio elementų aprašymas ir atitinkama informacija apie kūrimo procesą, be kita ko, šie elementai:

a) techninės priemonės (pvz., naudojimo instrukcijos, infrastruktūra, priemonės), reikalingos bendrosios paskirties DI modeliui integruoti į DI sistemas;

b) modelio projektavimo ir mokymo proceso rengimo specifikacijos, įskaitant mokymo metodiką ir būdus, pagrindinius projektavimo sprendimus, įskaitant loginį pagrindą ir prielaidas; jei taikytina, tai, ką modeliu siekiama optimizuoti, ir įvairių parametrų svarba;

c) kai taikytina, informacija apie mokymui, bandymui ir validavimui naudotus duomenis, įskaitant duomenų tipą bei kilmę ir priežiūros metodikas (pvz., valymą, filtravimą ir t. t.), duomenų taškų skaičių, jų apimtį ir pagrindinius ypatumus; kai taikytina, tai, kaip buvo gauti ir atrinkti duomenys, taip pat visos kitos priemonės, skirtos aptikti duomenų šaltinių ir metodų netinkamumą nustatytinam šališkumui aptikti;

d) kompiuterinio apdorojimo ištekliai, naudojami modeliui mokyti (pvz., slankiojo kablelio operacijų skaičius, mokymo laikas ir kita su mokymu susijusi informacija;

e) žinomas arba apskaičiuotas modelio energijos suvartojimas.

Atsižvelgiant į e punktą, kai modelio suvartojamos energijos kiekis nežinomas, energijos suvartojimas gali būti grindžiamas informacija apie naudojamus kompiuterinio apdorojimo išteklius.

2 skirsnis

Papildoma informacija, kurią turi pateikti
sisteminės rizikos bendrosios paskirties DI modelių tiekėjai

1. Išsamus vertinimo strategijų aprašymas, įskaitant vertinimo rezultatus, remiantis viešai prieinamais vertinimo protokolais ir priemonėmis arba kitomis vertinimo metodikomis. Vertinimo strategijos apima vertinimo kriterijus, metrikas ir ribotumų nustatymo metodiką.

2. Kai taikytina, išsamus priemonių, kurių imamasi siekiant atlikti vidaus ir (arba) išorės atsparumo kenksmingiems veiksmams bandymus (pvz., etišką įsilaužimą), modelių adaptavimo, įskaitant suderinimą ir pritaikymą, aprašymas.

3. Kai taikytina, išsamus sistemos architektūros aprašymas, kuriame paaiškinama, kaip programinės įrangos komponentai remiasi vienas kitu arba kaip papildo vienas kitą ir kaip jie integruoti į visą apdorojimo procesą.

XII PRIEDAS

53 straipsnio 1 dalies b punkte nurodyta skaidrumo informacija:
techniniai dokumentai, skirti bendrosios paskirties DI modelių tiekėjams,
tolesnės grandies tiekėjams, kurie integruoja modelį į savo DI sistemą

53 straipsnio 1 dalies b punkte nurodyta informacija yra bent ši informacija:

1. bendras bendrosios paskirties DI sistemos aprašymas, be kita ko:

   a) užduotys, kurias turėtų atlikti modelis, ir DI sistemų, į kurias jis gali būti integruojamas, tipas ir pobūdis;

   b) taikytinos priimtinos naudojimo taisyklės;

   c) išleidimo data ir platinimo būdai;

   d) kai taikytina, tai, kaip modelis sąveikauja su aparatine arba programine įranga, kuri nėra paties modelio sudedamoji dalis, arba kaip jis gali būti naudojamas, kad sąveikautų su tokia įranga;

   e) kai taikytina, atitinkamos programinės įrangos, susijusios su bendrosios paskirties DI modelio naudojimu, versijos;

   f) architektūra ir parametrų skaičius;

   g) įvedinių ir išvedinių būdai (pvz., tekstas, vaizdas) ir formatas;

   h) modelio licencija.

2. modelio ir jo kūrimo proceso elementų aprašymas, be kita ko:

   a) techninės priemonės (pvz., naudojimo instrukcijos, infrastruktūra, priemonės), reikalingos bendrosios paskirties DI modeliui integruoti į DI sistemas;

   b) įvedinių ir išvedinių būdai (pvz., tekstas, vaizdas ir kt.) ir formatas bei didžiausias jų dydis (pvz., konteksto lango dydis ir t. t.);

   c) kai taikytina, informacija apie mokymo, bandymo ir validavimo tikslais naudotus duomenis, įskaitant duomenų tipą ir kilmę bei priežiūros metodikas.

XIII PRIEDAS

51 straipsnyje nurodytų sisteminės rizikos
bendrosios paskirties DI modelių priskyrimo nurodymo kriterijai

Siekdama nustatyti, ar bendrosios paskirties DI modelio pajėgumai arba poveikis yra lygiaverčiai 51 straipsnio 1 dalies a punkte nustatytiems pajėgumams arba poveikiui, Komisija atsižvelgia į šiuos kriterijus:

a) modelio parametrų skaičių;

b) duomenų rinkinio kokybę ar dydį, pavyzdžiui, matuojamą žetonais;

c) modelio mokymui naudotą bendrą skaičiuojamąją galią, matuojamą slankiojo kablelio operacijomis, arba nurodomą kitų kintamųjų deriniu, pvz., numatoma mokymo kaina, mokymui reikalingu numatomu laiku arba numatomu energijos suvartojimu mokymui;

d) modelio įvedinių ir išvedinių būdus, pvz., iš teksto į tekstą (didieji kalbos modeliai), iš teksto į vaizdą, daugiabūviškumą ir pažangiausias ribines vertes, pagal kurias nustatomi kiekvieno būdo pajėgumai daryti didelį poveikį, ir konkretų įvedinių ir išvedinių tipą (pvz., biologines sekas);

e) modelio pajėgumų lyginamuosius parametrus ir vertinimus, be kita ko, atsižvelgiant į užduočių, atliekamų be papildomo mokymo, skaičių, gebėjimą išmokti atlikti naujas, skirtingas užduotis, jo savarankiškumo ir išplečiamumo lygį, priemones, kuriomis jis gali naudotis;

f) tai, ar jis daro didelį poveikį vidaus rinkai dėl jo aprėpties, kuri preziumuojama, kai modelis pateikiamas bent 10 000 Sąjungoje įsisteigusių registruotų verslo klientų;

g) registruotų galutinių naudotojų skaičių.