Europos Sąjungos
Taryba

Briuselis, 2022 m. gruodžio 6 d.
(OR. en)

15698/22

Tarpinstitucinė byla:
2021/0106(COD)

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

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2022 m. gruodžio 6 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	14954/22 + ADD 1
Komisijos dok. Nr.:	8115/21
Dalykas:	Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai – Bendras požiūris (2022 m. gruodžio 6 d.)

Delegacijoms priede pateikiamas Tarybos bendras požiūris dėl pirmiau nurodyto pasiūlymo, kurį 2022 m. gruodžio 6 d. įvykusiame 3917-ame posėdyje patvirtino Taryba (Transportas, telekomunikacijos ir energetika).

Šiuo bendru požiūriu nustatoma Tarybos preliminari pozicija dėl šio pasiūlymo ir juo remiantis bus rengiamasi deryboms su Europos Parlamentu.

PRIEDAS

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

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

(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 Regionų komiteto nuomonę[2],

atsižvelgdami į Europos Centrinio Banko nuomonę[3],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

[1] OL C […], […], p. […].
[2] OL C […], […], p. […].
[3] Nuoroda į ECB nuomonę.

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

(2) dirbtinio intelekto sistemos (DI sistemos) gali būti lengvai įdiegtos įvairiuose ekonomikos ir visuomenės sektoriuose, taip pat tarpvalstybiniu mastu, ir jos gali plisti visoje Sąjungoje. Tam tikros valstybės narės jau išnagrinėjo galimybę priimti nacionalines taisykles, siekiant užtikrinti, kad dirbtinis intelektas būtų saugus ir kuriamas bei naudojamas laikantis pagrindinių teisių ir pareigų. Dėl skirtingų nacionalinių taisyklių vidaus rinkoje gali atsirasti susiskaidymas ir sumažėti DI sistemas kuriančių, importuojančių ar naudojančių veiklos vykdytojų teisinis tikrumas. Todėl visoje Sąjungoje reikėtų užtikrinti nuoseklią ir aukšto lygio apsaugą ir reikėtų užkirsti kelią skirtumams, trukdantiems DI sistemoms ir susijusiems gaminiams ir paslaugoms laisvai cirkuliuoti vidaus rinkoje, nustatant vienodas pareigas veiklos vykdytojams ir garantuojant vienodą svarbių viešojo intereso priežasčių ir asmenų teisių apsaugą visoje vidaus rinkoje, remiantis Sutarties dėl Europos Sąjungos (toliau – SESV) veikimo 114 straipsniu. Tiek, kiek šiame reglamente yra konkrečių taisyklių dėl asmenų apsaugos asmens duomenų tvarkymo srityje, susijusių su DI sistemų naudojimo apribojimais, susijusiais su tikruoju laiku viešosiose erdvėse teisėsaugos tikslais naudojamomis nuotolinio biometrinio tapatybės nustatymo sistemomis, šį reglamentą konkrečių taisyklių atveju būtų tinkama grįsti SESV 16 straipsniu. Atsižvelgiant į tas konkrečias taisykles ir rėmimusi SESV 16 straipsniu, yra tinkama konsultuotis su Europos duomenų apsaugos valdyba;

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

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

(5) todėl Sąjungos teisinė sistema, kuria nustatomos suderintos dirbtinio intelekto taisyklės, yra reikalinga siekiant vidaus rinkoje skatinti kurti, naudoti ir įsisavinti dirbtinį intelektą, kartu užtikrinant aukšto lygio viešųjų interesų, kaip antai saugos ir sveikatos apsaugą, ir pagrindinių teisių apsaugą, kaip pripažįstama ir saugoma Sąjungos teisėje. Kad šis tikslas būtų pasiektas, reikėtų nustatyti taisykles, kuriomis reglamentuojamas tam tikrų DI sistemų pateikimas rinkai ir pradėjimas naudojimo, taip užtikrinant sklandų vidaus rinkos veikimą ir leidžiant išnaudoti tų sistemų privalumus, atsižvelgiant į prekių ir paslaugų laisvo judėjimo principą. Nustatant tas taisykles ir remiantis Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais darbu rengiant Patikimo dirbtinio intelekto ES gaires, šiuo reglamentu remiamas Sąjungos tikslas pirmauti pasaulyje kuriant saugų, patikimą ir etišką dirbtinį intelektą, kaip nurodė Europos Vadovų Taryba[4], ir užtikrinama etikos principų apsauga, atsižvelgiant į konkretų Europos Parlamento prašymą[5];

---

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

5 2020 m. spalio 20 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos, 2020/2012(INL).

(5a) šiame reglamente nustatytos suderintos DI sistemų pateikimo rinkai, pradėjimo naudoti ir naudojimo taisyklės turėtų būti taikomos visuose sektoriuose ir, laikantis naujosios teisės aktų sistemos principo, neturėtų daryti poveikio esamiems Sąjungos teisės aktams, visų pirma dėl duomenų apsaugos, vartotojų apsaugos, pagrindinių teisių, užimtumo ir gaminių saugos, kuriuos šis reglamentas papildo. Todėl visos teisės ir teisių gynimo priemonės, pagal tokią Sąjungos teisę suteiktos vartotojams ir kitiems asmenims, kuriems DI sistemos gali daryti neigiamą poveikį, įskaitant galimos žalos atlyginimą pagal 1985 m. liepos 25 d. Tarybos direktyvą 85/374/EEB dėl valstybių narių įstatymų ir kitų teisės aktų, reglamentuojančių atsakomybę už gaminius su trūkumais, derinimo, lieka nepakitusios ir visapusiškai taikomos. Šiuo reglamentu taip pat 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 nacionalinės teisės aktams bei laikantis Sąjungos teisės ir dėl to ribojamas tam tikrų DI sistemų naudojimas, kai tokie teisės aktai nepatenka į šio reglamento taikymo sritį arba jais siekiama kitų teisėtų viešojo intereso tikslų nei tie, kurių siekiama šiuo reglamentu. Pavyzdžiui, šis reglamentas neturėtų daryti poveikio nacionalinei darbo teisei ir nepilnamečių (t. y. jaunesnių nei 18 metų asmenų) apsaugos įstatymams, atsižvelgiant į Jungtinių Tautų bendrąją pastabą Nr. 25 (2021) dėl vaikų teisių, jei jie nėra susiję su DI sistemomis ir jais siekiama kitų teisėtų viešojo intereso tikslų;

(6) DI sistemos sąvoka turėtų būti aiškiai apibrėžta, siekiant užtikrinti teisinį tikrumą, kartu suteikiant lankstumo prisitaikyti prie būsimų technologinių pokyčių. Apibrėžtis turėtų būti grindžiama pagrindinėmis funkcinėmis dirbtinio intelekto charakteristikomis, pavyzdžiui, jo mokymosi, samprotavimo ar modeliavimo pajėgumais, atskiriant jį nuo paprastesnių programinės įrangos sistemų ir programavimo metodų. Visų pirma, šio reglamento tikslais DI sistemos turėtų turėti galimybę, remdamosi mašininiais ir (arba) žmogaus pateikiamais duomenimis ir įvediniais, numanyti, kaip pasiekti tam tikrus galutinius tikslus, kuriuos joms nustato žmonės, taikant mašinų mokymosi principus ir (arba) logika ir žiniomis pagrįstus metodus, ir kurti išvedinius, pavyzdžiui, generacinių DI sistemų turinį (pvz., tekstą, vaizdą ar nuotraukas), prognozes, rekomendacijas ar sprendimus, darančius poveikį aplinkai, su kuria sistema sąveikauja, tiek fiziniu, tiek skaitmeniniu aspektu. Sistema, kurioje operacijoms automatiškai atlikti naudojamos tik fizinių asmenų nustatytos taisyklės, neturėtų būti laikoma DI sistema. DI sistemos gali būti projektuojamos taip, kad veiktų įvairiais autonomijos lygmenimis ir veiktų atskirai arba kaip gaminio komponentas, nepaisant to, ar sistema yra fiziškai integruota (įmontuota) į gaminį arba atlieka gaminio funkciją, tačiau nėra į jį integruota (neįmontuota). DI sistemos savarankiškumo sąvoka susijusi su tokios sistemos gebėjimu veikti nedalyvaujant žmogui;

(6a) taikant mašinų mokymosi principus pirmiausia siekiama kurti sistemas, gebančias mokytis ir remiantis duomenimis daryti išvadas siekiant išspręsti taikymo problemą, jų aiškiai neprogramuojant su nuosekliais nurodymais nuo įvedinių iki išvedinių. Mokymasis – tai skaičiavimo procesas, kai optimizuojant duomenis nustatomi modelio, kuris yra matematinis konstruktas, generuojantis įvediniais pagrįstus išvedinius, parametrai. Mašinų mokymosi būdu sprendžiamos problemos paprastai susijusios su užduotimis, kurioms atlikti kiti metodai netinka dėl to, kad problema nėra tinkamai suformuluota, arba dėl to, kad problemos negalima išspręsti taikant su mokymusi nesusijusius metodus. Mašinų mokymosi principai apima, pavyzdžiui, prižiūrimą, neprižiūrimą ir sustiprintąjį mokymąsi, naudojant pačius įvairiausius metodus, įskaitant gilųjį mokymąsi pasitelkiant neuroninius tinklus, statistinius mokymosi metodus ir numanymą (įskaitant, pavyzdžiui, logistinę regresiją, Bejeso įvertį) ir paieškos bei optimizavimo metodus;

(6b) taikant logika ir žiniomis pagrįstus metodus pirmiausia siekiama kurti sistemas, turinčias žiniomis pagrįsto loginio samprotavimo gebėjimų, kad būtų galima išspręsti taikymo problemą. Tokios sistemos paprastai apima žinių bazę ir išvadų variklį, kuris remdamasis žinių baze samprotauja ir generuoja išvedinius. Žinių bazę, kurią paprastai suprogramuoja ekspertai žmonės, sudaro subjektai ir loginiai ryšiai, kurie yra svarbūs taikymo problemai, naudojant formalius parametrus, pagrįstus taisyklėmis, ontologijomis ar žinių grafikais. Išvadų variklis veikia remdamasis žinių baze ir gauna naują informaciją atlikdamas tokias operacijas, kaip rūšiavimas, paieška, derinimas arba sujungimas. Logika ir žiniomis pagrįsti metodai apima, pavyzdžiui, žinių pateikimą, induktyvųjį (loginį) programavimą, žinių bazes, išvadų ir dedukcinius mechanizmus, (simbolinį) argumentavimą, ekspertų sistemas ir paieškos bei optimizavimo metodus;

(6c) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, kiek tai susiję su mašinų mokymosi principais ir logika bei žiniomis pagrįstais metodais, ir atsižvelgti į rinkos ir technologinius pokyčius, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai;

(6d) šiame reglamente vartojama sąvoka „naudotojas“ turėtų būti aiškinama kaip bet kuris DI sistemą naudojantis fizinis ar juridinis asmuo, įskaitant valdžios instituciją, agentūrą ar kitą įstaigą, kuriai vadovaujant ta sistema naudojama. Priklausomai nuo DI sistemos rūšies, sistemos naudojimas gali turėti įtakos ne tik naudotojui, bet ir kitiems asmenims;

(7) šiame reglamente vartojama sąvoka „biometriniai duomenys“ turėtų būti aiškinama nuosekliai, kaip sąvoka „biometriniai duomenys“, apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2016/679[6] 4 straipsnio 14 punkte, Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[7] 3 straipsnio 18 punkte ir Europos Parlamento ir Tarybos direktyvos (ES) 2016/680[8] 3 straipsnio 13 punkte;

[6] 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).

[7] 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).

[8] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (Teisėsaugos direktyva) (OL L 119, 2016 5 4, p. 89).

(8) šiame reglamente vartojama nuotolinio biometrinio tapatybės nustatymo sistemos sąvoka turėtų būti apibrėžta funkciniu požiūriu, kaip DI sistema, skirta fizinių asmenų tapatybei paprastai nuotoliniu būdu nustatyti, šiuo tikslu, jiems aktyviai nedalyvaujant, palyginant asmens biometrinius duomenis su informacinėje duomenų saugykloje esančiais biometriniais duomenimis, nepriklausomai nuo naudojamos konkrečios technologijos, procesų arba biometrinių duomenų rūšies. Tokios nuotolinio biometrinio tapatybės nustatymo sistemos paprastai naudojamos siekiant vienu metu pastebėti (skenuoti) kelis asmenis arba jų elgesį, kad būtų gerokai lengviau nustatyti tam tikro skaičiaus asmenų tapatybę jiems aktyviai nedalyvaujant. Į tokią apibrėžtį neįtrauktos tikrinimo ir (arba) autentiškumo patvirtinimo sistemos, kurių vienintelis tikslas būtų patvirtinti, kad konkretus fizinis asmuo yra asmuo, kuris jis teigia esąs, taip pat sistemos, naudojamos fizinio asmens tapatybei patvirtinti vien tam, kad jis galėtų naudotis paslauga, prietaisu ar patalpomis. Ši 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 didelio skaičiaus asmenų biometriniams duomenims tvarkyti. Jeigu naudojamos tikralaikės sistemos, biometrinių duomenų rinkimas, lyginimas ir tapatybės nustatymas visuomet vyksta momentiškai, beveik momentiškai arba bet kuriuo atveju be didesnės delsos. Šiuo atžvilgiu neturėtų būti jokių galimybių apeiti šio reglamento taisyklių dėl tikralaikio atitinkamų DI sistemų naudojimo numatant nedidelę delsą. Tikralaikės sistemos yra susijusios su medžiagos naudojimu tiesiogiai arba beveik tiesiogiai, pavyzdžiui, filmuota medžiaga, sukurta naudojant kamerą arba kitą panašią funkciją atliekantį prietaisą. Kita vertus netikralaikių sistemų atveju biometriniai duomenys jau buvo surinkti ir palyginimas bei tapatybės nustatymas atliekami po ilgos delsos. Ji apima medžiagą, pavyzdžiui, nuotraukas arba vaizdo medžiagą, sukurtą naudojant apsaugines vaizdo stebėjimo sistemas arba asmeninius prietaisus prieš pradedant naudoti sistemą atitinkamų fizinių asmenų atžvilgiu;

(9) šiame reglamente sąvoka „viešoji erdvė“ turėtų būti suprantama kaip reiškianti bet kokią fizinę vietą, prieinamą neribotam skaičiui fizinių asmenų, neatsižvelgiant į tai, ar ta vieta yra privati ar vieša, ir neatsižvelgiant į veiklą, kuriai vykdyti ta vieta gali būti naudojama, – pavyzdžiui, prekyba (pvz., parduotuvės, restoranai, kavinės), paslaugos (pvz., bankai, profesinė veikla, svetingumo paslaugos), sportas (pvz., baseinai, sporto salės, stadionai), transportas (pvz., autobusai, metro ir geležinkelio stotys, oro uostai, transporto priemonės), pramogos (pvz., kino teatrai, teatrai, muziejai, koncertų ir konferencijų salės), laisvalaikio ar kitokia veikla (pvz., viešieji keliai ir aikštės, parkai, miškai, žaidimų aikštelės). Vieta turėtų būti laikoma viešąja erdve ir tuo atveju, jei, nepaisant galimų pajėgumų ar saugumo apribojimų, prieigai taikomos tam tikros iš anksto nustatytos sąlygos, kurias gali įvykdyti neribotas skaičius asmenų, pvz., bilieto ar važiavimo teisės įsigijimas, išankstinė registracija arba tam tikra amžiaus riba. Tačiau vieta neturėtų būti laikoma viešąja erdve, jei prieiga suteikiama tik konkretiems ir apibrėžtiems fiziniams asmenims pagal Sąjungos arba nacionalinę teisę, tiesiogiai susijusią su viešuoju ar visuomenės saugumu, arba aiškiai išreiškiant įgaliojimus dėl atitinkamos vietos turinčio asmens valią. Vien faktinė prieigos galimybė (pvz., atrakintos durys, atviri vartai užtvaroje) nereiškia, kad vieta yra viešoji erdvė, esant priešingų požymių ar aplinkybių (pvz., ženklų, kuriais prieiga draudžiama arba ribojama). Įmonių ir gamyklų patalpos, taip pat biurai ir darbo vietos, skirti tik atitinkamiems darbuotojams ir paslaugų teikėjams patekti, – tai vietos, kurios nėra viešosios erdvės. Viešosios erdvės neturėtų apimti kalėjimų ar pasienio kontrolės zonų. Kai kurias kitas zonas gali sudaryti ir neviešosios, ir viešosios erdvės, pavyzdžiui, privataus gyvenamojo pastato koridorius, būtinas norint patekti į gydytojo kabinetą arba oro uostą. Ši nuostata netaikoma internetinei erdvei, nes tai nėra fizinė erdvė. Tačiau tai, ar atitinkama vieta yra viešai prieinama, turėtų būti nustatyta kiekvienu konkrečiu atveju atsižvelgiant į konkrečios nagrinėjamos situacijos ypatumus;

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

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

(12) šis reglamentas taip pat turėtų būti taikomas Sąjungos institucijoms, tarnyboms, įstaigoms ir agentūroms, kai jos veikia kaip DI sistemos tiekėjai arba naudotojai;

(-12a) jei ir tokiu mastu, kokiu DI sistemos pateikiamos rinkai, pradedamos naudoti arba naudojamos tokias sistemas keičiant arba jų nekeičiant kariniais, gynybos ar nacionalinio saugumo tikslais, jos 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 Europos Sąjungos sutarties (toliau – ES sutartis) 4 straipsnio 2 dalimi, tiek valstybių narių ir bendros Sąjungos gynybos politikos, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius, ypatumais, 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 tuo, kad pagal ES sutarties 4 straipsnio 2 dalį už nacionalinį saugumą išimtinai išlieka atsakingos valstybės narės, tiek nacionalinio saugumo veiklos specifiniu pobūdžiu bei veiklos poreikiais ir tai veiklai taikomomis konkrečiomis nacionalinėmis taisyklėmis. 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 sistemą naudoja ne kariniais, gynybos ar nacionalinio saugumo tikslais, turėtų užtikrinti, kad sistema atitiktų šį reglamentą, išskyrus atvejus, kai sistema jau atitinka šį reglamentą. DI sistemos, pateiktos rinkai arba pradėtos naudoti tikslu (t. y. kariniu, gynybos ar nacionalinio saugumo), kuris nepatenka į taikymo sritį, ir vienu ar daugiau tikslų (pvz., civilinių tikslų, teisėsaugos ir kt.), kurie nėra neįtraukti į taikymo sritį, patenka į šio reglamento taikymo sritį ir tų sistemų tiekėjai turėtų užtikrinti, kad šio reglamento būtų laikomasi. Tais atvejais tai, kad DI sistema gali patekti į šio reglamento taikymo sritį, neturėtų daryti poveikio nacionalinio saugumo, gynybos ir karinę veiklą vykdančių subjektų galimybei, neatsižvelgiant į tą veiklą vykdančio subjekto rūšį, naudoti nacionalinio saugumo, kariniams ir gynybos tikslams skirtas 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 tą veiklą vykdančio subjekto rūšį;

(12a) šis reglamentas neturėtų daryti poveikio nuostatoms dėl tarpininkavimo tiekėjų atsakomybės, nustatytos Europos Parlamento ir Tarybos direktyvoje 2000/31/EB [iš dalies pakeistoje Skaitmeninių paslaugų aktu];

(12b) šiuo reglamentu neturėtų būti pakenkta mokslinių tyrimų ir plėtros veiklai ir turėtų būti gerbiama mokslo laisvė. Todėl būtina į jo taikymo sritį neįtraukti DI sistemų, specialiai sukurtų ir pradėtų naudoti tik mokslinių tyrimų ir plėtros tikslais, ir užtikrinti, kad reglamentas kitaip nedarytų poveikio DI sistemų mokslinių tyrimų ir plėtros veiklai. Tiekėjų vykdomai gaminio mokslinių tyrimų veiklai šio reglamento nuostatos taip pat neturėtų būti taikomos. Tai nedaro poveikio pareigai laikytis šio reglamento, kai DI sistema, patenkanti į šio reglamento taikymo sritį, dėl tokios mokslinių tyrimų ir plėtros veiklos pateikiama rinkai arba pradedama naudoti, ir nuostatų dėl apribotų bandomųjų reglamentavimo aplinkų ir bandymų realiomis sąlygomis taikymui. Be to, nedarant poveikio pirmiau išdėstytoms nuostatoms dėl DI sistemų, specialiai sukurtų ir pradėtų naudoti tik mokslinių tyrimų ir plėtros tikslais, bet kuriai kitai DI sistemai, kuri gali būti naudojama bet kokiai mokslinių tyrimų ir plėtros veiklai vykdyti, ir toliau turėtų būti taikomos šio reglamento nuostatos. Bet kokiomis aplinkybėmis bet kokia mokslinių tyrimų ir plėtros veikla turėtų būti vykdoma laikantis pripažintų mokslinių tyrimų etikos ir profesinių standartų;

(12c) atsižvelgiant į DI sistemų vertės grandinės pobūdį ir sudėtingumą, labai svarbu paaiškinti subjektų, kurie gali prisidėti prie DI sistemų, visų pirma didelės rizikos DI sistemų, kūrimo, vaidmenį. Visų pirma būtina paaiškinti, kad bendrosios paskirties DI sistemos – tai DI sistemos, kurios pagal tiekėjo numatytą paskirtį turi atlikti visuotinai taikomas funkcijas, pvz., vaizdo ir (arba) balso atpažinimą, įvairiomis aplinkybėmis. Jos pačios gali būti naudojamos kaip didelės rizikos DI sistemos arba gali būti kitų didelės rizikos DI sistemų komponentai. Todėl dėl ypatingo tokių sistemų pobūdžio ir siekiant užtikrinti teisingą atsakomybės pasidalijimą DI vertės grandinėje, tokioms sistemoms turėtų būti taikomi proporcingi ir konkretesni reikalavimai ir pareigos pagal šį reglamentą, kartu užtikrinant aukšto lygio pagrindinių teisių, sveikatos ir saugos apsaugą. Be to, bendrosios paskirties DI sistemų tiekėjai, nepriklausomai nuo to, ar kiti tiekėjai gali naudoti jas pačias kaip didelės rizikos DI sistemas arba kaip didelės rizikos DI sistemų komponentus, turėtų atitinkamai bendradarbiauti su atitinkamų didelės rizikos DI sistemų tiekėjais, kad jie galėtų vykdyti atitinkamas pareigas pagal šį reglamentą, ir su pagal šį reglamentą nustatytomis kompetentingomis institucijomis. Siekiant atsižvelgti į konkrečias bendrosios paskirties DI sistemų ypatybes ir sparčius rinkos ir technologinius pokyčius šioje srityje, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai patikslinti ir pritaikyti pagal šį reglamentą nustatytų reikalavimų taikymą bendrosios paskirties DI sistemoms ir nustatyti informaciją, kuria turi dalytis bendrosios paskirties DI sistemų tiekėjai, kad atitinkamos didelės rizikos DI sistemos tiekėjai galėtų vykdyti savo pareigas pagal šį reglamentą;

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

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

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

(16) 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 savarankiškumui, sprendimų priėmimui ir laisvam pasirinkimui. Tam tikrų DI sistemų, kuriomis siekiama iš esmės pakeisti žmogaus elgesį, sukeliant tikėtiną fizinę arba psichologinę žalą, pateikimas rinkai, pradėjimas naudoti arba naudojimas yra ypač pavojingas ir todėl turėtų būti draudžiamas. Tokiose DI sistemose naudojami pasąmonę veikiantys komponentai, pavyzdžiui, garso, vaizdo, vaizdo stimuliacijos, kurių žmonės negali suvokti, nes tos stimuliacijos priemonės yra žmogui nesuvokiamos, ar kiti pasąmonę veikiantys metodai, kuriais trukdoma arba kenkiama asmens savarankiškumui, sprendimų priėmimui ar laisvam pasirinkimui tokiais būdais, kurių žmonės sąmoningai nesuvokia arba, net jei suvokia, negali kontroliuoti ar jiems priešintis, pavyzdžiui, mašinos ir proto sąsajų ar virtualiosios realybės atvejais. Be to, DI sistemos taip pat gali kitaip išnaudoti konkrečios asmenų grupės pažeidžiamumą dėl jų amžiaus, negalios, kaip tai suprantama Direktyvoje (ES) 2019/882, arba konkrečios socialinės ar ekonominės padėties, dėl kurios tie asmenys gali būti labiau pažeidžiami išnaudojimo požiūriu, pavyzdžiui, ypač skurdžiai gyvenantys asmenys, etninės ar religinės mažumos. Tokios DI sistemos gali būti pateiktos rinkai, pradėtos naudoti arba naudojamos siekiant iš esmės pakeisti arba pakeičiant asmens elgesį ir tokiu būdu, kuris sukelia arba pagrįstai gali sukelti fizinę ar psichologinę žalą tam ar kitam asmeniui arba asmenų grupėms, įskaitant žalą, kuri laikui bėgant gali didėti. Ketinimas pakeisti elgesį negali būti preziumuojamas, jei pakeitimą lemia su DI sistema nesusiję veiksniai, kurių tiekėjas ar naudotojas negali kontroliuoti, t. y. veiksniai, kurių DI sistemos tiekėjas ar naudotojas negali pagrįstai numatyti ir sušvelninti. Bet kuriuo atveju nebūtina, kad tiekėjas ar naudotojas ketintų sukelti fizinę ar psichologinę žalą, jeigu tokia žala atsiranda dėl manipuliavimo ar išnaudojimo pasitelkiant DI grindžiamas priemones. Tokios DI praktikos draudimai papildo Direktyvos 2005/29/EB nuostatas, visų pirma tai, kad nesąžininga komercinė praktika, daranti ekonominę ar finansinę žalą vartotojams, yra draudžiama bet kokiomis aplinkybėmis, neatsižvelgiant į tai, 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 taikytinų medicinos standartų ir teisės aktų. Be to, įprasta ir teisėta komercinė praktika, kuri atitinka taikytiną teisę, neturėtų būti savaime laikoma DI grindžiama žalinga manipuliavimo praktika;

(17) valdžios institucijoms arba privatiems subjektams naudojant DI sistemas, kurių paskirtis vykdyti fizinių asmenų socialinį reitingavimą, gali būti pasiekti diskriminuojantys rezultatai, o tam tikros grupės gali patirti atskirtį. Taip gali būti pažeista teisė į orumą ir nediskriminavimą ir lygybės bei teisingumo vertybės. Tokiomis DI sistemomis vertinami arba klasifikuojami fiziniai asmenys, remiantis jų socialiniu elgesiu įvairiomis aplinkybėmis arba žinomomis arba nuspėjamomis asmeninėmis ar asmenybės savybėmis. Dėl tokių DI sistemų sukurto socialinio reitingavimo balo gali būti žalingai arba nepalankiai elgiamasi su fiziniais asmenimis arba ištisomis jų grupėmis ir tai gali būti daroma socialinėmis aplinkybėmis, kurios nėra susijusios su aplinkybėmis, kuriomis duomenys buvo iš pradžių sukurti arba surinkti, arba žalingai elgiantis, kai toks elgesys yra neproporcingas arba nepagrįstas atsižvelgiant į jų socialinio elgesio rimtumą. Todėl DI sistemos, kuriose naudojama tokia nepriimtina reitingavimo praktika, turėtų būti uždraustos. Šis draudimas neturėtų daryti poveikio teisėtai fizinių asmenų vertinimo praktikai, vykdomai vienu ar keliais konkrečiais tikslais laikantis teisės aktų;

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

(19) todėl šių sistemų naudojimas teisėsaugos tikslais turėtų būti draudžiamas, išskyrus išsamiai išvardytas ir siaurai apibrėžtas situacijas, kai sistemas naudoti tikrai būtina siekiant apginti esminį viešąjį interesą, kurio svarba nusveria riziką. Šios situacijos apima potencialių nusikaltimo aukų, įskaitant dingusius vaikus, paiešką, tam tikras grėsmes fizinių asmenų gyvybei arba fiziniam saugumui arba teroristinio išpuolio grėsmes ir Tarybos pamatiniame sprendime 2002/584/TVR[9] nurodytų nusikalstamų veikų vykdytojų arba įtariamųjų radimą, buvimo vietos ir tapatybės nustatymą ar baudžiamąjį persekiojimą, jeigu tos nusikalstamos veikos atitinkamoje valstybėje narėje yra baudžiamos skiriant laisvės atėmimo bausmę arba priimant nutartį dėl sulaikymo ne trumpiau nei trejiems metams ir atsižvelgiant į tai, kaip jos apibrėžtos tos valstybės narės teisėje. Tokia laisvės atėmimo bausmės arba nutarties dėl sulaikymo riba, kuri nustatyta nacionalinėje teisėje, padeda užtikrinti, kad nusikalstama veika būtų pakankamai rimta, siekiant pateisinti galimą tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimą. Be to, iš 32 nusikalstamų veikų, išvardytų Tarybos pamatiniame sprendime 2002/584/TVR, kai kurios praktiniu požiūriu gali būti svarbesnės, palyginti su kitomis, atsižvelgiant į tai, kad tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas gali būti būtinas ir proporcingas labai įvairiu mastu siekiant praktiškai išaiškinti įvairių išvardytų nusikalstamų veikų vykdytoją arba įtariamąjį, nustatyti jo buvimo vietą ir tapatybę ar vykdyti baudžiamąjį persekiojimą, kartu atsižvelgiant į tikėtinus žalos arba galimų neigiamų pasekmių rimtumo, tikėtinumo ir masto skirtumus. Be to, šiuo reglamentu turėtų būti išsaugota teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijų galimybė 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 asmens, kuris tapatybės patikrinimo metu atsisako leisti nustatyti jo tapatybę arba kuris negali nurodyti ar įrodyti savo tapatybės, tapatybei nustatyti, nereikalaujant pagal šį reglamentą gauti išankstinį leidimą. Tai galėtų būti, pavyzdžiui, asmuo, susijęs su nusikaltimu, nenorintis arba negalintis dėl nelaimingo atsitikimo ar sveikatos būklės atskleisti savo tapatybės teisėsaugos institucijoms;

[9] 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).

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

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

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

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

(24) bet koks biometrinių duomenų ir kitų asmens duomenų, susijusių su DI sistemų naudojimu biometrinio tapatybės nustatymo tikslais, naudojimas, išskyrus atvejus, kai viešosiose erdvėse teisėsaugos tikslais naudojamos 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 siekiant vienareikšmiškai nustatyti fizinio asmens tapatybę, išskyrus atvejus, kai yra susiklosčiusi viena iš situacijų, nurodytų tų dviejų straipsnių atitinkamose antrose pastraipose;

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

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

(27) didelės rizikos DI sistemos Sąjungos rinkai turėtų būti pateikiamos arba pradedamos naudoti tik jeigu jos atitinka tam tikrus privalomus reikalavimus. Šiais reikalavimais turėtų būti užtikrinama, kad Sąjungoje prieinamos didelės rizikos DI sistemos arba sistemos, kurių išvedinys kitu atveju naudojamas Sąjungoje, nekeltų nepriimtinos rizikos svarbiems Sąjungos interesams, kurie pripažįstami ir saugomi pagal Sąjungos teisę. DI sistemos, kurios įvardytos kaip keliančios didelę riziką, turėtų apimti tik tas sistemas, kurios daro didelį žalingą poveikį Sąjungoje esančių asmenų sveikatai, saugumui ir pagrindinėms teisėms, ir tokiu apribojimu kuo labiau sumažinamas galimas tarptautinės prekybos suvaržymas, jei toks yra;

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

(29) dėl didelės rizikos DI sistemų, kurios yra gaminių arba sistemų saugos komponentai, arba pačios yra gaminiai arba sistemos, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008[10], Europos Parlamento ir Tarybos reglamentas (ES) Nr. 167/2013[11], Europos Parlamento ir Tarybos reglamentas (ES) Nr. 168/2013[12], Europos Parlamento ir Tarybos direktyva 2014/90/ES[13], Europos Parlamento ir Tarybos reglamentas direktyva (ES) 2016/797[14], Europos Parlamento ir Tarybos reglamentas (ES) 2018/858[15], Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139[16] ir Europos Parlamento ir Tarybos reglamentas (ES) 2019/2144[17], tinkama iš dalies pakeisti šiuos aktus, siekiant užtikrinti, kad Komisija, paisydama kiekvieno sektoriaus techninių ir reglamentavimo ypatumų ir nedarydama poveikio esamiems valdymo, atitikties vertinimo ir vykdymo užtikrinimo mechanizmams ir jais nustatytiems įgaliojimams, atsižvelgia į šiame reglamente nustatytus privalomus reikalavimus didelės rizikos DI sistemoms tuo atveju, kai, remdamasi šiais išvardytais aktais, priima bet kokį būsimą deleguotąjį ar įgyvendinimo aktą;

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

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

(31) DI sistemos klasifikavimas kaip keliančios didelę riziką pagal šį reglamentą nebūtinai turėtų reikšti, kad gaminys, kurio saugos komponentas yra DI sistema, arba pati DI sistema yra gaminys, laikomas keliančiu didelę riziką pagal atitinkamame Sąjungos derinamajame teisės akte nustatytus kriterijus, kurie taikomi gaminiui. Tai visų pirma pasakytina apie Europos Parlamento ir Tarybos reglamentą (ES) 2017/745[18] ir Europos Parlamento ir Tarybos reglamentą (ES) 2017/746[19], kuriuose numatyta galimybė trečiajai šaliai atlikti vidutinės rizikos ir didelės rizikos gaminių atitikties vertinimą;

---

18 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).

19 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).

(32) didelės rizikos DI sistemas, išskyrus sistemas, kurios yra gaminių saugos komponentai arba kurios pačios yra gaminiai, tinkama klasifikuoti kaip keliančias didelę riziką, jeigu, atsižvelgiant į jų numatytąją paskirtį, jos kelia žalos asmenų sveikatai ir saugumui arba pagrindinėms teisėms riziką, atsižvelgiant į galimos žalos dydį ir jos pasireiškimo tikimybę, ir į tai, kad šios sistemos naudojamos įvairiose šiame reglamente iš anksto konkrečiai apibrėžtose srityse. Šių sistemų identifikavimas yra grindžiamas ta pačia metodika ir kriterijais, kurie taip pat numatyti bet kuriuose būsimuose didelės rizikos DI sistemų sąrašo pakeitimuose. Taip pat svarbu paaiškinti, kad pagal III priede nurodytus didelės rizikos scenarijus gali būti sistemų, kurios nekelia reikšmingos rizikos pagal tuos scenarijus saugomiems teisiniams interesams, atsižvelgiant į DI sistemos išvedinius. Todėl tik tuo atveju, kai tokie išvediniai yra labai svarbūs (t. y. nėra tik pagalbiniai) atitinkamam veiksmui ar sprendimui, kad saugomiems teisiniams interesams kiltų reikšminga rizika, tokius išvedinius generuojanti DI sistema turėtų būti laikoma didelės rizikos sistema. Pavyzdžiui, kai DI sistemų žmogui teikiamą informaciją sudaro fizinių asmenų profiliavimas, kaip tai suprantama Reglamento (ES) 2016/679 4 straipsnio 4 dalyje, Direktyvos (ES) 2016/680 3 straipsnio 4 dalyje ir Reglamento (ES) 2018/1725 3 straipsnio 5 dalyje, tokia informacija paprastai neturėtų būti laikoma pagalbinio pobūdžio informacija didelės rizikos DI sistemų kontekste, kaip nurodyta III priede. Tačiau, jei DI sistemos išvediniai yra tik nereikšmingi arba nėra svarbūs žmogaus veiksmams ar sprendimams, jie gali būti laikomi tik pagalbiniais, įskaitant, pavyzdžiui, DI sistemas, naudojamas vertimui informaciniais tikslais arba dokumentų tvarkymui;

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

(34) dėl ypatingos svarbos infrastruktūros objektų valdymo ir veikimo pažymėtina, kad juos tinkama klasifikuoti kaip didelės rizikos DI sistemas, skirtas naudoti kaip saugos komponentus valdant ir naudojant Direktyvos dėl ypatingos svarbos subjektų atsparumo I priedo 8 punkte nurodytą ypatingos svarbos skaitmeninę infrastruktūrą, kelių transportą ir vandens, dujų, šilumos ir elektros energijos tiekimą, nes joms sugedus arba sutrikus gali kilti rizika daugelio žmonių gyvybei ir sveikatai ir sukelti didelių įprastos socialinės ir ekonominės veiklos sutrikimų. 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;

(35) švietimo ar profesinio mokymo srityje naudojamos DI sistemos, visų pirma suteikiant prieigą, priimant arba skiriant asmenis į švietimo ir profesinio mokymo įstaigas ar visų lygmenų programas arba siekiant įvertinti asmenų mokymosi rezultatus, turėtų būti laikomos keliančiomis didelę riziką, nes gali nulemti asmenų švietimo ir profesinio kelio kryptį, taigi ir daryti poveikį jų gebėjimui užsitikrinti pragyvenimą. Tokios sistemos, jeigu jos netinkamai sukuriamos ir naudojamos, gali pažeisti teisę į švietimą ir mokymą, taip pat teisę nebūti diskriminuojamam ir jose gali būti atkartojami istoriniai diskriminacijos modeliai;

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

(37) kita sritis, kurioje DI sistemų naudojimui reikia skirti ypatingą dėmesį, yra prieiga prie tam tikrų esminių privačių ir viešųjų paslaugų ir išmokų, būtinų žmonėms tam, kad jie galėtų visapusiškai dalyvauti visuomenėje arba pagerinti savo pragyvenimo lygį, ir galimybė jomis pasinaudoti. Visų pirma DI sistemos, kurios naudojamos fizinių asmenų kredito reitingui arba kreditingumui įvertinti, turėtų būti klasifikuojamos kaip didelės rizikos DI sistemos, nes jomis remiantis asmenims suteikiama prieiga prie finansinių išteklių arba esminių paslaugų, pavyzdžiui, apgyvendinimo, elektros energijos ir telekomunikacijų paslaugų. Dėl šiuo tikslu naudojamų DI sistemų gali būti diskriminuojami asmenys arba grupės ir atkartojami istoriniai diskriminacijos modeliai, pavyzdžiui, dėl rasinės ar etninės kilmės, negalios, amžiaus, seksualinės orientacijos, arba gali būti sukuriamos naujas diskriminacinis poveikis. Atsižvelgiant į labai ribotą poveikio mastą ir rinkoje prieinamas alternatyvas, tinkama taikyti išimtį DI sistemoms, kurias kreditingumo patikimumo ir vertinimo tikslu pradėjo naudoti labai mažos arba mažosios įmonės, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB priede, savo reikmėms. Fiziniai asmenys, prašantys valdžios institucijų suteikti pagrindines viešosios paramos išmokas ir paslaugas, paprastai yra priklausomi nuo šių išmokų ir paslaugų ir santykyje su atsakingomis institucijomis yra pažeidžiamoje padėtyje. Jeigu DI sistemos naudojamos siekiant nustatyti, ar institucija turėtų neskirti tokių išmokų ir paslaugų, sumažinti jų dydį ar apimtį, panaikinti arba susigrąžinti, įskaitant tai, ar naudos gavėjai teisėtai turi teisę gauti tokias išmokas ar paslaugas, tos sistemos gali turėti reikšmingą poveikį asmenų pragyvenimui ir gali pažeisti jų pagrindines teises, pavyzdžiui, teisę į socialinę apsaugą, nediskriminavimą, žmogaus orumą arba veiksmingą teisių gynimą. Todėl šios sistemos turėtų būti klasifikuojamos kaip keliančios didelę riziką. Vis dėlto šis reglamentas neturėtų trukdyti kurti ir naudoti naujoviškus viešojo administravimo metodus, kuriuos būtų galima pritaikyti platesniu mastu naudojant reikalavimus atitinkančias ir saugias DI sistemas, jeigu jos nekelia didelės rizikos juridiniams ir fiziniams asmenims. Galiausiai DI sistemos, kurios naudojamos suteikiant arba nustatant prioritetą teikiant pirmojo skubaus atsako į incidentą paslaugą, taip pat turėtų būti klasifikuojamos kaip keliančios didelę riziką, nes jos sprendimus priima ypač kritinėse situacijose, susijusiose su asmenų gyvybe ir sveikata bei jų turtu. DI sistemos taip pat vis dažniau naudojamos vertinant riziką, susijusią su fiziniais asmenimis ir kainodara gyvybės ir sveikatos draudimo atveju, todėl, jei jos nėra suprojektuotos, sukurtos ir naudojamos tinkamai, jos gali turėti rimtų pasekmių žmonių gyvybei ir sveikatai, įskaitant finansinę atskirtį ir diskriminaciją. Siekiant užtikrinti nuoseklų požiūrį finansinių paslaugų sektoriuje, pirmiau minėta išimtis turėtų būti taikoma labai mažoms arba mažosioms įmonėms, jeigu jos pačios savo reikmėms tiekia ir pradeda naudoti DI sistemą, kad galėtų parduoti savo draudimo produktus;

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

(39) migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos daro poveikį žmonėms, kurie dažnai būna ypač pažeidžiamoje padėtyje ir yra priklausomi nuo kompetentingų valdžios institucijų veiksmų rezultato. Todėl šiomis aplinkybėmis naudojamų DI sistemų tikslumas, nediskriminacinis pobūdis ir skaidrumas yra labai svarbūs, siekiant garantuoti pagarbą asmenų, kuriems daromas poveikis, pagrindinėms teisėms, ypač jų teisei laisvai judėti, teisei nebūti diskriminuojamiems, teisei į privataus gyvenimo ir asmens duomenų apsaugą, teisei į tarptautinę apsaugą ir gerą administravimą. Todėl būtų tinkama didelės rizikos kategorijai priskirti DI sistemas, skirtas naudoti kompetentingoms valdžios institucijoms, kurioms pavestos užduotys migracijos, prieglobsčio ir sienų valdymo srityje, pavyzdžiui, poligrafus ir panašias priemones, arba siekiant nustatyti fizinio asmens emocinę būklę; skirtas įvertinti tam tikrą fizinių asmenų, atvykstančių į valstybės narės teritoriją arba prašančių išduoti vizą ar suteikti prieglobstį, keliamą riziką; skirtas padėti kompetentingoms valdžios institucijoms išnagrinėti prašymus suteikti prieglobstį, išduoti vizą ir leidimus gyventi ir susijusius skundus, siekiant nustatyti, ar fizinis asmuo, kuris prašo tam tikro statuso, atitinka reikalavimus. Migracijos, prieglobsčio ir sienų kontrolės valdymo srityje naudojamos DI sistemos, kurioms taikomas šis reglamentas, turėtų atitikti susijusius procedūrinius reikalavimus, nustatytus Europos Parlamento ir Tarybos direktyvoje 2013/32/ES[20], Europos Parlamento ir Tarybos reglamente (EB) Nr. 810/2009[21] ir kituose susijusiuose teisės aktuose;

[20] 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).

[21] 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).

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

(41) tai, kad DI sistema pagal šį reglamentą klasifikuojama kaip kelianti didelę riziką, neturėtų būti vertinama kaip požymis, iš kurio matyti, kad 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 naudojimo siekiant nustatyti fizinių asmenų emocinę būklę. Bet kuris toks naudojimas turėtų būti tęsiamas tik laikantis iš Chartijos ir taikomų Sąjungos antrinės teisės aktų ir nacionalinės teisės kylančių taikytinų reikalavimų. Nereikėtų manyti, kad šiame reglamente nustatytas teisinis asmens duomenų, kai tinkama, įskaitant specialias asmens duomenų kategorijas, tvarkymo pagrindas, nebent šiame reglamente konkrečiai nurodyta kitaip;

(42) siekiant sumažinti didelės rizikos DI sistemų, pateikiamų arba kitaip pradėtų naudoti Sąjungos rinkoje, keliamą riziką, reikėtų taikyti tam tikrus privalomus reikalavimus, atsižvelgiant į numatytąją sistemos naudojimo paskirtį ir paisant rizikos valdymo sistemos, kurią privalo nustatyti tiekėjas. Visų pirma rizikos valdymo sistemą turėtų sudaryti suplanuotas ir per visą didelės rizikos DI sistemos gyvavimo ciklą vykstantis nuolatinis kartotinis procesas. Šiuo procesu turėtų būti užtikrinta, kad tiekėjas nustatytų ir analizuotų riziką asmenų, kuriems sistema dėl jos numatytosios paskirties gali daryti poveikį, sveikatai, saugai ir pagrindinėms teisėms, įskaitant galimą riziką, kylančią dėl DI sistemos ir aplinkos, kurioje ji veikia, sąveikos, ir atitinkamai priimtų tinkamas rizikos valdymo priemones, atsižvelgdamas į naujausius technikos laimėjimus;

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

(44) kokybiški duomenys turi esminę reikšmę užtikrinant daugybės DI sistemų efektyvų veikimą, ypač tais atvejais, kai naudojami su mokymo modeliais susiję metodai, siekiant užtikrinti, kad didelės rizikos DI sistema veiktų kaip numatyta ir saugiai ir netaptų pagal Sąjungos teisę draudžiamos diskriminacijos šaltiniu. Kokybiškų mokymų, validavimo ir bandymo duomenų rinkinių srityje reikia įgyvendinti tinkamą duomenų valdymo ir administravimo praktiką. Mokymų, validavimo ir bandymo duomenų rinkiniai turėtų būti pakankamai aktualūs, reprezentatyvūs ir turėti tinkamus statistinius ypatumus, įskaitant duomenis apie asmenis arba asmenų grupes, kurių atžvilgiu numatyta naudoti didelės rizikos DI sistemą. Šiuose duomenų rinkiniuose taip pat turėtų būti kuo mažiau klaidų ir jie turėtų būti kuo išsamesni atsižvelgiant į numatytąją DI sistemos paskirtį, proporcingai atsižvelgiant į technines galimybes ir naujausius technikos laimėjimus, duomenų prieinamumą ir tinkamų rizikos valdymo priemonių įgyvendinimą, kad būtų deramai pašalinti galimi duomenų rinkinių trūkumai. Reikalavimas, kad duomenų rinkiniai būtų išsamūs ir juose nebūtų klaidų, neturėtų daryti poveikio privatumo užtikrinimo priemonių naudojimui kuriant ir bandant DI sistemas. Mokymų, validavimo ir bandymo duomenų rinkiniuose tiek, kiek to reikia pagal jų numatytąją paskirtį, turėtų būti atsižvelgta į ypatumus, savybes arba elementus, kurie yra būdingi konkrečioje geografinėje, elgsenos ar funkcinėje aplinkoje arba aplinkybėmis, kuriomis numatoma naudoti DI sistemą. Siekiant apsaugoti kitų asmenų teises nuo diskriminacijos, kurią gali sukelti šališkos DI sistemos, tiekėjai turėtų turėti galimybę tvarkyti ir specialių kategorijų asmens duomenis, jei tai yra susiję su esminiu viešuoju interesu, kaip tai suprantama Reglamento (ES) 2016/679 9 straipsnio 2 dalies g punkte ir Reglamento (ES) 2018/1725 10 straipsnio 2 dalies g punkte, kad užtikrintų didelės rizikos DI sistemų šališkumo stebėseną, nustatymą ir ištaisymą;

(44a) taikant Reglamento 2016/679 5 straipsnio 1 dalies c punkte ir Reglamento 2018/1725 4 straipsnio 1 dalies c punkte nurodytus principus, visų pirma duomenų kiekio mažinimo principą, mokymo, validavimo ir bandymo duomenų rinkinių atžvilgiu pagal šį reglamentą, turėtų būti tinkamai atsižvelgiama į visą DI sistemos gyvavimo ciklą;

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

(46) informacijos apie tai, kaip buvo sukurtos didelės rizikos DI sistemos ir kaip jos veikia per visą savo gyvavimo ciklą, turėjimas yra labai svarbus siekiant patikrinti atitiktį šio reglamento reikalavimams. Šiuo tikslu reikia saugoti įrašus ir užtikrinti techninių dokumentų, kuriuose pateikiama informacija, būtina DI sistemos atitikčiai atitinkamiems reikalavimams įvertinti, prieinamumą. Tokią informaciją turėtų sudaryti bendrieji sistemos ypatumai, pajėgumai ir apribojimai, algoritmai, duomenys, mokymai, bandymai ir naudojami validavimo procesai, taip pat dokumentacija apie atitinkamą rizikos valdymo sistemą. Techniniai dokumentai turėtų būti nuolat atnaujinami. Be to, tiekėjai arba naudotojai turėtų saugoti didelės rizikos DI sistemos automatiškai generuojamus žurnalus, įskaitant, pavyzdžiui, duomenų išvedinius, pradžios datą ir laiką ir t. t., jei tokią sistemą ir susijusius žurnalus jie kontroliuoja, tiek laiko, kiek reikia, kad jie galėtų įvykdyti savo pareigas;

(47) siekiant spręsti neskaidrumo problemą, dėl kurios tam tikros DI sistemos fiziniams asmenims gali būti nesuprantamos arba pernelyg sudėtingos, didelės rizikos DI sistemoms reikėtų nustatyti reikalavimus dėl tam tikro skaidrumo lygio. Naudotojai turėtų turėti galimybę aiškinti sistemos išvedinį ir jį tinkamai panaudoti. Todėl dėl didelės rizikos DI sistemų turėtų būti parengiama atitinkama dokumentacija ir naudojimo instrukcijos, įskaitant nuoseklią ir aiškią informaciją, be kita ko, susijusią su galima rizika asmenų, kuriems sistema dėl jos numatytosios paskirties gali turėti poveikį, pagrindinėms teisėms ir jų diskriminacijos rizika, kai tinkama. Kad naudotojams būtų lengviau suprasti naudojimo instrukcijas, jose atitinkamai turėtų būti pateikiami aiškinamieji pavyzdžiai;

(48) didelės rizikos DI sistemos turėtų būti kuriamos ir plėtojamos taip, kad fiziniai asmenys galėtų prižiūrėti jų veikimą. Šiuo tikslu sistemos tiekėjas prieš pateikdamas sistemą rinkai arba pradėdamas ją naudoti turėtų nustatyti atitinkamas žmogaus atliekamos priežiūros priemones. Visų pirma, kai tinkama, tokiomis priemonėmis turėtų būti garantuojama, kad sistemai būtų taikomi integruoti veikimo apribojimai, kurie būtų nepriklausomi nuo pačios sistemos ir kuriuos galėtų kontroliuoti žmogus, ir kad fiziniai asmenys, kuriems pavesta atlikti žmogaus priežiūrą, turėtų būtiną kompetenciją, kvalifikaciją ir įgaliojimus atlikti tą funkciją; Atsižvelgiant į tai, kad neteisingos atitikties tam tikrose biometrinio tapatybės nustatymo sistemose atveju asmenims kyla reikšmingų pasekmių, tikslinga numatyti griežtesnį žmogaus vykdomos tų sistemų priežiūros reikalavimą, kad naudotojas 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;

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

(50) techninis patvarumas yra pagrindinis didelės rizikos DI sistemoms keliamas reikalavimas. Jos turėtų būti atsparios kenkėjiškam ar kitokiam nepageidaujamam elgesiui, kurį gali lemti sistemų ar aplinkos, kurioje tos sistemos veikia, apribojimai (pvz., klaidos, gedimai, nenuoseklumas, netikėtos situacijos). Todėl didelės rizikos DI sistemos turėtų būti kuriamos ir plėtojamos taikant tinkamus techninius sprendimus, kad būtų užkirstas kelias kenkėjiškam ar kitokiam nepageidaujamam elgesiui arba jis būtų kuo labiau sumažintas, pavyzdžiui, mechanizmus, leidžiančius sistemai saugiai nutraukti savo veikimą (atsparumo gedimams planai) esant tam tikroms anomalijoms arba kai veikimas vyksta ne tam tikrose iš anksto nustatytose ribose. Nesugebėjimas apsisaugoti nuo šios rizikos galėtų sukelti pasekmių saugumui arba daryti neigiamą poveikį pagrindinėms teisėms, pavyzdžiui, dėl klaidingų sprendimų arba neteisingų arba šališkų DI sistemos sugeneruotų išvedinių;

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

(52) atsižvelgiant į Sąjungos derinamuosius teisės aktus, didelės rizikos DI sistemų pateikimui rinkai, pradėjimui naudoti ir naudojimui taikytinos taisyklės turėtų derėti su Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008[22], kuriuo nustatomi su gaminių prekyba susiję akreditavimo ir rinkos priežiūros reikalavimai, Europos Parlamento ir Tarybos sprendimu 768/2008/EB [23]dėl bendrosios gaminių pardavimo sistemos ir Europos Parlamento ir Tarybos reglamentu (ES) 2019/1020[24] dėl rinkos priežiūros ir gaminių atitikties (naujoji gaminių pardavimo teisės aktų sistema);

(52a) laikantis naujosios teisės aktų sistemos principų, atitinkamiems veiklos DI vertės grandinėje vykdytojams reikėtų nustatyti konkrečias pareigas, kad būtų užtikrintas teisinis tikrumas ir sudarytos palankesnės sąlygos šio reglamento laikymuisi. 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;

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

---

22 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

23 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).

24 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1020 dėl rinkos priežiūros ir gaminių atitikties, kuriuo iš dalies keičiama Direktyva 2004/42/EB ir reglamentai (EB) Nr. 765/2008 ir (ES) Nr. 305/2011 (tekstas svarbus EEE) (OL L 169, 2019 6 25, p. 1–44).

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

(54a) siekiant užtikrinti teisinį tikrumą, būtina paaiškinti, kad tam tikromis konkrečiomis sąlygomis bet kuris fizinis ar juridinis asmuo turėtų būti laikomas naujos didelės rizikos DI sistemos tiekėju ir todėl turėtų prisiimti visas atitinkamas pareigas. Pavyzdžiui, taip būtų tuo atveju, jeigu tas asmuo savo pavadinimą ar vardą ir pavardę ar prekių ženklą nurodo didelės rizikos DI sistemoje, kuri jau pateikta rinkai arba pradėta naudoti, arba jeigu tas asmuo pakeistų numatytąją DI sistemos, kuri nėra didelės rizikos ir jau yra pateikta rinkai arba pradėta naudoti, paskirtį taip, kad modifikuota sistema taptų didelės rizikos DI sistema. Šios nuostatos turėtų būti taikomos nedarant poveikio konkretesnėms nuostatoms, nustatytoms tam tikruose naujosios teisės aktų sistemos sektorių teisės aktuose, 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, kurie galėtų turėti įtakos jos atitikčiai taikytiniems reikalavimams, turėtų būti toliau taikoma didelės rizikos DI sistemoms, kurios yra medicinos priemonės, kaip tai suprantama tame reglamente;

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

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

(56a) tiekėjų, kurie nėra įsisteigę Sąjungoje, įgaliotasis atstovas atlieka pagrindinį vaidmenį užtikrinant didelės rizikos DI sistemų, kurias jie jau pateikė rinkai arba kurios jau pradėtos naudoti Sąjungoje, atitiktį ir būdamas jų kontaktiniu asmeniu, įsisteigusiu Sąjungoje. Atsižvelgiant į šį pagrindinį vaidmenį ir siekiant užtikrinti, kad šio reglamento vykdymo užtikrinimo tikslais būtų prisiimama atsakomybė, tikslinga nustatyti, kad įgaliotasis atstovas ir tiekėjas būtų solidariai atsakingi už defektų turinčias didelės rizikos DI sistemas. Šiame reglamente numatytos įgaliotojo atstovo atsakomybės nuostata nedaromas poveikis Direktyvos 85/374/EEB dėl atsakomybės už gaminius su trūkumais nuostatoms;

(57) [išbraukta]

(58) atsižvelgiant į DI sistemų pobūdį ir riziką saugumui ir pagrindinėms teisėms, kurios gali būti susijusios su jų naudojimu, įskaitant poreikį užtikrinti tinkamą DI sistemos efektyvų veikimą realiomis sąlygomis, tinkama naudotojams nustatyti konkrečias pareigas. Naudotojai didelės rizikos DI sistemas visų pirma turėtų naudoti laikydamiesi naudojimosi instrukcijų, be to, turėtų būti numatytos tam tikros kitos pareigos, susijusios su DI sistemų veikimo stebėsena ir, kai tinkama, įrašų tvarkymu. Šios pareigos neturėtų daryti poveikio kitoms su didelės rizikos DI sistemomis susijusioms naudotojų pareigoms pagal Sąjungos arba nacionalinę teisę ir neturėtų būti taikomos tais atvejais, kai sistema naudojamasi užsiimant asmenine neprofesine veikla;

(58a) tikslinga paaiškinti, kad šiuo reglamentu nedaromas poveikis DI sistemų tiekėjų ir naudotojų, kaip duomenų valdytojų ar tvarkytojų, pareigoms, kylančioms iš Sąjungos teisės dėl asmens duomenų apsaugos, tiek, kiek DI sistemų kūrimas, plėtojimas 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;

(59) [išbraukta]

(60) [išbraukta]

(61) standartizacija turėtų atlikti svarbų vaidmenį, kad tiekėjams būtų suteikti techniniai sprendimai ir taip užtikrinta atitiktis šiam reglamentui, atsižvelgiant į naujausius technikos laimėjimus. Atitiktis darniesiems standartams, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) Nr. 1025/2012[25], kurie, tikėtina, paprastai turėtų būti rengiami atsižvelgiant į naujausius technikos laimėjimus, turėtų būti viena iš priemonių tiekėjams įrodyti atitiktį šio reglamento reikalavimams. Tačiau, nesant atitinkamų nuorodų į darniuosius standartus, Komisija turėtų galėti įgyvendinimo aktais nustatyti tam tikrų reikalavimų pagal šį reglamentą bendrąsias specifikacijas kaip išimtinį atsarginį sprendimą, kad tiekėjui būtų lengviau vykdyti pareigą laikytis šio reglamento reikalavimų, kai standartizacijos procesas blokuojamas arba vėluojama parengti tinkamą darnųjį standartą. Jei tokią delsą lemia techninis atitinkamo standarto sudėtingumas, Komisija turėtų į tai atsižvelgti prieš svarstydama galimybę nustatyti bendrąsias specifikacijas. Tinkamas mažųjų ir vidutinių įmonių dalyvavimas rengiant standartus, kuriais remiamas šio reglamento įgyvendinimas, yra labai svarbus siekiant Sąjungoje skatinti inovacijas ir konkurencingumą dirbtinio intelekto srityje. Toks dalyvavimas turėtų būti tinkamai užtikrintas pagal Reglamento (ES) Nr. 1025/2012 5 ir 6 straipsnius;

[25] 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).

(61a) tikslinga, kad, nedarant poveikio darniųjų standartų ir bendrųjų specifikacijų naudojimui, tiekėjams būtų taikoma atitikties atitinkamam reikalavimui dėl duomenų prezumpcija, kai jų didelės rizikos DI sistema buvo apmokyta ir išbandyta naudojant duomenis, atspindinčius konkrečią geografinę, elgsenos ar funkcinę aplinką, kurioje ketinama naudoti tą DI sistemą. Panašiai, vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2019/881 54 straipsnio 3 dalimi, turėtų būti daroma prielaida, 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. Tai nedaro poveikio savanoriškam tos kibernetinio saugumo sertifikavimo schemos pobūdžiui;

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

(63) tinkama, kad, siekiant kuo labiau sumažinti naštą veiklos vykdytojams ir išvengti bet kokio galimo dubliavimo, didelės rizikos DI sistemoms, susijusioms su gaminiais, kuriems, vadovaujantis naujosios teisės aktų sistemos principu, taikomi esami Sąjungos derinamieji teisės aktai, šių DI sistemų atitiktis šio reglamento reikalavimams turėtų būti vertinama atliekant pagal tuos teisės aktus jau numatytą atitikties vertinimą. Todėl šio reglamento reikalavimų taikymas neturėtų daryti poveikio konkrečiai atitikties vertinimo, atliekamo pagal atitinkamus naujosios teisės aktų sistemos teisės aktus, logikai, metodikai ar bendrajai struktūrai. Šis principas visiškai atsispindi atsižvelgiant į šio reglamento ir [Mašinų reglamento] sąveiką. Nors DI sistemų, kuriomis užtikrinamos saugios mašinų funkcijos, saugos rizikai taikomi šio reglamento reikalavimai, tam tikri [Mašinų reglamento] konkretūs reikalavimai padės užtikrinti saugią DI sistemos integravimą į visas mašinas, kad nebūtų pažeista visų mašinų sauga. [Mašinų reglamente] taikoma tokia pati DI sistemos apibrėžtis kaip ir šiame reglamente. Kalbant apie didelės rizikos DI sistemas, susijusias su gaminiais, kuriems taikomi reglamentai (ES) 745/2017 ir (ES) 746/2017 dėl medicinos priemonių, taikant šio reglamento reikalavimus neturėtų būti daromas poveikis rizikos valdymo logikai ir naudos ir rizikos vertinimui, atliekamiems pagal tuos medicinos priemonių teisės aktus, ir turėtų būti į juos atsižvelgiama;

(64) atsižvelgiant į didesnę profesionalių sertifikuotojų prieš pateikiant rinkai patirtį gaminių saugos srityje ir skirtingą kylančios rizikos pobūdį, tinkama riboti (bent jau pradiniame šio reglamento taikymo etape) trečiosios šalies atliekamo didelės rizikos DI sistemų, išskyrus su gaminiais susijusias DI sistemas, atitikties vertinimo taikymo sritį. Todėl tokių sistemų atitikties vertinimą paprastai turėtų atlikti tiekėjas ir už tai atsakyti, išskyrus vienintelę išimtį, susijusią su DI sistemomis, kurios skirtos naudoti nuotolinio biometrinio asmenų tapatybės nustatymo tikslais, kai turėtų būti numatyta notifikuotosios įstaigos galimybė dalyvauti atliekant atitikties vertinimą, jei minėtos DI sistemos nedraudžiamos;

(65) siekiant, kad trečioji šalis atliktų DI sistemų, skirtų naudoti nuotolinio biometrinio asmens tapatybės nustatymo tikslais, atitikties vertinimą, nacionalinės kompetentingos institucijos pagal šį reglamentą turėtų paskirti notifikuotąsias įstaigas, jeigu jos atitinka reikalavimų rinkinį, visų pirma nepriklausomumo, kompetencijos ir interesų konflikto nebuvimo reikalavimus. Nacionalinės kompetentingos institucijos turėtų siųsti pranešimus apie šias įstaigas Komisijai ir kitoms valstybėms narėms naudodamosi Komisijos pagal Sprendimo Nr. 768/2008/EB R23 straipsnį parengta ir prižiūrima elektronine notifikavimo priemone;

(66) 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 algoritmo ir DI sistemų, kurios toliau „mokosi“ po to, kai buvo pateiktos rinkai arba pradėtos naudoti (t. y. automatiškai prisitaiko vykdant funkcijas), veikimo pakeitimai neturėtų būti laikomi esminiu pakeitimu, jeigu tuos pakeitimus tiekėjas numatė iš anksto ir jie buvo įvertinti atitikties vertinimo metu;

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

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

(69) siekiant palengvinti Komisijos ir valstybių narių darbą dirbtinio intelekto srityje, taip pat padidinti skaidrumą visuomenės atžvilgiu, turėtų būti reikalaujama, kad didelės rizikos DI sistemų, išskyrus DI sistemas, susijusias su gaminiais, kuriems taikomi atitinkami esami Sąjungos derinamieji teisės aktai, tiekėjai įsiregistruotų patys ir įregistruotų informaciją apie savo didelės rizikos DI sistemą Komisijos sukursimoje ir tvarkysimoje duomenų bazėje. Prieš naudodami III priede nurodytą didelės rizikos DI sistemą, didelės rizikos DI sistemų naudotojai, kurie yra valdžios institucijos, agentūros ar įstaigos, išskyrus teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijas, ir institucijos, kurios yra didelės rizikos DI sistemų naudotojos ypatingos svarbos infrastruktūros srityje, taip pat užsiregistruoja tokioje duomenų bazėje ir pasirenka sistemą, kurią numato naudoti. Komisija turėtų būti šios duomenų bazės valdytoja, laikantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[26]. Siekiant užtikrinti visapusišką įdiegtos duomenų bazės veikimą, pagal duomenų bazės kūrimo procedūrą turėtų būti numatyta, kad Komisija parengs funkcines specifikacijas ir kad bus parengta nepriklausomo audito ataskaita;

[26] 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).

(70) tam tikros DI sistemos, kurių paskirtis – sąveikauti su fiziniais asmenimis arba kurti turinį, gali kelti konkrečią apsimetinėjimo arba apgaulės riziką, nepaisant to, ar jos klasifikuojamos kaip didelės rizikos DI sistemos, ar ne. Todėl šių sistemų naudojimui tam tikromis aplinkybėmis turėtų būti taikomi konkretūs skaidrumo įpareigojimai, nedarant poveikio didelės rizikos DI sistemoms taikomiems reikalavimams ir įpareigojimams. Visų pirma fiziniai asmenys turėtų būti informuojami apie tai, kad bendrauja su DI sistema, nebent, fizinio asmens, kuris yra pakankamai informuotas, pastabus ir nuovokus, nuomone, tai yra akivaizdu, atsižvelgiant į aplinkybes ir naudojimo kontekstą. Vykdant tokią pareigą, reikėtų atsižvelgti į 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 jiems taikomos sistemos, 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 arba kiti aspektai, pavyzdžiui, seksualinė ar politinė orientacija. Tokia informacija ir pranešimai neįgaliesiems turėtų būti teikiami prieinama forma. Be to, DI sistemų, kuriomis sukuriamas į realius asmenis, objektus, vietas ar kitus dalykus ar įvykius labai panašus judamo bei nejudamo vaizdo ir garso turinys, kurį asmuo gali klaidingai palaikyti autentišku, naudotojai turėtų nurodyti, kad tas turinys sukurtas dirbtinai arba kad su juo atliktos manipuliacijos, atitinkamai paženklinant dirbtinio intelekto išvedinį ir atskleidžiant informaciją apie jo dirbtinę kilmę. Pirmiau nurodytų informavimo pareigų laikymasis neturėtų būti aiškinamas kaip reiškiantis, kad 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 naudotojams taikomoms skaidrumo pareigoms. Be to, jis neturėtų būti aiškinamas kaip reiškiantis, kad sistemos ar jos išvedinių naudojimas trukdo įgyvendinti teisę į saviraiškos laisvę ir teisę į menų ir mokslo laisvę, garantuojamas ES pagrindinių teisių chartijoje, visų pirma tais atvejais, kai turinys yra akivaizdžiai kūrybinio, satyrinio, meninio ar išgalvoto darbo ar programos dalis, taikant tinkamas trečiųjų šalių teisių ir laisvių apsaugos priemones;

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

(72) DI apribotos bandomosios reglamentavimo aplinkos tikslai turėtų būti susiję su DI inovacijų skatinimu sukuriant kontroliuojamą eksperimentavimo ir bandymų aplinką, kuri būtų taikoma kūrimo etapu ir etapu prieš pateikimą rinkai, siekiant užtikrinti naujoviškų DI sistemų atitiktį šiam reglamentui ir kitiems susijusiems Sąjungos ir valstybių narių teisės aktams; siekiant didinti novatorių teisinį tikrumą ir kompetentingų institucijų priežiūrą ir supratimą apie galimybes, naują riziką ir DI naudojimo poveikį ir paspartinti patekimą į rinką, įskaitant kliūčių mažosioms ir vidutinėms įmonėms (MVĮ), įskaitant startuolius, pašalinimą. Dalyvaujant DI apribotoje bandomojoje reglamentavimo aplinkoje daugiausia dėmesio turėtų būti skiriama klausimams, dėl kurių tiekėjams ir galimiems tiekėjams kyla teisinis netikrumas diegti inovacijas, eksperimentuoti su DI Sąjungoje ir prisidėti prie faktiniais duomenimis grindžiamo mokymosi reglamentavimo srityje. Todėl DI sistemų priežiūra DI apribotoje bandomojoje reglamentavimo aplinkoje turėtų apimti jų plėtojimą, 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. Kai tinkama, nacionalinės kompetentingos institucijos, kuriančios DI apribotas bandomąsias reglamentavimo aplinkas, turėtų bendradarbiauti su kitomis atitinkamomis institucijomis, įskaitant tas, kurios prižiūri pagrindinių teisių apsaugą, ir galėtų sudaryti sąlygas dalyvauti kitiems DI ekosistemos dalyviams, pavyzdžiui, nacionalinėms ar Europos standartizacijos organizacijoms, notifikuotosioms įstaigoms, bandymų ir eksperimentavimo įstaigoms, mokslinių tyrimų ir eksperimentavimo laboratorijoms, inovacijų centrams ir atitinkamiems suinteresuotiesiems subjektams bei pilietinės visuomenės organizacijoms. Kad būtų užtikrintas vienodas įgyvendinimas visoje Sąjungoje ir masto ekonomija, tinkama sukurti bendras apribotos bandomosios reglamentavimo aplinkos įgyvendinimo taisykles ir atitinkamų institucijų, dalyvaujančių vykdant apribotos bandomosios aplinkos priežiūrą, bendradarbiavimo sistemą. Pagal šį reglamentą sukurtos DI apribotos bandomosios reglamentavimo aplinkos neturėtų daryti poveikio kitiems teisės aktams, kuriais 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 DI apribotos bandomosios reglamentavimo aplinkos dalyviams susitarus, bandymai realiomis sąlygomis taip pat gali būti atliekami ir prižiūrimi DI apribotos bandomosios reglamentavimo aplinkos sąlygomis;

(-72a) šiame reglamente turėtų būti numatytas DI apribotos bandomosios reglamentavimo aplinkos dalyviams skirtas asmens duomenų, kurie buvo surinkti kitais tikslais, siekiant DI apribotoje bandomojoje reglamentavimo aplinkoje sukurti tam tikras su viešuoju interesu susijusias DI sistemas, naudojimo teisinis pagrindas, laikantis Reglamento (ES) 2016/679 6 straipsnio 4 dalies bei 9 straipsnio 2 dalies g punkto ir Reglamento (ES) 2018/1725 5 ir 10 straipsnių, nedarant poveikio Direktyvos (ES) 2016/680 4 straipsnio 2 daliai ir 10 straipsniui. Toliau taikomos visos kitos duomenų valdytojų pareigos ir duomenų subjektų teisės pagal Reglamentą (ES) 2016/679, Reglamentą (ES) 2018/1725 ir Direktyvą (ES) 2016/680. Visų pirma šis reglamentas neturėtų būti 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. Bandomosios aplinkos dalyviai turėtų užtikrinti tinkamas apsaugos priemones ir bendradarbiauti su kompetentingomis institucijomis, taip pat vadovautis jų rekomendacijomis ir veikti greitai bei sąžiningai, kad sumažintų bet kokią didelę riziką saugumui ir pagrindinėms teisėms, kurios gali kilti kuriant ir eksperimentuojant bandomojoje aplinkoje. Kompetentingoms institucijoms nusprendžiant, ar skirti administracinę nuobaudą pagal Reglamento (ES) 2016/679 83 straipsnio 2 dalį ir Direktyvos (ES) 2016/680 57 straipsnį, reikėtų atsižvelgti į dalyvių elgesį apribotoje bandomojoje aplinkoje;

(72a) siekiant paspartinti III priede išvardytų didelės rizikos DI sistemų plėtojimo 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 ir atsižvelgiant į galimas tokių bandymų pasekmes asmenims, reikėtų užtikrinti, kad tiekėjams ar galimiems tiekėjams reglamentu būtų nustatytos tinkamos ir pakankamos garantijos bei sąlygos. Tokios garantijos, be kita ko, turėtų apimti reikalavimą, kad fiziniai asmenys duotų informacija grindžiamą sutikimą dalyvauti bandymuose realiomis sąlygomis, išskyrus su teisėsauga susijusius atvejus, kai informacija grindžiamo sutikimo prašymas užkirstų kelią DI sistemai išbandyti. Tiriamų 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;

(73) siekiant skatinti ir apsaugoti inovacijas, svarbu, kad būtų konkrečiai atsižvelgiama į DI sistemų MVĮ tiekėjų ir naudotojų interesus. Siekdamos šio tikslo, valstybės narės turėtų rengti šiems veiklos vykdytojams skirtas iniciatyvas, įskaitant informuotumo didinimą ir informacijos perdavimą. Be to, notifikuotosios įstaigos, nustatydamos atitikties vertinimo mokesčius, turi atsižvelgti į specifinius MVĮ tiekėjų interesus ir poreikius. Tiekėjai ir kiti veiklos vykdytojai, visų pirma smulkieji, gali patirti didelių vertimo raštu išlaidų, susijusių su privaloma dokumentacija ir komunikacija su institucijomis. Valstybės narės turėtų numatyti galimybę užtikrinti, kad viena iš jų nustatytų ir priimtų kalbų, vartojamų atitinkamiems tiekėjams rengiant dokumentaciją ir bendraujant su veiklos vykdytojais, būtų plačiai suprantama kuo didesniam tarpvalstybinių naudotojų ratui;

(73a) siekiant skatinti ir apsaugoti inovacijas, reikminė DI platforma, visos atitinkamos ES finansavimo programos ir projektai, pavyzdžiui, Skaitmeninės Europos programa, programa „Europos horizontas“, kurias įgyvendina Komisija ir valstybės narės nacionaliniu arba ES lygmeniu, turėtų padėti siekti šio reglamento tikslų;

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

(74a) be to, siekiant užtikrinti inovacijų išlaidų proporcingumą, atsižvelgiant į tai, kad kai kurie veiklos vykdytojai yra labai nedideli, tikslinga labai mažas įmones atleisti nuo daugiausiai kainuojančių įpareigojimų, pavyzdžiui, sukurti kokybės valdymo sistemą, kuri sumažintų tų įmonių administracinę naštą ir išlaidas nedarant poveikio apsaugos lygiui ir poreikiui laikytis didelės rizikos DI sistemoms taikomų reikalavimų;

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

(76) siekiant palengvinti sklandų, veiksmingą ir suderintą šio reglamento įgyvendinimą, reikėtų įsteigti Europos dirbtinio intelekto valdybą. Valdyboje turėtų būti atstovaujama įvairiems DI ekosistemos interesams ir ją turėtų sudaryti valstybių narių atstovai. Siekiant užtikrinti atitinkamų suinteresuotųjų subjektų dalyvavimą, turėtų būti sukurtas nuolatinis Valdybos pogrupis. 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 bei valstybes nares ir jų nacionalines kompetentingas institucijas konkrečiais klausimais, susijusiais su dirbtiniu intelektu. Siekiant suteikti valstybėms narėms tam tikro lankstumo skiriant savo atstovus DI 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. Atsižvelgdama į Komisijos vaidmenį ir užduotis pagal Reglamento (ES) 2019/1020 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 ES įstaigomis, ekspertų grupėmis ir tinklais, veikiančiais atitinkamų ES teisės aktų kontekste, įskaitant visų pirma tuos, kurie veikia vadovaudamiesi atitinkamu ES reglamentavimu duomenų, skaitmeninių produktų ir paslaugų srityje;

(76a) Komisija turėtų aktyviai remti valstybes nares ir veiklos vykdytojus įgyvendinant šį reglamentą ir užtikrinant jo vykdymą. Šiuo atžvilgiu ji turėtų parengti gaires konkrečiomis temomis, kuriomis būtų siekiama palengvinti šio reglamento taikymą, ypatingą dėmesį skiriant MVĮ ir startuolių sektoriuose, kurie gali būti labiausiai paveikti, poreikiams. Siekiant remti tinkamą vykdymo užtikrinimą ir valstybių narių pajėgumus, turėtų būti įsteigtos ir valstybėms narėms prieinamos Sąjungos DI bandymų įstaigos ir atitinkamų ekspertų grupė;

(77) labai svarbus vaidmuo taikant šį reglamentą ir užtikrinant jo vykdymą tenka valstybėms narėms. Šiuo atžvilgiu kiekviena valstybė narė turėtų paskirti vieną ar daugiau nacionalinių kompetentingų institucijų, kad jos prižiūrėtų, kaip taikomas ir įgyvendinamas šis reglamentas. Valstybės narės gali nuspręsti paskirti bet kurį viešąjį subjektą, kuris vykdytų nacionalinių kompetentingų institucijų užduotis, kaip tai suprantama šiame reglamente, atsižvelgdamas į konkrečius nacionalinius organizacinius ypatumus ir poreikius;

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

(79) siekiant užtikrinti tinkamą ir veiksmingą šiame reglamente, kuris yra Sąjungos derinamasis teisės aktas, nustatytų reikalavimų ir pareigų vykdymą, turėtų būti visa apimtimi taikoma rinkos priežiūros ir gaminių atitikties sistema, nustatyta Reglamentu (ES) 2019/1020. Pagal šį reglamentą paskirtos rinkos priežiūros institucijos turėtų turėti visus vykdymo užtikrinimo įgaliojimus pagal šį reglamentą ir Reglamentą (ES) 2019/1020 ir turėtų vykdyti savo įgaliojimus bei 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 paskirti Europos duomenų apsaugos priežiūros pareigūną jų 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;

(79a) 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. Jei tai būtina 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;

(80) Sąjungos teisės aktuose dėl finansinių paslaugų nustatytos vidaus valdymo ir rizikos valdymo taisyklės ir reikalavimai, kurie yra taikomi reguliuojamoms finansų įstaigoms joms teikiant paslaugas, įskaitant atvejus, kai jos naudoja DI sistemas. Siekiant užtikrinti nuoseklų pareigų pagal šį reglamentą ir Sąjungos finansinių paslaugų teisės aktuose nustatytų atitinkamų taisyklių ir reikalavimų taikymą ir vykdymo užtikrinimą, už finansinių paslaugų teisės aktų priežiūrą ir vykdymo užtikrinimą atsakingos institucijos turėtų būti paskirtos kompetentingomis institucijomis, atsakingomis už šio reglamento įgyvendinimo priežiūrą, taip pat rinkos priežiūros veiklos vykdymą, kiek tai susiję su DI sistemomis, kurias tiekia arba naudoja reguliuojamos ir prižiūrimos finansų įstaigos, nebent valstybės narės nusprendžia paskirti kitą instituciją šioms rinkos priežiūros užduotims atlikti. Tos kompetentingos institucijos turėtų turėti visus įgaliojimus pagal šį reglamentą ir Reglamentą (ES) 2019/1020 dėl rinkos priežiūros, 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 atitinkamus Sąjungos finansinių paslaugų teisės aktus. 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 sukurtame bendrame priežiūros mechanizme (BPM), 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 Europos Parlamento ir Tarybos direktyvą 2013/36/ES[27] reglamentuojamoms kredito įstaigoms taikomų taisyklių nuoseklumą, taip pat yra tinkama kai kurias tiekėjų procedūrines pareigas, susijusias su rizikos valdymu, priežiūra po pateikimo rinkai ir dokumentacija, 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 naudotojams 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/ES (Mokumas II) ir draudimo tarpininkams pagal Direktyvą

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

2016/97/ES, taip pat kitų rūšių finansų įstaigoms, kurioms taikomi vidaus valdymo, tvarkos ar procesų reikalavimai, nustatyti pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus, siekiant užtikrinti nuoseklumą ir vienodas sąlygas finansų sektoriuje;

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

(82) svarbu, kad DI sistemos, susijusios su gaminiais, kurie, remiantis šiuo reglamentu, nekelia didelės rizikos ir todėl neturi atitikti jame nustatytų reikalavimų, vis tiek būtų saugios jas pateikiant rinkai arba pradedant naudoti. Siekiant prisidėti prie šio tikslo, Europos Parlamento ir Tarybos direktyva 2001/95/EB[28] būtų taikoma kaip saugumo sistema;

(83) siekdamos 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;

[28] 2001 m. gruodžio 3 d. Europos Parlamento ir Tarybos direktyva 2001/95/EB dėl bendros gaminių saugos (OL L 11, 2002 1 15, p. 4).

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

(85) siekiant užtikrinti, kad reglamentavimo sistemą prireikus būtų galima pritaikyti, įgaliojimai priimti aktus pagal SESV 290 straipsnį turėtų būti deleguoti Komisijai, kad ji galėtų iš dalies pakeisti II priede išvardytus Sąjungos derinamuosius teisės aktus, III priede išvardytas didelės rizikos DI sistemas, IV priede išvardytas nuostatas dėl techninės dokumentacijos, V priedo pateiktos ES atitikties deklaracijos turinį, VI ir VII priedų nuostatas dėl atitikties vertinimo procedūrų ir nuostatas, kuriomis nustatomos didelės rizikos DI sistemos, kurioms turėtų būti taikoma atitikties vertinimo procedūra, pagrįsta kokybės valdymo sistemos vertinimu ir techninių dokumentų vertinimu. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros[29] 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. Tokios konsultacijos ir konsultacinė parama taip pat turėtų būti teikiamos vykdant DI valdybos ir jos pogrupių veiklą;

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

(86) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011[30]. Ypač svarbu, kad, vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais, tais atvejais, kai ankstyvame įgyvendinimo aktų projektų rengimo etape reikia daugiau ekspertinių žinių, Komisija atitinkamai kreiptųsi į ekspertų grupes, konsultuotųsi su tiksliniais suinteresuotaisiais subjektais arba vykdytų viešas konsultacijas. Tokios konsultacijos ir konsultacinė parama taip pat turėtų būti teikiamos vykdant DI valdybos ir jos pogrupių veiklą, be kita ko, rengiant įgyvendinimo aktus, susijusius su 4, 4b ir 6 straipsniais;

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

(87a) 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 bendrosios taikymo pradžios datos, nebent tik jei nuo tos datos tų sistemų konstrukcija ar numatytoji paskirtis reikšmingai pasikeistų. Tikslinga paaiškinti, kad šiuo atžvilgiu reikšmingo pakeitimo sąvoka turėtų būti suprantama kaip iš esmės lygiavertė esminio pakeitimo sąvokai, kuri taikoma tik didelės rizikos DI sistemoms, kaip apibrėžta šiame reglamente;

---

[30] 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).

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

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

PRIĖMĖ ŠĮ REGLAMENTĄ:

I ANTRAŠTINĖ DALIS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

Šiuo reglamentu nustatoma:

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

a) tam tikros su dirbtiniu intelektu susijusios praktikos draudimai;

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

c) suderintos skaidrumo taisyklės, taikomos tam tikroms DI sistemoms;

d) rinkos stebėsenos, rinkos priežiūros ir valdymo taisyklės;

e) inovacijų rėmimo priemonės.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas:

a) tiekėjams, rinkai arba naudojimui Sąjungoje pateikiantiems DI sistemas, nepriklausomai nuo to, ar tie tiekėjai yra fiziškai Sąjungoje ar trečiojoje valstybėje, ar yra įsisteigę Sąjungoje ar trečiojoje valstybėje;

b) Sąjungoje fiziškai esantiems arba įsisteigusiems DI sistemų naudotojams;

c) trečiojoje valstybėje fiziškai esantiems arba įsisteigusiems DI sistemų, kurių sugeneruoti išvediniai naudojami Sąjungoje, tiekėjams ir naudotojams;

d) DI sistemų importuotojams ir platintojams;

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

f) Sąjungoje įsisteigusiems tiekėjų įgaliotiesiems atstovams.

2. DI sistemoms, kurios pagal 6 straipsnio 1 ir 2 dalis priskiriamos didelės rizikos DI sistemoms ir kurios susijusios su produktais, kuriems taikomi II priedo B skirsnyje išvardyti Sąjungos derinamieji teisės aktai, taikomas tik šio reglamento 84 straipsnis. 53 straipsnis taikomas tik tuo atveju, jei didelės rizikos DI sistemoms pagal šį reglamentą taikomi reikalavimai buvo integruoti į tuos Sąjungos derinamuosius teisės aktus.

3. Šis reglamentas netaikomas DI sistemoms, jei ir tiek, kiek jos jau pateiktos rinkai, pradėtos naudoti arba yra naudojamos tokias sistemas iš dalies pakeitus arba jų niekaip nepakeitus, siekiant vykdyti veiklą, kuri nepatenka į Sąjungos teisės taikymo sritį, ir bet kuriuo atveju su kariniu, gynybos ar nacionaliniu saugumu susijusią veiklą, neatsižvelgiant į tą veiklą vykdančio subjekto rūšį.

   Be to, šis reglamentas netaikomas DI sistemoms, kurios nėra pateiktos rinkai ir nėra pradėtos naudoti Sąjungoje, kai jų išvediniai yra naudojami Sąjungoje siekiant vykdyti veiklą, kuri nepatenka į Sąjungos teisės taikymo sritį, ir bet kuriuo atveju su kariniu, gynybos ar nacionaliniu saugumu susijusią veiklą, neatsižvelgiant į tą veiklą vykdančio subjekto rūšį.

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

5. Šis reglamentas nedaro poveikio Europos Parlamento ir Tarybos direktyvos 2000/31/EB[31] II skyriaus 4 skirsnio nuostatų dėl tarpinių paslaugų teikėjų atsakomybės [*jos bus pakeistos atitinkamomis Skaitmeninių paslaugų akto nuostatomis*] taikymui.

6. Šis reglamentas netaikomas DI sistemoms, įskaitant jų išvedinius, kurios specialiai sukurtos ir pradėtos naudoti vien mokslinių tyrimų ir plėtros tikslais.

7. Šis reglamentas netaikomas jokiai su DI sistemomis susijusiai mokslinių tyrimų ir plėtros veiklai.

8. Šis reglamentas netaikomas naudotojų, kurie yra fiziniai asmenys, naudojantys DI sistemas vykdydami tik asmeninę neprofesinę veiklą, pareigoms, išskyrus 52 straipsnio atveju.

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

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

(1) dirbtinio intelekto sistema (DI sistema) – sistema, kuri yra suprojektuota veikti su autonomiškumo elementais ir kuri, remdamasi mašininiais ir (arba) žmogaus pateiktais duomenimis ir įvediniais, numano, kaip pasiekti konkrečius tikslus taikant mašinų mokymosi principus ir (arba) logika ir žiniomis pagrįstus metodus, ir kuri sukuria sistemos generuojamus išvedinius, pvz., turinį (generacinės DI sistemos), prognozes, rekomendacijas ar sprendimus, darančius poveikį aplinkai, su kuria DI sistema sąveikauja;

1a) DI sistemos gyvavimo ciklas – DI sistemos taikymo trukmė nuo jos suprojektavimo iki nurašymo. Nedarant poveikio rinkos priežiūros institucijų įgaliojimams, toks nurašymas tiekėjo sprendimu gali įvykti bet kuriuo metu priežiūros po pateikimo rinkai etape ir jis reiškia, kad sistema negali būti toliau naudojama. DI sistemos gyvavimo ciklas taip pat užbaigiamas, jei tiekėjas arba bet kuris kitas fizinis ar juridinis asmuo padaro esminį DI sistemos pakeitimą; tokiu atveju iš esmės pakeista DI sistema laikoma nauja DI sistema;

1b) bendrosios paskirties DI sistema – DI sistema, kuri, nepaisant to, kaip ji pateikiama rinkai arba pradedama naudoti, be kita ko, kaip atvirojo šaltinio programinė įranga, pagal tiekėjo numatytą paskirtį gali atlikti visuotinai taikomas funkcijas, pvz., vaizdo ar balso atpažinimą, garso ar vaizdo kūrimą, modelių nustatymą, atsakymų į klausimus pateikimą, vertimą ir pan.; bendrosios paskirties DI sistema gali būti naudojama pačiomis įvairiausiomis aplinkybėmis ir gali būti integruota į pačias įvairiausias kitas DI sistemas;

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

(3) [išbraukta]

3a) mažosios ir vidutinės įmonės (MVĮ) – įmonės, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB dėl labai mažų įmonių, mažųjų ir vidutinių įmonių apibrėžimo, priede;

4) naudotojas – fizinis arba juridinis asmuo, įskaitant valdžios institucijas, agentūras ar įstaigas, kurių įgaliojimu sistema naudojama;

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

5a) gaminio gamintojas – gamintojas, kaip tai suprantama bet kuriame iš II priede išvardytų Sąjungos derinamųjų teisės aktų;

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

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

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

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

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

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

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

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

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

15) naudojimo instrukcija – informacija, kurią tiekėjas pateikia visų pirma siekdamas informuoti naudotoją apie numatytąją DI sistemos paskirtį bei tinkamą naudojimą;

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

17) DI sistemos pašalinimas – priemonės, kuriomis siekiama užkirsti kelią tiekimo grandinėje esančios DI sistemos tiekimui rinkai;

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

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

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

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

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

23) esminis pakeitimas – rinkai pateiktos arba pradėtos naudoti DI sistemos pakeitimas, kuris daro poveikį DI sistemos atitikčiai šio reglamento III antraštinės dalies 2 skyriuje nustatytiems reikalavimams, arba numatytosios įvertintos DI sistemos paskirties pakeitimas. 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;

24) CE atitikties ženklas (CE ženklas) – ženklas, kuriuo tiekėjas nurodo, kad DI sistema atitinka reikalavimus, nustatytus šio reglamento III antraštinės dalies 2 skyriuje arba 4b straipsnyje ir kituose taikytinuose Sąjungos teisės aktuose, kuriais suderinamos prekybos šiuo ženklu ženklinamais gaminiais sąlygos (Sąjungos derinamuosiuose teisės aktuose);

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, apibrėžtas Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 dalies c punkte;

28) bendroji specifikacija – techninių specifikacijų, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 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 persimokymo. Validavimo duomenų rinkinys gali būti atskiras duomenų rinkinys arba pastovi ar kintama mokymo duomenų rinkinio dalis;

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

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

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

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

35) biometrinio kategorizavimo sistema – DI sistema, kurios paskirtis – fizinius asmenis remiantis jų biometriniais duomenimis suskirstyti į tam tikras kategorijas;

36) nuotolinio biometrinio tapatybės nustatymo sistema – DI sistema, kurios paskirtis – paprastai nuotoliniu būdu nustatyti fizinių asmenų tapatybę jų faktiškai neįtraukiant, lyginant tų asmenų biometrinius duomenis su informacinėje duomenų saugykloje esančiais biometriniais duomenimis;

37) tikralaikio nuotolinio biometrinio tapatybės nustatymo sistema – nuotolinio biometrinio tapatybės nustatymo sistema, biometrinius duomenis fiksuojanti, lyginanti ir tapatybę nustatanti momentiškai arba beveik momentiškai;

38) [išbraukta]

39) viešoji erdvė – vieša ar privati fizinė vieta, prieinama neribotam skaičiui fizinių asmenų, neatsižvelgiant į tai, ar buvo iš anksto nustatytos tam tikros prieigos prie jos sąlygos ar aplinkybės ir neatsižvelgiant į potencialius talpumo apribojimus;

40) teisėsaugos institucija:

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

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

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

42) [išbraukta]

43) nacionalinė kompetentinga institucija – bet kuri iš šių institucijų: notifikuojančioji institucija ir rinkos priežiūros institucija. Kalbant apie DI sistemas, kurias pradeda naudoti arba naudoja ES institucijos, agentūros, organai ir įstaigos, Europos duomenų apsaugos priežiūros pareigūnas vykdo pareigas, kurios valstybėse narėse pavestos nacionalinei kompetentingai institucijai, ir, kai aktualu, visos nuorodos į nacionalines kompetentingas institucijas arba rinkos priežiūros institucijas šiame reglamente suprantamos kaip nuorodos į Europos duomenų apsaugos priežiūros pareigūną;

44) didelis incidentas – incidentas arba DI sistemos veikimo sutrikimas, kuris tiesiogiai ar netiesiogiai nulemia, galėjo arba gali nulemti:

a) asmens mirtį arba didelę žalą asmens sveikatai,

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

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

d) didelę žalą turtui arba aplinkai;

45) ypatingos svarbos infrastruktūra – turtas, sistema arba jų dalis, būtini teikiant paslaugą, kuri yra būtina gyvybiškai svarbioms visuomenės funkcijoms arba ekonominei veiklai, kaip tai suprantama pagal Direktyvos …/… dėl ypatingos svarbos subjektų atsparumo 2 straipsnio 4 ir 5 punktus;

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

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

48) bandymas realiomis sąlygomis – laikinas DI sistemos testavimas pagal jos numatytąją paskirtį realiomis sąlygomis ne laboratorijoje ar kitoje dirbtinėje aplinkoje siekiant surinkti patikimus ir įtikinamus duomenis ir įvertinti bei patikrinti DI sistemos atitiktį šio reglamento reikalavimams; bandymas realiomis sąlygomis nelaikomas DI sistemos pateikimu rinkai arba pradėjimu naudoti, kaip tai suprantama šiame reglamente, su sąlyga, kad tenkinamos visos 53 arba 54a straipsnyje nustatytos sąlygos;

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

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

51) informuoto asmens sutikimas – laisvas ir savanoriškas subjekto noro dalyvauti konkrečiame bandyme realiomis sąlygomis pareiškimas po to, kai jis buvo informuotas apie visus bandymo aspektus, aktualius subjekto sprendimui dalyvauti; nepilnamečių ir neveiksnių subjektų atveju informuoto asmens sutikimą duoda jų teisėtai paskirtas atstovas;

52) DI apribota bandomoji reglamentavimo aplinka – nacionalinės kompetentingos institucijos sukurta konkreti sistema, pagal kurią DI sistemų tiekėjams arba galimiems tiekėjams suteikiama galimybė, kai tikslinga, realiomis sąlygomis kurti, mokyti, patvirtinti ir išbandyti novatorišką DI sistemą pagal konkretų planą ribotą laiką, prižiūrint reguliavimo institucijoms.

4 straipsnis

Įgyvendinimo aktai

Siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, susijusias su 3 straipsnio 1 dalyje nurodytais mašinų mokymosi principais ir logika bei žiniomis pagrįstais metodais, Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi tų principų techniniai elementai, atsižvelgiant į rinkos ir technologinius pokyčius. Tie įgyvendinimo aktai priimami laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

IA ANTRAŠTINĖ DALIS

BENDROSIOS PASKIRTIES DI SISTEMOS

4a straipsnis

Bendrosios paskirties DI sistemų atitiktis šiam reglamentui

1. Nedarant poveikio šio reglamento 5, 52, 53 ir 69 straipsniams, bendrosios paskirties DI sistemos turi atitikti tik 4b straipsnyje nustatytus reikalavimus ir pareigas.

2. Tokie reikalavimai ir pareigos taikomi neatsižvelgiant į tai, ar bendrosios paskirties DI sistema pateikiama rinkai ar pradedama naudoti kaip iš anksto išmokytas modelis, ir į tai, ar bendrosios paskirties DI sistemos naudotojas turi atlikti tolesnį modelio tobulinimą.

4b straipsnis

Bendrosios paskirties DI sistemoms taikomi reikalavimai ir tokių sistemų tiekėjų pareigos

1. Bendrosios paskirties DI sistemos, kurios gali būti naudojamos kaip didelės rizikos DI sistemos arba kaip didelės rizikos DI sistemų komponentai, kaip tai suprantama 6 straipsnyje, turi atitikti šio reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus nuo įgyvendinimo aktų, kuriuos Komisija, laikydamasi 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros, turi priimti ne vėliau kaip per 18 mėnesių nuo šio reglamento įsigaliojimo dienos, taikymo pradžios dienos. Tuose įgyvendinimo aktuose tiksliai apibrėžiamas ir pritaikomas III antraštinės dalies 2 skyriuje nustatytų reikalavimų taikymas bendrosios paskirties DI sistemoms, atsižvelgiant į jų charakteristikas, technines galimybes, DI vertės grandinės ypatumus ir rinkos bei technologinius pokyčius. Vykdant tuos reikalavimus, atsižvelgiama į visuotinai pripažintus naujausius technikos laimėjimus.

2. 1 dalyje nurodytų bendrosios paskirties DI sistemų tiekėjai nuo 1 dalyje nurodytų įgyvendinimo aktų taikymo pradžios dienos turi laikytis 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 ir 61 straipsniuose nustatytų pareigų.

3. Siekdami laikytis 16e straipsnyje nustatytų pareigų, tiekėjai vadovaujasi VI priedo 3 ir 4 punktuose nustatyta vidaus kontrole pagrįsta atitikties vertinimo procedūra.

4. Be to, tokių sistemų tiekėjai 11 straipsnyje nurodytus techninius dokumentus saugo, kad jie būtų prieinami nacionalinėms kompetentingoms institucijoms, dešimt metų po bendrosios paskirties DI sistemos pateikimo Sąjungos rinkai arba pradėjimo ją naudoti Sąjungoje.

5. Bendrosios paskirties DI sistemų tiekėjai bendradarbiauja su kitais tiekėjais, ketinančiais tokias sistemas pradėti naudoti Sąjungoje arba jas pateikti Sąjungos rinkai kaip didelės rizikos DI sistemas arba didelės rizikos DI sistemų komponentus, ir teikia jiems būtiną informaciją, kad pastarieji galėtų laikytis pareigų pagal šį reglamentą. Tokiu tiekėjų tarpusavio bendradarbiavimu atitinkamai užtikrinamos intelektinės nuosavybės teisės ir konfidenciali verslo informacija ar komercinės paslaptys pagal 70 straipsnį. Siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, susijusias su informacija, kuria turi dalytis bendrosios paskirties DI sistemų tiekėjai, Komisija pagal 74 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą gali priimti įgyvendinimo aktus.

6. Laikantis 1, 2 ir 3 dalyse nurodytų reikalavimų ir pareigų:

– visos nuorodos į numatytąją paskirtį suprantamos kaip nuorodos į galimą bendrosios paskirties DI sistemų naudojimą kaip didelės rizikos DI sistemas arba kaip didelės rizikos DI sistemų komponentus, kaip tai suprantama 6 straipsnyje;

– visos nuorodos į III antraštinės dalies II skyriuje išdėstytus didelės rizikos DI sistemoms taikomus reikalavimus suprantamos kaip nuorodos tik į šiame straipsnyje išdėstytus reikalavimus.

4c straipsnis

4b straipsnio išimtys

1. 4b straipsnis netaikomas, kai tiekėjas aiškiai neįtraukė visų didelės rizikos naudojimo būdų į naudojimo instrukcijas arba į informaciją, pridedamą prie bendrosios paskirties DI sistemos.

2. Toks neįtraukimas atliekamas gera valia ir nėra laikomas pagrįstu, jei tiekėjas turi pakankamai priežasčių manyti, kad sistema gali būti piktnaudžiaujama.

3. Kai tiekėjas nustato piktnaudžiavimą rinkoje arba yra apie jį informuojamas, jis imasi visų būtinų ir proporcingų priemonių, kad užkirstų kelią tokiam tolesniam piktnaudžiavimui, visų pirma atsižvelgdamas į piktnaudžiavimo mastą ir susijusios rizikos rimtumą.

II ANTRAŠTINĖ DALIS

DRAUDŽIAMA SU DIRBTINIU INTELEKTU SUSIJUSI PRAKTIKA

5 straipsnis

1. Draudžiama taikyti šią su dirbtiniu intelektu susijusią praktiką:

   a) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kuria pasitelkiami pasąmonę veikiantys metodai, kurių asmuo nesuvokia, siekiant iš esmės pakeisti asmens elgesį arba kurią pasitelkiant asmens elgesys iš esmės pakeičiamas taip, kad jis pats arba kitas asmuo patirtų fizinę ar psichologinę žalą arba būtų pagrįstai tikėtina, kad jis ar kitas asmuo tokią žalą patirs;

   b) pateikti rinkai, pradėti naudoti arba naudoti DI sistemą, kuria pasinaudojama konkrečios asmenų grupės pažeidžiamumu dėl jų amžiaus, negalios ar konkrečios socialinės ar ekonominės padėties, siekiant iš esmės pakeisti tai grupei priklausančio asmens elgesį arba kuria pasinaudojant to asmens elgesys iš esmės pakeičiamas taip, kad jis pats arba kitas asmuo patirtų fizinę ar psichologinę žalą arba būtų tikėtina, kad jis ar kitas asmuo tokią žalą patirs;

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

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

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

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

i) vykdant tikslinę konkrečių galimų nusikaltimo aukų paiešką;

ii) siekiant išvengti konkrečios didelės grėsmės ypatingos svarbos infrastruktūrai, fizinių asmenų gyvybei, sveikatai ar fizinei saugai arba siekiant užkirsti kelią teroristiniams išpuoliams;

iii) siekiant lokalizuoti ar nustatyti fizinius asmenis baudžiamosios veikos tyrimo, baudžiamojo persekiojimo ar baudžiamųjų sankcijų skyrimo už Tarybos pagrindų sprendimo 2002/584/TVR[32] 2 straipsnio 2 dalyje nurodytą nusikalstamą veiką, už kurią atitinkamoje valstybėje narėje jos teisėje nustatyta tvarka baudžiama laisvės atėmimo bausme arba įkalinimu, kurio ilgiausias terminas – bent treji metai, arba už kitą konkrečią nusikalstamą veiką, už kurią atitinkamoje valstybėje narėje jos teisėje nustatyta tvarka baudžiama laisvės atėmimo bausme arba įkalinimu, kurio ilgiausias terminas – bent penkeri metai, tikslu.

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

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

[32] 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).

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

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

3. 1 dalies d punkto ir 2 dalies tikslais tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemą naudoti viešosiose erdvėse teisėsaugos tikslais galima tik kiekvienu atveju gavus išankstinį valstybės narės, kurioje tą sistemą ketinama naudoti, teisminės institucijos arba nepriklausomos administracinės institucijos leidimą, išduotą pagal pagrįstą prašymą ir 4 dalyje nurodytas išsamias nacionalinės teisės taisykles. Tačiau tinkamai pagrįstais skubos atvejais sistemą galima pradėti naudoti be leidimo, su sąlyga, kad tokio leidimo bus paprašyta nepagrįstai nedelsiant AI sistemos naudojimo metu, o tuo atveju, jei leidimas būtų nesuteiktas, sistemos naudojimas būtų nedelsiant nutrauktas.

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

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

III ANTRAŠTINĖ DALIS

DIDELĖS RIZIKOS DI SISTEMOS

1 SKYRIUS

DI SISTEMŲ PRISKYRIMAS DIDELĖS RIZIKOS SISTEMŲ KATEGORIJAI

6 straipsnis

DI sistemų priskyrimo didelės rizikos sistemų kategorijai taisyklės

1. DI sistema, kuri pati savaime yra gaminys, kuriam taikomi II priede išvardyti Sąjungos derinamieji teisės aktai, laikoma didelės rizikos sistema, jei pagal minėtus teisės aktus reikalaujama, kad trečioji šalis atliktų gaminio atitikties vertinimą, kurio reikia, kad tą gaminį būtų galima pateikti rinkai arba pradėti naudoti.

2. DI sistema, skirta naudoti kaip gaminio, kuriam taikomi 1 dalyje nurodyti teisės aktai, saugos komponentas, laikoma didelės rizikos, jei pagal minėtus teisės aktus reikalaujama, kad trečioji šalis atliktų gaminio atitikties vertinimą, kurio reikia, kad tą gaminį būtų galima pateikti rinkai arba pradėti naudoti. Ši nuostata taikoma nepriklausomai nuo to, ar DI sistema pateikiama rinkai ar pradedama naudoti atskirai nuo gaminio.

3. III priede nurodytos DI sistemos laikomos didelės rizikos sistemomis, išskyrus atvejus, kai sistemos išvedinys yra tik antraeilis atitinkamo veiksmo ar sprendimo, kurį reikia priimti, atžvilgiu ir todėl neturėtų kelti didelės rizikos sveikatai, saugai ar pagrindinėms teisėms.

Siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisija ne vėliau kaip per vienus metus nuo šio reglamento įsigaliojimo dienos priima įgyvendinimo aktus, kuriais patikslinamos aplinkybės, kuriomis III priede nurodytų DI sistemų išvedinys būtų tik antraeilis atitinkamo veiksmo ar sprendimo, kurį reikia priimti, atžvilgiu. Tie įgyvendinimo aktai priimami laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

7 straipsnis

III priedo pakeitimai

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

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

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

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

a) numatytąją DI sistemos paskirtį;

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

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

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

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

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

g) kiek DI sistemos padarinių negalima lengvai ištaisyti (padariniai, darantys poveikį žmonių sveikatai ar saugai, nelaikomi lengvai ištaisomais);

h) kiek galiojančiuose Sąjungos teisės aktuose numatyta:

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

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

i) dirbtinio intelekto naudojimo naudos asmenims, grupėms ar plačiajai visuomenei mastą ir tikimybę.

3. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais III priede pateiktas sąrašas iš dalies keičiamas iš jo išbraukiant didelės rizikos DI sistemas, kurios tenkina abi šias sąlygas:

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

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

2 SKYRIUS

DIDELĖS RIZIKOS DI SISTEMOMS TAIKOMI REIKALAVIMAI

8 straipsnis

Atitiktis reikalavimams

1. Didelės rizikos DI sistemos turi atitikti šiame skyriuje nustatytus reikalavimus, atsižvelgiant į visuotinai pripažintus naujausius technikos laimėjimus.

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

9 straipsnis

Rizikos valdymo sistema

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

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

   a) kiekvienos žinomos ir numatomos rizikos, kuri labiausiai tikėtina sveikatai, saugai ir pagrindinėms teisėms, nustatymas ir analizė, atsižvelgiant į numatytąją didelės rizikos DI sistemos paskirtį;

   b) [išbraukta]

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

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

   Šioje dalyje 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.

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

4. 2 dalies d punkte nurodytos rizikos valdymo priemonės turi būti tokios, kad su kiekvienu pavojumi susijusi liekamoji rizika ir bendra didelės rizikos DI sistemų liekamoji rizika būtų laikoma priimtina.

Nustatant tinkamiausias rizikos valdymo priemones, užtikrinama, kad:

a) pagal 2 dalį nustatyta ir įvertinta rizika būtų pašalinta arba kuo labiau sumažinta tinkamomis didelės rizikos DI sistemos projektavimo ir kūrimo priemonėmis;

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

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

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

5. Siekiant užtikrinti, kad didelės rizikos DI sistemos veiktų taip, kad atitiktų numatytąją paskirtį ir tenkintų šiame skyriuje nustatytus reikalavimus, jos turi būti išbandomos.

6. Bandymo procedūros gali apimti bandymą realiomis sąlygomis pagal 54a straipsnį.

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

8. 1–7 dalyse aprašyta rizikos valdymo sistema ypatingas dėmesys skiriamas tam, ar didelės rizikos DI sistema gali būti prieinama jaunesniems nei 18 metų asmenims arba daryti jiems poveikį.

9. Didelės rizikos DI sistemų tiekėjų, kuriems pagal atitinkamą sektorių Sąjungos teisę taikomi reikalavimai dėl vidaus rizikos valdymo procesų, atveju 1–8 dalyse aprašyti aspektai gali būti įtraukiami į pagal tą teisę nustatytas rizikos valdymo procedūras.

10 straipsnis

Duomenys ir jų valdymas

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

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

   a) atitinkamais projektavimo sprendimais;

   b) duomenų rinkimo procesais;

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

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

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

f) nagrinėjimu atsižvelgiant į galimą šališkumą, kuris, tikėtina, turės įtakos asmenų sveikatai ir saugai arba dėl kurio atsiras diskriminacija, draudžiama pagal Sąjungos teisę;

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

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

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

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

6. Kuriant didelės rizikos DI sistemas nenaudojant 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 jais būtų galima įrodyti, jog didelės rizikos DI sistema atitinka šiame skyriuje nustatytus reikalavimus, ir nacionalinėms kompetentingoms institucijoms bei notifikuotosioms įstaigoms juose būtų aiškia ir išsamia forma pateikta visa informacija, būtina DI sistemos atitikčiai tiems reikalavimams įvertinti. Tuos dokumentus turi sudaryti bent IV priede nustatyti elementai, o MVĮ, įskaitant startuolius, atveju – bet kokie lygiaverčiai tuos pačius tikslus atitinkantys dokumentai, nebent kompetentinga institucija nuspręstų, kad jie yra netikslingi.

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

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

12 straipsnis

Registravimas

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

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

   i) situacijų, kuriose DI sistema gali kelti riziką, kaip tai suprantama 65 straipsnio 1 dalyje, arba dėl kurių gali prireikti atlikti esminį pakeitimą, nustatymui;

   ii) 61 straipsnyje nurodytos priežiūros po pateikimo rinkai palengvinimui ir

   iii) 29 straipsnio 4 dalyje nurodytai didelės rizikos DI sistemų veikimo stebėsenai.

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

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

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

   c) įvesties duomenis, kurių atitikmenys rasti atlikus paiešką;

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

13 straipsnis

Skaidrumas ir informacijos teikimas naudotojams

1. Projektuojant ir kuriant didelės rizikos DI sistemas užtikrinama, kad jos veiktų pakankamai skaidriai, kad naudotojai ir tiekėjai galėtų įvykdyti atitinkamas šios antraštinės dalies 3 skyriuje nustatytas pareigas ir kad naudotojai galėtų tinkamai suprasti ir naudoti sistemą.

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

3. 2 dalyje nurodyta informacija apima:

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

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

      i) jos numatytąją paskirtį, įskaitant informaciją apie konkrečią geografinę, elgesio ar funkcinę aplinką, kurioje ketinama naudoti didelės rizikos DI sistemą;

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

      iii) visas žinomas ar numatomas aplinkybes, susijusias su didelės rizikos DI sistemos naudojimu pagal numatytąją paskirtį, dėl kurių gali kilti rizika sveikatai ir saugai ar pagrindinėms teisėms, nurodytoms 9 straipsnio 2 dalyje;

iv) kai tikslinga, jos elgesį, susijusį su konkrečiais asmenimis ar asmenų grupėmis, kurių atžvilgiu sistemą ketinama naudoti;

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

vi) kai tikslinga, numatomo sistemos išvedinio aprašymą;

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

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

e) būtinus kompiuterių 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) į DI sistemą įtraukto mechanizmo, suteikiančio galimybę naudotojams tinkamai rinkti, saugoti ir interpretuoti žurnalus, kai aktualu, aprašymą.

14 straipsnis

Žmogaus vykdoma priežiūra

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

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

3. Žmogaus vykdoma priežiūra užtikrinama viena arba visomis 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 naudotojui įgyvendinti.

4. 1–3 dalių įgyvendinimo tikslu didelės rizikos DI sistema naudotojui tiekiama taip, kad fiziniams asmenims, kuriems pavesta vykdyti tokią priežiūrą, galėtų, jei tai tinkama ir proporcinga pagal aplinkybes:

a) suprasti didelės rizikos DI sistemos pajėgumus ir apribojimus ir sugebėti tinkamai stebėti jos veikimą;

b) nepamiršti galimos tendencijos automatiškai arba pernelyg pasikliauti didelės rizikos DI sistemos išvediniais (automatiško šališkumo);

c) sugebėti teisingai interpretuoti didelės rizikos DI sistemos išvedinius, atsižvelgiant, pavyzdžiui, į turimas interpretavimo priemones bei metodus;

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

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

5. III priedo 1 punkto a papunktyje nurodytoms didelės rizikos DI sistemoms taikomomis 3 dalyje nurodytomis priemonėmis turi būti užtikrinta, kad, be minėtų dalykų, naudotojas nesiimtų jokių veiksmų ir nepriimtų sprendimų remdamasis sistemos pateiktu identifikavimo rezultatu, išskyrus tuo atveju, jei jį atskirai patikrino ir patvirtino bent du fiziniai asmenys. 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, atvejais, kai pagal Sąjungos ar nacionalinę teisę šio reikalavimo taikymas laikomas neproporcingu.

15 straipsnis

Tikslumas, patikimumas ir kibernetinis saugumas

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

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

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

Didelės rizikos DI sistemų patikimumą galima užtikrinti techniniais perteklumo sprendimais, kurie gali apimti atsarginio kopijavimo arba veikimo be gedimų 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 įvediniams (grįžtamojo ryšio grandinėms), rizika ir kad tiems išvediniams būtų deramai taikomos tinkamos rizikos mažinimo priemonės.

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

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

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

3 SKYRIUS

DIDELĖS RIZIKOS DI SISTEMŲ TIEKĖJŲ BEI NAUDOTOJŲ IR KITŲ ŠALIŲ PAREIGOS

16 straipsnis

Didelės rizikos DI sistemų tiekėjų pareigos

Didelės rizikos DI sistemų tiekėjai:

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

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

b) įdiegia 17 straipsnio reikalavimus atitinkančią kokybės valdymo sistemą;

c) saugo 18 straipsnyje nurodytus dokumentus;

d) saugo savo didelės rizikos DI sistemų automatiškai generuojamus žurnalus, jei tik tie žurnalai yra jų žinioje, kaip nurodyta 20 straipsnyje;

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

f) laikosi 51 straipsnio 1 dalyje nurodytų pareigų įregistruoti sistemą;

g) jei didelės rizikos DI sistema neatitinka šios antraštinės dalies 2 skyriuje nustatytų reikalavimų, imasi būtinų taisomųjų veiksmų, kaip nurodyta 21 straipsnyje;

h) apie neatitiktį ir taisomuosius veiksmus, kurių buvo imtasi, informuoja atitinkamą valstybių narių, kuriose jie tiekė DI sistemą arba pradėjo ją naudoti, nacionalinę kompetentingą instituciją ir, kai taikoma, notifikuotąją įstaigą;

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

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

17 straipsnis

Kokybės valdymo sistema

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

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

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

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

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

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

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

g) 9 straipsnyje nurodytą rizikos valdymo sistemą;

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

i) pranešimo apie didelį incidentą pagal 62 straipsnį procedūras;

j) ryšių su nacionalinėmis ir kitomis kompetentingomis institucijomis, įskaitant sektorių kompetentingas institucijas, teikiančiomis arba palaikančiomis prieigą prie duomenų, notifikuotosiomis įstaigomis, kitais veiklos vykdytojais, klientais ar kitais suinteresuotaisiais subjektais palaikymą;

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

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

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

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

2a. Kalbant apie didelės rizikos DI sistemų tiekėjus, kuriems pagal atitinkamą sektorių Sąjungos teisę taikomos pareigos dėl kokybės valdymo sistemų, 1 dalyje aprašyti aspektai gali būti įtraukiami į pagal tą teisę nustatytas rizikos valdymo sistemas.

3. 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 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 atveju atsižvelgiama į visus šio reglamento 40 straipsnyje nurodytus darniuosius standartus.

18 straipsnis

Dokumentų saugojimas

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

a) 11 straipsnyje nurodytus techninius dokumentus;

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

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

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

e) 48 straipsnyje nurodytą ES atitikties deklaraciją.

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

2. 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, tvarkomų pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus.

19 straipsnis

Atitikties vertinimas

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

2. [išbraukta]

20 straipsnis

Automatiškai generuojami žurnalai

1. Didelės rizikos DI sistemų tiekėjai saugo savo didelės rizikos DI sistemų automatiškai generuojamus žurnalus, nurodytus 12 straipsnio 1 dalyje, tiek, kiek tokie žurnalai yra jų žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisę. Jie juos saugo 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, tvarkomų pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus.

21 straipsnis

Taisomieji veiksmai

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

22 straipsnis

Pareiga informuoti

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

23 straipsnis

Bendradarbiavimas su kompetentingomis institucijomis

Gavę atitinkamos valstybės narės nacionalinės kompetentingos institucijos prašymą, didelės rizikos DI sistemų tiekėjai tai institucijai jai lengvai suprantama kalba pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. Gavę pagrįstą nacionalinės kompetentingos institucijos prašymą, tiekėjai tai institucijai taip pat suteikia galimybę susipažinti su savo didelės rizikos DI sistemos automatiškai generuojamais 12 straipsnio 1 dalyje nurodytais žurnalais, jei tik tokie žurnalai yra jų žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus.

23a straipsnis

Sąlygos, kurių turi laikytis kiti asmenys, kuriems taikomos tiekėjo pareigos

1. Taikant šį reglamentą fiziniai ar juridiniai asmenys laikomi naujos didelės rizikos DI sistemos tiekėjais ir turi vykdyti 16 straipsnyje nustatytas tiekėjo pareigas bet kuriuo iš šių atvejų:

    a) 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) [išbraukta]

c) jie padaro jau rinkai pateiktos arba pradėtos naudoti didelės rizikos DI sistemos esminį pakeitimą;

d) jie pakeičia jau rinkai pateiktos arba pradėtos naudoti didelės rizikos nekeliančios DI sistemos numatytąją paskirtį taip, kad pakeista sistema tampa didelės rizikos DI sistema;

e) jie bendrosios paskirties DI sistemą pateikia rinkai arba pradeda naudoti kaip didelės rizikos DI sistemą arba didelės rizikos DI sistemos komponentą.

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

3. Didelės rizikos DI sistemų, kurios yra gaminių, kuriems taikomi II priedo A skirsnyje išvardyti teisės aktai, saugos komponentai, atveju tų gaminių gamintojai laikomi didelės rizikos DI sistemos tiekėjais ir jiems taikomos 16 straipsnyje numatytos pareigos, jei yra kuri nors iš šių aplinkybių:

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

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

24 straipsnis

[išbraukta]

25 straipsnis

Įgaliotieji atstovai

1. Prieš pateikdami savo sistemas Sąjungos rinkai, už Sąjungos ribų įsisteigę tiekėjai rašytiniu įgaliojimu paskiria Sąjungoje įsisteigusį įgaliotąjį atstovą.

2. Įgaliotasis atstovas atlieka tiekėjo suteiktame įgaliojime nurodytas užduotis. Šio reglamento tikslais įgaliojimu įgaliotajam atstovui suteikiama teisė atlikti tik šias užduotis:

-a) patikrinti, ar parengta ES atitikties deklaracija ir techniniai dokumentai ir ar teikėjas atliko tinkamą atitikties vertinimo procedūrą;

a) 10 metų nuo didelės rizikos DI sistemos pateikimo rinkai arba pradėjimo naudoti dienos saugoti tiekėjo, kuris yra paskyręs įgaliotąjį atstovą, kontaktinius duomenis, ES atitikties deklaracijos kopiją, techninius dokumentus, ir, jei taikoma, notifikuotosios įstaigos išduotą sertifikatą, kad juos galėtų patikrinti nacionalinės kompetentingos institucijos arba 63 straipsnio 7 dalyje nurodytos nacionalinės institucijos;

b) gavus pagrįstą prašymą, pateikti nacionalinei kompetentingai institucijai visą informaciją ir dokumentus, įskaitant saugomus pagal b punktą, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus, be kita ko, suteikti galimybę susipažinti su didelės rizikos DI sistemos automatiškai generuojamais 12 straipsnio 1 dalyje nurodytais žurnalais, jei tik tokie žurnalai yra tiekėjo žinioje pagal sutartį su naudotoju arba – kitais atvejais – pagal teisės aktus;

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

d) įvykdyti 51 straipsnio 1 dalyje nurodytas registravimo pareigas ir, jei sistemą registruoja pats tiekėjas, patikrinti, kad VIII priedo II dalies 1–11 punktuose nurodyta informacija būtų teisinga.

Įgaliotasis atstovas panaikina įgaliojimą, jei turi pakankamai priežasčių matyti, kad tiekėjas veikia nesilaikydamas šiame reglamente nustatytų pareigų. Tokiu atveju jis taip pat nedelsdamas informuoja valstybės narės, kurioje yra įsisteigęs, rinkos priežiūros instituciją, taip pat, kai taikytina, atitinkamą notifikuotąją įstaigą, apie įgaliojimo panaikinimą ir jo priežastis.

Įgaliotasis atstovas yra teisiškai atsakingas už defektų turinčias DI sistemas tuo pačiu pagrindu kaip tiekėjas ir solidariai su tiekėju, kiek tai susiję su jo galima atsakomybe pagal Tarybos direktyvą 85/374/EEB.

26 straipsnis

Importuotojų pareigos

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

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

b) tiekėjas būtų pagal IV priedą parengęs techninius dokumentus;

c) sistema būtų pažymėta reikiamu EB atitikties ženklu ir kartu su ja būtų pateikiama ES atitikties deklaracija ir naudojimo instrukcijos;

d) tiekėjas būtų paskyręs 25 straipsnyje nurodytą įgaliotąjį atstovą.

2. Jei importuotojas turi pakankamai priežasčių 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 DI sistema kelia riziką, kaip apibrėžta 65 straipsnio 1 dalyje, importuotojas apie tai informuoja DI sistemos tiekėją, įgaliotuosius atstovus ir rinkos priežiūros institucijas.

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

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

4a. Importuotojai 10 metų nuo sistemos pateikimo rinkai arba pradėjimo naudoti dienos saugo notifikuotosios įstaigos išduoto sertifikato, kai taikytina, naudojimo instrukcijų ir ES atitikties deklaracijos kopiją.

5. Gavę pagrįstą prašymą importuotojai nacionalinei kompetentingai institucijai pateikia visą tai institucijai lengvai suprantama kalba parengtą informaciją ir dokumentus, įskaitant saugomus pagal 5 dalį, būtinus siekiant įrodyti, kad didelės rizikos DI sistema atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus. Šiuo tikslu jie taip pat užtikrina, kad toms institucijoms būtų galima pateikti techninius dokumentus.

5a. Importuotojai bendradarbiauja su nacionalinėmis kompetentingomis institucijomis joms imantis bet kurių veiksmų dėl DI sistemos, kurios importuotojai jie yra.

27 straipsnis

Platintojų pareigos

1. Prieš tiekdami didelės rizikos DI sistemą rinkai, platintojai patikrina, ar ji pažymėta reikiamu CE atitikties ženklu, ar kartu su ja pateikiama ES atitikties deklaracijos kopija ir naudojimo instrukcijos ir ar sistemos tiekėjas ir importuotojas (jei taikytina) įvykdė atitinkamai 16 straipsnio b punkte ir 26 straipsnio 3 dalyje nustatytas pareigas.

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

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

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

5. Gavę pagrįstą nacionalinės kompetentingos institucijos prašymą, didelės rizikos DI sistemos platintojai jai pateikia visą informaciją ir dokumentus, susijusius su 1–4 dalyse apibūdinta jų veikla.

5a. Platintojai bendradarbiauja su nacionalinėmis kompetentingomis institucijomis joms imantis bet kurių veiksmų dėl DI sistemos, kurios platintojai jie yra.

28 straipsnis

[išbraukta]

29 straipsnis

Didelės rizikos DI sistemų naudotojų pareigos

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

1a. Atlikti žmogaus priežiūrą naudotojai paveda fiziniams asmenims, turintiems reikiamą kompetenciją, kvalifikaciją ir įgaliojimus tai daryti.

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

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

4. Naudotojai įgyvendina žmogaus atliekamą priežiūrą ir stebi didelės rizikos DI sistemos veikimą, atsižvelgdami į jos naudojimo instrukcijas. Jei jie turi pagrindo manyti, kad pagal naudojimo instrukcijas naudojama DI sistema gali kelti riziką, kaip apibrėžta 65 straipsnio 1 dalyje, jie apie tai informuoja tiekėją arba platintoją ir sustabdo sistemos naudojimą. Be to, nustatę didelių incidentų, jie apie tai informuoja tiekėją arba platintoją ir nutraukia DI sistemos naudojimą. Jei naudotojas negali susisiekti su tiekėju, *mutatis mutandis* taikomas 62 straipsnis. Ši pareiga netaikoma DI sistemos naudotojų, kurie yra teisėsaugos institucijos, neskelbtiniems operatyviniams duomenims.

Jei naudotojas yra finansų įstaiga, kuriai pagal Sąjungos finansinių paslaugų teisės aktus taikomi su vidaus valdymo, tvarka ar procesais susiję reikalavimai, pirmoje pastraipoje nustatyta stebėjimo pareiga laikoma įvykdyta, jei laikomasi atitinkamuose finansinių paslaugų teisės aktuose nustatytų taisyklių dėl vidaus valdymo, tvarkos, procesų ir mechanizmų.

5. Didelės rizikos DI sistemos naudotojai saugo tos sistemos automatiškai generuojamus 12 straipsnio 1 dalyje nurodytus žurnalus, jei tik tokie žurnalai yra jų žinioje. Jie juos saugo ne trumpiau kaip šešis mėnesius, nebent taikytinoje Sąjungos ar nacionalinėje teisėje, visų pirma Sąjungos teisėje dėl asmens duomenų apsaugos, numatyta kitaip.

Naudotojai, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi su vidaus valdymu, tvarka ar procesais susiję reikalavimai, žurnalus tvarko kaip dalį dokumentų, tvarkomų pagal atitinkamus Sąjungos finansinių paslaugų teisės aktus.

5a. Didelės rizikos DI sistemų naudotojai, kurie yra valdžios institucijos, agentūros ar įstaigos, išskyrus teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijas, laikosi 51 straipsnyje nurodytų registravimo pareigų. Nustačiusios, kad sistema, kurią jos ketina naudoti, nėra įregistruota 60 straipsnyje nurodytoje duomenų bazėje, jos tos sistemos nenaudoja ir informuoja tiekėją ar platintoją.

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

6a. Naudotojai bendradarbiauja su nacionalinėmis kompetentingomis institucijomis joms imantis bet kurių veiksmų dėl DI sistemos, kurios naudotojai jie yra.

4 SKYRIUS

NOTIFIKUOJANČIOSIOS INSTITUCIJOS IR NOTIFIKUOTOSIOS ĮSTAIGOS

30 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.

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 70 straipsnį užtikrina savo gaunamos informacijos konfidencialumą.

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

8. [Išbraukta]

31 straipsnis

Atitikties vertinimo įstaigos notifikavimo paraiška

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

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

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

32 straipsnis

Notifikavimo procedūra

1. Notifikuojančiosios institucijos gali notifikuoti tik tas atitikties vertinimo įstaigas, kurios atitinka 33 straipsnyje nustatytus reikalavimus.

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

3. 2 dalyje nurodytame notifikavimo pranešime pateikiama išsami informacija apie atitikties vertinimo veiklą, atitikties vertinimo modulį ar modulius, atitinkamas DI sistemas ir atitinkamą kompetencijos atestaciją. Jei notifikavimas nėra pagrįstas akreditacijos pažymėjimu, kaip nurodyta 31 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 33 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 po nofitikuojančiosios įstaigos pateikto notifikavimo pranešimo gavimo, kai prie jo yra pridėtas 31 straipsnio 2 dalyje nurodytas akreditacijos pažymėjimas, arba per du mėnesius po notifikuojančiosios įstaigos pateikto notifikavimo pranešimo gavimo, kai prie jo yra pridėti 31 straipsnio 3 dalyje nurodyti patvirtinamieji dokumentai.

5. [Išbraukta]

33 straipsnis

Notifikuotosioms įstaigoms taikomi reikalavimai

1. Notifikuotoji įstaiga turi būti įsteigta pagal nacionalinę teisę ir 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.

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

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

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

6. Notifikuotosios įstaigos taiko dokumentuotas procedūras, kuriomis užtikrinama, kad jų darbuotojai, komitetai, pavaldžiosios įstaigos, subrangovai, visos susijusios įstaigos ar išorės įstaigų darbuotojai laikytųsi informacijos, kurią jie gauna vykdydami atitikties vertinimo veiklą, konfidencialumo reikalavimų pagal 70 straipsnį, išskyrus atvejus, kai ją atskleisti reikalaujama pagal teisės aktus. Notifikuotųjų įstaigų darbuotojai visą informaciją, kurią jie gauna atlikdami savo užduotis pagal šį reglamentą, saugo kaip profesinę paslaptį – tai netaikoma tik valstybės narės, kurioje tos įstaigos vykdo savo veiklą, notifikuojančiųjų institucijų atžvilgiu.

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

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

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

10. Notifikuotosios įstaigos turi turėti pakankamai vidinės kompetencijos, kad galėtų veiksmingai įvertinti jų vardu užduotis atliekančių išorės subjektų darbą. Notifikuotoji įstaiga turi visada turėti pakankamai administracinių, techninių, teisinių ir mokslinių darbuotojų, turinčių patirties ir žinių, susijusių su atitinkamomis dirbtinio intelekto technologijomis, duomenimis, duomenų kompiuterija ir šios antraštinės dalies 2 skyriuje nustatytais reikalavimais.

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

12. [Išbraukta]

33a straipsnis

Atitikties notifikuotosioms įstaigoms taikomiems reikalavimams prielaida

Jei atitikties vertinimo įstaiga įrodo, kad atitinka kriterijus, nustatytus atitinkamuose darniuosiuose standartuose arba jų dalyse, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, daroma prielaida, kad ji atitinka 33 straipsnyje nustatytus reikalavimus tiek, kiek juos apima taikomi darnieji standartai.

34 straipsnis

Notifikuotųjų įstaigų pavaldžiosios įstaigos ir subrangovai

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

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

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

4. Aktualūs dokumentai, susiję su subrangovo ar pavaldžiosios įstaigos kvalifikacijos įvertinimu ir jų pagal šį reglamentą atliktu darbu, saugomi 5 metus nuo subrangos veiklos pabaigos dienos, kad notifikuojančioji institucija galėtų juos patikrinti.

34a straipsnis

Notifikuotųjų įstaigų veiklos pareigos

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

2. Notifikuotosios įstaigos savo veiklą vykdo vengdamos užkrauti tiekėjams bereikalingą naštą ir deramai atsižvelgdamos į įmonės dydį, sektorių, kuriame ji veikia, jos struktūrą ir konkrečios didelės rizikos DI sistemos sudėtingumo laipsnį. Tačiau tai darydama notifikuotoji įstaiga laikosi tokio griežtumo ir apsaugos lygio, kokio reikia, kad būtų užtikrinta didelės rizikos DI sistemos atitiktis šio reglamento reikalavimams.

3. Notifikuotosios įstaigos sudaro 30 straipsnyje nurodytai notifikuojančiajai institucijai sąlygas susipažinti su visa reikiama dokumentacija, 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 skyriuje aprašytą vertinimą.

35 straipsnis

Pagal šį reglamentą paskirtų notifikuotųjų įstaigų identifikaciniai numeriai ir sąrašai

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

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

36 straipsnis

Notifikavimo galiojimo pokyčiai

1. Notifikuojančioji institucija, naudodamasi 32 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 31 ir 32 straipsniuose apibūdintos procedūros. Jei notifikavimo pakeitimai nėra susiję su jo aprėpties išplėtimu, taikomos toliau išdėstytose dalyse nustatytos procedūros.

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

3. Jeigu notifikuojančioji institucija turi pakankamai priežasčių manyti, kad notifikuotoji įstaiga nebeatitinka 33 straipsnyje nustatytų reikalavimų arba nevykdo savo pareigų, notifikuojančioji institucija (su sąlyga, kad notifikuotajai įstaigai buvo suteikta galimybė pareikšti nuomonę) atitinkamai apriboja, sustabdo arba panaikina notifikavimą, atsižvelgdama į tų reikalavimų nebeatitikimo arba tų pareigų nevykdymo rimtumą. Ji nedelsdama apie tai informuoja Komisiją ir kitas valstybes nares.

4. Jei notifikuotosios įstaigos notifikavimas sustabdomas, apribojamas arba visai ar iš dalies panaikinamas, ji ne vėliau kaip per 10 dienų apie tai informuoja atitinkamus gamintojus.

5. Jei notifikavimas 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.

6. Notifikavimo apribojimo, sustabdymo arba panaikinimo atveju notifikuojančioji institucija:

a) įvertina poveikį notifikuotosios įstaigos išduotiems sertifikatams;

b) per tris mėnesius po pranešimo apie notifikavimo 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 DI sistemų atitiktis;

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

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

7. Išskyrus nepagrįstai išduotus sertifikatus, ir tais atvejais, kai notifikavimas buvo sustabdytas ar apribotas, sertifikatai toliau galioja šiomis aplinkybėmis:

a) notifikuojančioji institucija per mėnesį nuo sustabdymo ar apribojimo yra patvirtinusi, kad nėra pavojaus sveikatai, saugai ar pagrindinėms teisėms, susijusio su sertifikatais, kuriems turi įtakos tas sustabdymas arba apribojimas, ir notifikuojančioji institucija yra nustačiusi tvarkaraštį ir numatomus veiksmus sustabdymui ar apribojimui panaikinti; 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 už notifikuotąsias įstaigas atsakinga institucija nustato, kad notifikuotoji įstaiga nėra pajėgi prižiūrėti galiojančių išduotų sertifikatų, tiekėjas per tris mėnesius nuo sustabdymo arba apribojimo pateikia valstybės narės, kurioje yra sistemos, kuriai taikomas sertifikatas, registruota buveinė, kompetentingoms institucijoms rašytinį patvirtinimą, kad kita reikalavimus atitinkanti notifikuotoji įstaiga laikinai prisiima notifikuotosios įstaigos funkcijas – vykdyti sertifikatų stebėseną ir būti atsakinga už juos sustabdymo arba apribojimo laikotarpiu.

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

a) kai valstybės narės, kurioje yra DI sistemos, kuriai išduotas sertifikatas, tiekėjo registruota buveinė, nacionalinė kompetentingas institucija patvirtino, kad nėra su atitinkamomis sistemomis susijusio pavojaus sveikatai, saugai ir pagrindinėms teisėms, ir

b) kita notifikuotoji įstaiga yra raštu patvirtinusi, kad ji nedelsiant prisiims atsakomybę už šias sistemas ir bus užbaigusi jų įvertinimą per dvylika mėnesių nuo notifikavimo panaikinimo dienos.

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

Nacionalinė kompetentingas institucija arba notifikuotoji įstaiga, prisiimanti notifikuotosios įstaigos, kurią paveikė notifikavimo pakeitimas, 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, kad notifikuotoji įstaiga atitinka 33 straipsnyje nustatytus reikalavimus.

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

3. Komisija užtikrina, kad visa konfidenciali informacija, gaunama atliekant šiame straipsnyje nurodytus tyrimus, būtų tvarkoma konfidencialiai pagal 70 straipsnį.

4. Jei Komisija nustato, kad notifikuotoji įstaiga neatitinka arba nebeatitinka 33 straipsnyje nustatytų reikalavimų, ji informuoja notifikuojančiąją instituciją apie tokio nustatymo priežastis ir paprašo jos imtis būtinų taisomųjų priemonių, įskaitant, jei būtina, notifikavimo sustabdymą, apribojimą ar panaikinimą. Jei notifikuojančioji institucija nesiima būtinų taisomųjų priemonių, Komisija gali priimti įgyvendinimo aktus, kuriais notifikavimą sustabdo, apriboja ar panaikina. Tas įgyvendinimo aktas priimamas laikantis 74 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. Notifikuojančioji institucija užtikrina, kad jos notifikuotos įstaigos tiesiogiai arba per paskirtus atstovus dalyvautų tos grupės veikloje.

39 straipsnis

Trečiųjų valstybių atitikties vertinimo įstaigos

Pagal trečiųjų valstybių, su kuriomis Sąjunga yra sudariusi susitarimus, teisę įsteigtoms atitikties vertinimo įstaigoms gali būti leista vykdyti šiame reglamente nurodytą notifikuotųjų įstaigų veiklą, jeigu jos atitinka 33 straipsnyje nustatytus reikalavimus.

5 SKYRIUS

STANDARTAI, ATITIKTIES VERTINIMAS, SERTIFIKATAI, REGISTRACIJA

40 straipsnis

Darnieji standartai

1. Didelės rizikos DI sistemų arba bendrosios paskirties DI sistemų, atitinkančių darniuosius standartus ar jų dalis, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, atveju daroma prielaida, kad jos atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus arba, kai taikytina, 4a ir 4b straipsniuose nustatytus reikalavimus, jei tik tie reikalavimai yra įtraukti į tuos standartus.

2. Pateikdama standartizacijos prašymą Europos standartizacijos organizacijoms pagal Reglamento (ES) 1025/2012 10 straipsnį, Komisija nurodo, kad standartai yra nuoseklūs, aiškūs ir parengti taip, kad jais būtų siekiama įgyvendinti visų pirma šiuos tikslus:

   a) užtikrinti, kad Sąjungoje rinkai pateikiamos arba pradedamos naudoti DI sistemos būtų saugios ir atitiktų Sąjungos vertybes, taip pat stiprintų Sąjungos atvirą strateginį savarankiškumą;

   b) skatinti investicijas ir inovacijas DI srityje, be kita ko, didinant teisinį tikrumą, taip pat Sąjungos rinkos konkurencingumą bei augimą;

   c) tobulinti įvairių suinteresuotųjų subjektų dalyvavimu grindžiamą valdymą, kuriame atstovaujama visiems atitinkamiems Europos suinteresuotiesiems subjektams (pvz., pramonei, MVĮ, pilietinei visuomenei, tyrėjams);

   d) prisidėti prie pasaulinio bendradarbiavimo standartizacijos klausimais DI srityje, kuris derėtų su Sąjungos vertybėmis ir interesais, stiprinimo.

Komisija paprašo Europos standartizacijos organizacijų pateikti įrodymų, patvirtinančių, kad jos deda visas pastangas siekdamos įgyvendinti pirmiau nurodytus tikslus.

41 straipsnis

Bendrosios specifikacijos

1. Komisijai, pasikonsultavus su 56 straipsnyje nurodyta DI valdyba, laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros, suteikiami įgaliojimai priimti įgyvendinimo aktus, kuriais nustatomos šios antraštinės dalies 2 skyriuje arba atitinkamai 4a ir 4b straipsniuose nustatytų reikalavimų bendrosios techninės specifikacijos, jei yra tenkinamos šios sąlygos:

   a) *Europos Sąjungos oficialiajame leidinyje* nėra pagal Reglamentą (ES) Nr. 1025/2012 paskelbta jokios nuorodos į darniuosius standartus, skirtus esminiams susirūpinimą keliantiems saugos ar pagrindinių teisių klausimams;

   b) Komisija pagal Reglamento (ES) Nr. 1025/2012 10 straipsnio 1 dalį yra paprašiusi vienos ar daugiau Europos standartizacijos organizacijų parengti šios antraštinės dalies 2 skyriuje išdėstytų reikalavimų darnųjį standartą;

   c) nė viena iš Europos standartizacijos organizacijų nepriėmė b punkte nurodyto prašymo arba per terminą, nustatytą pagal Reglamento (ES) Nr. 1025/2021 10 straipsnio 1 dalį, tą prašymą atitinkantys darnieji standartai nebuvo pateikti arba tie standartai neatitinka prašymo.

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

2. Ankstyvame įgyvendinimo akto projekto, kuriuo nustatomos bendrosios specifikacijos, rengimo etape Komisija įvykdo 40 straipsnio 2 dalyje nurodytus tikslus ir sužino atitinkamų įstaigų arba ekspertų grupių, įsteigtų pagal atitinkamus sektorių Sąjungos teisės aktus, nuomones. Remdamasi tų konsultacijų rezultatais, Komisija parengia įgyvendinimo akto projektą.

3. Didelės rizikos DI sistemos arba bendrosios paskirties DI sistemų, atitinkančių 1 dalyje nurodytas bendrąsias specifikacijas, atveju daroma prielaida, kad jos atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus arba atitinkamai 4a ir 4b straipsniuose nustatytus reikalavimus, jei tik tie reikalavimai yra įtraukti į tas bendrąsias specifikacijas.

4. Kai *Europos Sąjungos oficialiajame leidinyje* paskelbiamos nuorodos į darnųjį standartą, 1 dalyje nurodyti įgyvendinimo aktai, kurie taikomi šios antraštinės dalies 2 skyriuje nustatytiems reikalavimams arba 4a ir 4b straipsnyje nustatytiems reikalavimams, atitinkamai panaikinami.

5. Jei valstybė narė mano, kad bendroji specifikacija ne visiškai atitinka šios antraštinės dalies 2 skyriuje nustatytus reikalavimus arba atitinkamai 4a ir 4b straipsniuose nustatytus reikalavimus, ji apie tai informuoja Komisiją, pateikdama išsamų paaiškinimą, o Komisija įvertina tą informaciją ir, jei tinkama, iš dalies pakeičia įgyvendinimo aktą, kuriuo nustatyta atitinkama bendroji specifikacija.

42 straipsnis

Atitikties tam tikriems reikalavimams prielaida

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

2. Jei didelės rizikos DI sistema arba bendrosios paskirties DI sistema yra, laikantis Europos Parlamento ir Tarybos reglamento (ES) 2019/881[33], sertifikuota pagal kibernetinio saugumo sertifikavimo schemą, kurios nuoroda yra paskelbta *Europos Sąjungos oficialiajame leidinyje*, arba jai pagal šią schemą yra išduotas atitikties pareiškimas, daroma prielaida, kad ji atitinka šio reglamento 15 straipsnyje nustatytus kibernetinio saugumo reikalavimus, jei tik tas kibernetinio saugumo sertifikatas, atitikties pareiškimas arba jų dalys apima tuos reikalavimus.

43 straipsnis

Atitikties vertinimas

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

   a) VI priede nurodytą vidaus kontrole grindžiamą atitikties vertinimo procedūrą arba

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

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

[33] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 1).

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

2. III priedo 2–8 punktuose nurodytoms didelės rizikos DI sistemoms ir 1a antraštinėje dalyje nurodytoms bendrosios paskirties DI sistemoms tiekėjai taiko VI priede nurodytą vidaus kontrole grindžiamą atitikties vertinimo procedūrą, kurioje notifikuotosios įstaigos dalyvavimas nenumatytas.

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

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

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

4. [Išbraukta]

5. Komisijai pagal 73 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kurių tikslas – atnaujinti VI ir VII priedus atsižvelgiant į technikos pažangą.

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

44 straipsnis

Sertifikatai

1. Pagal VII priedą notifikuotųjų įstaigų išduodami sertifikatai parengiami valstybės narės, kurioje yra įsisteigusi notifikuotoji įstaiga, atitinkamoms institucijoms lengvai suprantama kalba.

2. Sertifikatai galioja juose nurodytą laikotarpį, kuris negali būti ilgesnis nei penkeri metai. Tiekėjui pateikus paraišką, remiantis pakartotiniu vertinimu pagal taikytinas atitikties vertinimo procedūras, sertifikato galiojimas gali būti pratęstas papildomiems laikotarpiams, kurių nė vienas negali būti ilgesnis nei penkeri metai. Bet koks sertifikato papildymas galioja tol, kol galioja sertifikatas, kurį jis papildo.

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

45 straipsnis

Notifikuotųjų įstaigų sprendimų apskundimas

Turi būti nustatyta notifikuotųjų įstaigų sprendimų apskundimo tvarka.

46 straipsnis

Notifikuotųjų įstaigų pareiga informuoti

1. Notifikuotoji įstaiga informuoja notifikuojančiąją instituciją apie:

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

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

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

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

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

2. Kiekviena notifikuotoji įstaiga informuoja kitas notifikuotąsias įstaigas apie:

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

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

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

4. 1–3 dalyje nurodytos pareigos vykdomos laikantis 70 straipsnio.

47 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 ir svarbiausių pramonės ir infrastruktūros objektų apsauga, leisti atitinkamos valstybės narės teritorijoje rinkai pateikti arba pradėti naudoti konkrečias didelės rizikos DI sistemas. Tas leidimas išduodamas ribotam laikotarpiui, per kurį atliekamos būtinos atitikties vertinimo procedūros, atsižvelgiant į išimtines nukrypti leidžiančią nuostatą pagrindžiančias priežastis. Tos procedūros užbaigiamos nepagrįstai nedelsiant.

1a. 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, o jei tokį leidimą atsisakoma išduoti, sistemos naudojimas nedelsiant nutraukiamas, o visi šio naudojimo rezultatai ir gauti duomenys nedelsiant ištrinami.

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

3. [išbraukta]

4. [išbraukta]

5. [išbraukta]

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

48 straipsnis

ES atitikties deklaracija

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

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

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

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

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

49 straipsnis

CE atitikties ženklas

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

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

3. Jei taikytina, greta CE ženklo nurodomas notifikuotosios įstaigos, atsakingos už 43 straipsnyje nustatytas atitikties vertinimo procedūras, identifikacinis numeris. Identifikacinis numeris taip pat nurodomas visoje reklaminėje medžiagoje, kurioje užsimenama, kad didelės rizikos DI sistema atitinka žymėjimo CE ženklu reikalavimus.

50 straipsnis

[išbraukta]

51 straipsnis

Atitinkamų veiklos vykdytojų ir III priede išvardytų didelės rizikos DI sistemų registravimas

1. Prieš pateikdamas rinkai arba pradėdamas naudoti III priede išvardytą didelės rizikos DI sistemą, išskyrus III priedo 1, 6 ir 7 punktuose nurodytas didelės rizikos DI sistemas teisėsaugos, migracijos, prieglobsčio ir sienų kontrolės valdymo srityse, taip pat III priedo 2 punkte nurodytas didelės rizikos DI sistemas, tiekėjas ir, kai taikytina, įgaliotasis atstovas, užsiregistruoja 60 straipsnyje nurodytoje ES duomenų bazėje. Tiekėjas arba, kai taikytina, įgaliotasis atstovas, toje duomenų bazėje užregistruoja ir savo sistemas.

2. Prieš naudodami III priede išvardytą didelės rizikos DI sistemą, didelės rizikos DI sistemų naudotojai, kurie yra valdžios institucijos, agentūros ar įstaigos arba jų vardu veikiantys subjektai, užsiregistruoja 60 straipsnyje nurodytoje duomenų bazėje ir pasirenka sistemą, kurią jie numato naudoti.

   Pirmesnėje pastraipoje nustatytos pareigos netaikomos teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijoms, agentūroms ar įstaigoms ir institucijoms, agentūroms ar įstaigoms, naudojančioms III priedo 2 punkte nurodytas didelės rizikos DI sistemas, taip pat jų vardu veikiantiems subjektams.

IV ANTRAŠTINĖ DALIS

TAM TIKRŲ DI SISTEMŲ TIEKĖJAMS IR NAUDOTOJAMS TAIKOMOS SKAIDRUMO PAREIGOS

52 straipsnis

Tam tikrų DI sistemų tiekėjams ir naudotojams taikomos skaidrumo pareigos

1. Tiekėjai užtikrina, kad DI sistemos, kurių paskirtis – bendrauti su fiziniais asmenimis, būtų suprojektuotos ir sukurtos taip, kad fiziniai asmenys būtų informuojami apie tai, kad bendrauja su DI sistema, nebent, fizinio asmens, kuris yra pakankamai informuotas, pastabus ir nuovokus, nuomone, tai yra 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, išskyrus atvejus, kai tomis sistemomis pranešimo apie nusikalstamą veiką tikslais leidžiama naudotis visuomenei.

2. Biometrinio kategorizavimo sistemos naudotojai informuoja fizinius asmenis, kurių atžvilgiu ji naudojamos, apie tokios sistemos veikimą. Ši pareiga netaikoma DI sistemoms, naudojamoms biometriniam kategorizavimui, 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.

2a. Emocijų atpažinimo sistemos naudotojai informuoja fizinius asmenis, kurių atžvilgiu ji naudojama, apie tokios sistemos veikimą. Ši pareiga netaikoma emocijų atpažinimui naudojamoms 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.

3. DI sistemų, kuriomis sukuriamas į realius asmenis, objektus, vietas ar kitus dalykus ar įvykius labai panašus judamo bei nejudamo vaizdo ir garso turinys, kurį asmuo gali klaidingai palaikyti autentišku ar tikru (sintetinė sankaita), arba kuriomis tokiu turiniu manipuliuojama, naudotojai nurodo, kad tas turinys sukurtas dirbtinai arba kad su juo atliktos manipuliacijos.

Tačiau pirma pastraipa netaikoma, kai naudojimas yra leidžiamas pagal teisės aktus siekiant nustatyti nusikalstamas veikas, užkirsti joms kelią, jas tirti ir už jas patraukti baudžiamojon atsakomybėn, arba kai turinys yra akivaizdžiai kūrybinio, satyrinio, meninio arba fiktyvaus kūrinio ar programos dalis, taikant atitinkamas trečiųjų šalių teisių ir laisvių apsaugos priemones.

3a. 1–3 dalyse nurodyta informacija fiziniams asmenims pateikiama aiškiai ir matomai ne vėliau nei pirmosios sąveikos arba sistemos panaudojimo jų atžvilgiu metu.

4. 1, 2, 2a, 3 ir 3a dalys nedaro poveikio šio reglamento III antraštinėje dalyje nustatytiems reikalavimams bei pareigoms ir nedaro poveikio kitoms Sąjungos ar nacionalinėje teisėje nustatytoms DI sistemų naudotojams taikomoms skaidrumo pareigoms.

V ANTRAŠTINĖ DALIS

INOVACIJŲ RĖMIMO PRIEMONĖS

53 straipsnis

DI srities apribotos bandomosios reglamentavimo aplinkos

-1a. Nacionalinės kompetentingos institucijos gali sukurti DI srities apribotas bandomąsias reglamentavimo aplinkas, skirtas novatoriškų DI sistemų kūrimui, mokymui, bandymui ir validavimui, atliekamam tiesiogiai prižiūrint, vadovaujant ir padedant nacionalinei kompetentingai institucijai, prieš pateikiant tas sistemas rinkai arba pradedant jas naudoti. Tokios apribotos bandomosios reglamentavimo aplinkos gali apimti bandymą realiomis sąlygomis prižiūrint nacionalinėms kompetentingoms institucijoms.

-1b. [išbraukta]

-1c Kai tinkama, nacionalinės kompetentingos institucijos bendradarbiauja su kitomis atitinkamomis institucijomis ir gali leisti dalyvauti kitiems DI ekosistemos subjektams.

-1d. Šis straipsnis nedaro poveikio kitoms pagal nacionalinę arba Sąjungos teisę sukurtoms apribotoms bandomosioms reglamentavimo aplinkoms, įskaitant atvejus, kai jose bandomi gaminiai ar paslaugos yra susiję su novatoriškų DI sistemų naudojimu. Valstybės narės užtikrina tinkamą institucijų, prižiūrinčių tas kitas apribotas bandomąsias aplinkas, ir nacionalinių kompetentingų institucijų bendradarbiavimą.

1. [išbraukta]

1a. [išbraukta]

1b. Pagal šį reglamentą sukuriant DI srities apribotas bandomąsias reglamentavimo aplinkas siekiama padėti siekti vieno ar daugiau iš šių tikslų:

a) skatinti inovacijas bei konkurencingumą ir palengvinti DI ekosistemos plėtojimą;
b) palengvinti ir paspartinti DI sistemų patekimą į Sąjungos rinką, visų pirma kai jas teikia mažosios ir vidutinės įmonės (MVĮ), įskaitant startuolius;
c) padidinti teisinį tikrumą ir prisidėti prie dalijimosi geriausios patirties pavydžiais bendradarbiaujant su institucijomis, susijusiomis su DI srities apribota bandomąja reglamentavimo aplinka, siekiant užtikrinti, kad ateityje būtų laikomasi šio reglamento ir, kai tinkama, kitų Sąjungos ir valstybių narių teisės aktų;
d) prisidėti prie faktiniais duomenimis grindžiamo mokymosi reglamentavimo srityje.

2. [išbraukta]

2a. Prieiga prie DI srities apribotų bandomųjų reglamentavimo aplinkų suteikiama visiems DI sistemos tiekėjams ar galimiems tiekėjams, kurie atitinka 6 dalies a punkte nurodytus tinkamumo ir atrankos kriterijus ir kuriuos nacionalinės kompetentingos institucijos atrinko po 6 dalies b punkte nurodytos atrankos procedūros. Tiekėjai arba galimi tiekėjai paraiškas taip pat gali teikti kartu su naudotojais ar kitomis atitinkamomis trečiosiomis šalimis.

Dalyvavimas DI srities apribotoje bandomojoje reglamentavimo aplinkoje trunka laikotarpį, kuris yra tinkamas atsižvelgiant į projekto sudėtingumą ir mastą. Nacionalinė kompetentinga institucija šį laikotarpį gali pratęsti.

Dalyvavimas DI srities apribotoje bandomojoje reglamentavimo aplinkoje grindžiamas šio straipsnio 6 dalyje nurodytu konkrečiu planu, dėl kurio atitinkamai susitaria dalyvis (-iai) ir nacionalinė (-ės) kompetentinga (-os) institucija (-os).

3. DI srities apribotos bandomosios reglamentavimo aplinkos nedaro poveikio tokias aplinkas prižiūrinčių kompetentingų institucijų įgaliojimams, susijusiems su priežiūra ir taisomaisiais veiksmais. Siekiant remti DI inovacijas Sąjungoje, tos institucijos savo priežiūros įgaliojimais naudojasi lanksčiai, laikydamosi atitinkamuose teisės aktuose nustatytų ribų, naudodamosi savo veiksmų laisve įgyvendinant teisines nuostatas konkretaus DI srities apribotos bandomosios reglamentavimo aplinkos projekto atveju.

Jeigu dalyvis (-iai) laikosi apribotos bandomosios reglamentavimo aplinkos plano ir jo (jų) dalyvavimo sąlygų, kaip nurodyta 6 dalies c punkte, ir sąžiningai laikosi valdžios institucijų pateiktų gairių, institucijos neskiria administracinių baudų už taikytinų Sąjungos ar valstybių narių teisės aktų, susijusių su apribotoje bandomojoje reglamentavimo aplinkoje prižiūrima DI sistema, įskaitant šio reglamento nuostatas, pažeidimą.

4. Dalyviai lieka pagal taikytinus Sąjungos ir valstybių narių atsakomybę reglamentuojančius teisės aktus atsakingi už bet kokią žalą, padarytą jiems dalyvaujant DI srities apribotoje bandomojoje reglamentavimo aplinkoje.

4a. DI sistemos tiekėjo arba galimo tiekėjo prašymu nacionalinė kompetentinga institucija, kai taikytina, pateikia apribotoje bandomojoje reglamentavimo aplinkoje sėkmingai įvykdytos veiklos rašytinį įrodymą. Nacionalinė kompetentinga institucija taip pat pateikia pasitraukimo ataskaitą, kurioje išsamiai aprašoma apribotoje bandomojoje reglamentavimo aplinkoje vykdyta veikla ir susiję rezultatai bei mokymosi rezultatai. Į tokius rašytinius įrodymus ir pasitraukimo ataskaitą atitikties vertinimo procedūrų arba rinkos priežiūros patikrinimų kontekste galėtų atsižvelgti atitinkamai rinkos priežiūros institucijos arba notifikuotosios įstaigos.

Atsižvelgiant į 70 straipsnyje nustatytas konfidencialumo nuostatas ir gavus apribotos bandomosios reglamentavimo aplinkos dalyvių sutikimą, Europos Komisijai ir DI valdybai suteikiama teisė susipažinti su pasitraukimo ataskaitomis ir, kai tinkama, į jas atsižvelgti vykdant savo užduotis pagal šį reglamentą. Jei dalyvis ir nacionalinė kompetentinga institucija tam aiškiai pritaria, pasitraukimo ataskaita gali būti paskelbta viešai per 55 straipsnio 3 dalies b punkte nurodytą bendrą informacinę platformą.

4b. DI srities apribotos bandomosios reglamentavimo aplinkos projektuojamos ir įgyvendinamos taip, kad, kai aktualu, jomis būtų palengvintas tarpvalstybinis nacionalinių kompetentingų institucijų bendradarbiavimas.

5. Nacionalinės kompetentingos institucijos viešai paskelbia metines ataskaitas dėl DI srities apribotų bandomųjų reglamentavimo aplinkų įgyvendinimo, įskaitant gerosios praktikos pavyzdžius, įgytą patirtį ir rekomendacijas dėl jų struktūros, ir, kai aktualu, dėl šio reglamento ir kitų Sąjungos teisės aktų, kurių laikymasis prižiūrimas konkrečioje apribotoje bandomojoje reglamentavimo aplinkoje, taikymo. Tos metinės ataskaitos pateikiamos DI valdybai, kuri viešai paskelbia visos gerosios praktikos, įgytos patirties ir rekomendacijų santrauką. Ši pareiga viešai skelbti metines ataskaitas neapima neskelbtinų operatyvinių duomenų, susijusių su teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijų veikla. Kai tinkama, Komisija ir DI valdyba atsižvelgia į metines ataskaitas vykdydamos savo užduotis pagal šį reglamentą.

5b. Komisija užtikrina, kad su informacija apie DI srities apribotas bandomąsias reglamentavimo aplinkas, be kita ko, apie pagal šį straipsnį sukurtas aplinkas, būtų galima susipažinti naudojantis 55 straipsnio 3 dalies b punkte nurodyta bendra informacine platforma.

6. DI srities apribotų bandomųjų reglamentavimo aplinkų sukūrimo ir veikimo pagal šį reglamentą tvarka ir sąlygos patvirtinamos įgyvendinimo aktais, priimtais laikantis 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Nustatant tvarką ir sąlygas kuo labiau remiamas nacionalinių kompetentingų institucijų lankstumas nustatyti ir eksploatuoti DI srities apribotas bandomąsias reglamentavimo aplinkas, skatinamos inovacijos bei mokymasis reglamentavimo srityje, ypač atsižvelgiama į konkrečias dalyvaujančių MVĮ, įskaitant startuolius, aplinkybes ir pajėgumus.

Į tuos įgyvendinimo aktus įtraukiami bendri pagrindiniai principai, susiję su šiais klausimais:

a) tinkamumu dalyvauti DI srities apribotoje bandomojoje reglamentavimo aplinkoje ir atranka;
b) prašymais dalyvauti DI srities apribotoje bandomojoje reglamentavimo aplinkoje, dalyvavimu joje, stebėsena, pasitraukimu iš tokios aplinkos ir jos taikymo nutraukimą, įskaitant apribotos bandomosios reglamentavimo aplinkos planą ir pasitraukimo ataskaitą;
c) dalyviams taikomomis sąlygomis.

7. Kai nacionalinės kompetentingos institucijos svarsto galimybę leisti atlikti bandymą realiomis sąlygomis, prižiūrimą pagal šį straipsnį sukurtoje DI srities apribotoje bandomojoje 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.

54 straipsnis

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

1. Kitais tikslais teisėtai surinkti asmens duomenys gali būti tvarkomi DI srities apribotoje bandomojoje reglamentavimo aplinkoje siekiant joje sukurti, bandyti ir mokyti novatoriškas DI sistemas, jei tenkinamos visos šios sąlygos:

   a) novatoriškas DI sistemas kuria valdžios institucija arba kitas viešosios ar privatinės teisės reglamentuojamas fizinis arba juridinis asmuo, siekiant apsaugoti svarbų viešąjį interesą vienoje ar keliose iš šių sričių:

      i) [išbraukta]

      ii) visuomenės saugos ir sveikatos, įskaitant ligų prevenciją, kontrolę ir gydymą bei sveikatos priežiūros sistemų tobulinimą;

      iii) aplinkos kokybės apsaugos ir gerinimo, įskaitant žaliąją pertvarką, klimato kaitos švelninimą ir prisitaikymą prie jos;

      iv) energetikos tvarumo, transporto ir judumo;

      v) viešojo administravimo ir viešųjų paslaugų veiksmingumo ir kokybės;

      vi) kibernetinio saugumo ir ypatingos svarbos subjektų atsparumo;

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

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

d) visi asmens duomenys, kurie bus tvarkomi apribotos bandomosios reglamentavimo aplinkos kontekste, saugomi funkciniu požiūriu atskirtoje, izoliuotoje ir apsaugotoje dalyvių prižiūrimoje duomenų tvarkymo aplinkoje, o prieigą prie tų duomenų turi tik įgalioti asmenys;

e) kitos šalys, kurios nėra apribotos bandomosios reglamentavimo aplinkos dalyvės, nepateikia ir neperduoda jokių tvarkomų asmens duomenų ir negali su šiais duomenimis susipažinti kitais būdais, išskyrus atvejus, kai toks atskleidimas vykdomas laikantis Reglamento (ES) 2016/679 arba, kai taikytina, Reglamento (ES) 2018/1725 ir visi dalyviai su tuo sutinka;

f) bet koks asmens duomenų tvarkymas apribotoje bandomojoje reglamentavimo aplinkoje nedaro poveikio duomenų subjektų teisių taikymui, kaip numatyta Sąjungos teisėje dėl asmens duomenų apsaugos, visų pirma Reglamento (ES) 2016/679 22 straipsnyje ir Reglamento (ES) 2018/1725 24 straipsnyje;

g) visi apribotoje bandomojoje reglamentavimo aplinkoje 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, išskyrus atvejus, kai Sąjungos arba nacionalinėje teisėje 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.

1a. 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 DI srities apribotose bandomosiose reglamentavimo aplinkose grindžiamas konkrečia valstybės narės arba Sąjungos teise ir jam taikomos visos tos pačios 1 dalyje nurodytos sąlygos.

2. Laikantis Sąjungos teisės dėl asmens duomenų apsaugos, 1 dalis nedaro poveikio Sąjungos ar valstybių narių teisės aktams, kuriais nustatomas novatoriškų DI sistemų kūrimo, bandymo ir mokymo tikslais būtino asmens duomenų tvarkymo pagrindas ar bet kuris kitas teisinis pagrindas.

54a straipsnis

Didelės rizikos DI sistemų bandymas realiomis sąlygomis ne DI srities apribotose bandomosiose reglamentavimo aplinkose

1. DI sistemų bandymą realiomis sąlygomis ne DI srities apribotose bandomosiose reglamentavimo aplinkose gali atlikti III priede išvardytų didelės rizikos DI sistemų tiekėjai arba galimi tiekėjai, laikydamiesi šio straipsnio nuostatų ir šiame straipsnyje nurodyto bandymo realiomis sąlygomis plano.

Išsamūs bandymo realiomis sąlygomis plano elementai nurodomi įgyvendinimo aktuose, kuriuos Komisija priima laikydamasi 74 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Ši nuostata nedaro poveikio Sąjungos ar valstybių narių teisės aktams dėl didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi II priede išvardyti teisės aktai, bandymo realiomis sąlygomis.

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

3. Didelės rizikos DI sistemų bandymas realiomis sąlygomis pagal šį straipsnį nedaro poveikio etikos aspektų vertinimui, kurio gali būti reikalaujama pagal nacionalinę arba Sąjungos 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 (-ių) narės (-ių), kurioje (-iose) turi būti atliekamas bandymas realiomis sąlygomis, rinkos priežiūros institucijai;

b) valstybės (-ių) narės (-ių), kurioje (-iose) turi būti atliekamas bandymas realiomis sąlygomis, rinkos priežiūros institucija per 30 dienų nuo plano pateikimo nepareiškė prieštaravimų dėl bandymo;

c) tiekėjas arba galimas tiekėjas bandymą realiomis sąlygomis, 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, atvejus, yra užregistravęs 60 straipsnio 5a dalyje nurodytoje ES duomenų bazėje, jam yra suteiktas visoje Sąjungoje taikomas vienintelis unikalusis identifikacinis numeris, ir jis pateikė VIIIa priede nurodytą informaciją;

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, kurie yra surinkti ir tvarkomi bandymo realiomis sąlygomis tikslais, neperduodami Sąjungai nepriklausančioms šalims, išskyrus atvejus, kai perdavimo ir tvarkymo metu užtikrinamos apsaugos priemonės, kurios yra lygiavertės nustatytoms pagal Sąjungos teisę;

f) bandymas realiomis sąlygomis trunka ne ilgiau nei būtina jo tikslams pasiekti ir bet kuriuo atveju ne ilgiau kaip 12 mėnesių;

g) yra tinkamai apsaugoti asmenys, dėl savo amžiaus, fizinės ar psichinės negalios priklausantys pažeidžiamoms grupėms;

h) [išbraukta]

i) jeigu tiekėjas arba galimas tiekėjas, bendradarbiaudamas su vienu ar daugiau galimų naudotojų, organizuoja bandymą realiomis sąlygomis, pastarieji yra informuoti apie visus bandymo aspektus, kurie yra aktualūs jų sprendimui dalyvauti, ir jiems buvo pateikti 13 straipsnyje nurodyti atitinkami nurodymai dėl DI sistemos naudojimo; tiekėjas arba galimas tiekėjas ir naudotojas (-ai) 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 valstybių narių teisės aktus;

j) bandymo realiomis sąlygomis subjektai yra davę informuoto asmens sutikimą pagal 54b 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 subjektui;

k) bandymą realiomis sąlygomis veiksmingai prižiūri tiekėjas arba galimas tiekėjas ir naudotojas (-ai) kartu su asmenimis, kurie turi tinkamą kvalifikaciją atitinkamoje srityje ir turi savo užduotims atlikti reikiamų pajėgumų, kompetencijos ir įgaliojimus;

l) su DI sistema susijusios predikcijos, rekomendacijos ar sprendimai gali būti veiksmingai atšaukti arba į juos gali būti neatsižvelgiama.

5. Bet kuris bandymo realiomis sąlygomis subjektas arba atitinkamai jo teisėtai paskirtas atstovas gali bet kuriuo metu atšaukti savo informuoto asmens sutikimą nepatirdamas jokios žalos ir neprivalėdamas pateikti jokio pagrindimo. Informuoto asmens sutikimo atšaukimas nedaro poveikio jau atliktai veiklai ir duomenų, gautų remiantis informuoto asmens sutikimu iki jo atšaukimo, naudojimui.

6. Apie visus rimtus incidentus, nustatytus atliekant bandymą realiomis sąlygomis, pagal šio reglamento 62 straipsnį pranešama nacionalinei rinkos priežiūros institucijai. Tiekėjas arba galimas tiekėjas imasi neatidėliotinų poveikio sumažinimo priemonių arba, kai tai neįmanoma, sustabdo bandymą realiomis sąlygomis, kol toks poveikis bus sumažintas, arba kitaip jį nutraukia. Tiekėjas arba galimas tiekėjas nustato procedūrą, pagal kurią DI sistema būtų nedelsiant atšaukta, jei toks bandymas realiomis sąlygomis būtų nutrauktas.

7. Tiekėjai arba galimi tiekėjai valstybės (-ių) narės (-ių), kurioje (-iose) turi būti atliekamas bandymas realiomis sąlygomis, nacionalinei rinkos priežiūros institucijai praneša apie bandymo realiomis sąlygomis sustabdymą arba nutraukimą ir galutinius rezultatus.

8. Tiekėjai arba galimi tiekėjai yra pagal taikytinus Sąjungos ir valstybių narių atsakomybę reglamentuojančius teisės aktus atsakingi už bet kokią žalą, padarytą jų dalyvavimo bandyme realiomis sąlygomis metu.

54b straipsnis

Informuoto asmens sutikimas dalyvauti bandyme realiomis sąlygomis ne DI srities apribotose bandomosiose reglamentavimo aplinkose

1. Bandymo realiomis sąlygomis pagal 54a straipsnį tikslais informuoto asmens sutikimą prieš pradėdamas dalyvauti tokiame bandyme subjektas duoda laisva valia ir po to, kai jis tinkamai informuojamas pateikiant glaustą, aiškią, aktualią ir suprantamą informaciją apie:

i) bandymo realiomis sąlygomis pobūdį ir tikslus bei galimus nepatogumus, kurie gali būti susiję su jo dalyvavimu;

ii) sąlygas, kuriomis turi būti atliekamas bandymas realiomis sąlygomis, įskaitant numatomą subjekto dalyvavimo trukmę;

iii) subjekto teises ir garantijas, susijusias su jo dalyvavimu, visų pirma jo teisę atsisakyti dalyvauti ir teisę bet kuriuo metu pasitraukti iš bandymo realiomis sąlygomis nepatiriant jokios žalos ir neprivalant pateikti pagrindimo;

iv) prašymo atšaukti su DI sistema susijusias predikcijas, rekomendacijas ar sprendimus arba į juos neatsižvelgti tvarką;

v) bandymo realiomis sąlygomis visoje Sąjungoje taikomą vienintelį unikalųjį identifikacinį numerį pagal 54a straipsnio 4c dalį 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 subjektas arba jo teisinis atstovas gauna šio dokumento kopiją.

55 straipsnis

Veiklos vykdytojų, ypač MVĮ, įskaitant startuolius, rėmimo priemonės

1. Valstybės narės imasi šių veiksmų:

a) suteikia MVĮ, įskaitant startuolius, pirmenybę dalyvauti DI srities apribotose bandomosiose reglamentavimo aplinkose, jei jie tenkina tinkamumo ir atrankos sąlygas;

b) organizuoja specialią informuotumo apie šio reglamento taikymą didinimo ir mokymo šia tema veiklą, specialiai pritaikytą MVĮ, įskaitant startuolius, ir atitinkamai vietos valdžios institucijų poreikiams;

c) kai tinkama, sukuria specialų ryšių su MVĮ, įskaitant startuolius, ir atitinkamai vietos valdžios institucijomis, kanalą, kad būtų teikiamos konsultacijos ir atsakoma į užklausas dėl šio reglamento įgyvendinimo, be kita ko, dėl dalyvavimo DI srities apribotose bandomosiose reglamentavimo aplinkose.

2. Nustatant rinkliavas už 43 straipsnyje nurodytą atitikties vertinimą atsižvelgiama į konkrečius MVĮ tiekėjų, įskaitant startuolius, interesus ir poreikius; šios rinkliavos proporcingai sumažinamos atsižvelgiant į jų dydį, rinkos dydį ir kitus atitinkamus rodiklius.

3. Komisija imasi šių veiksmų:

a) DI valdybos prašymu pateikia standartinius šablonus, skirtus sritims, kurioms taikomas šis reglamentas;

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 šiame reglamente nustatytas pareigas didinti;

d) vertina ir skatina su DI sistemomis susijusių viešųjų pirkimų procedūrų geriausios praktikos konvergenciją.

55a straipsnis

Konkretiems veiklos vykdytojams taikomos nukrypti leidžiančios nuostatos

1. Šio reglamento 17 straipsnyje nustatytos pareigos netaikomos labai mažoms įmonėms, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB dėl labai mažų, mažųjų ir vidutinių įmonių apibrėžties priedo 2 straipsnio 3 dalyje, jeigu tos įmonės neturi įmonių partnerių arba susijusių įmonių, kaip apibrėžta to paties priedo 3 straipsnyje.

2. Negali būti suprantama, kad 1 dalimi tie veiklos vykdytojai atleidžiami nuo bet kurių kitų šiame reglamente nustatytų reikalavimų ir pareigų vykdymo, įskaitant 9, 61 ir 62 straipsniuose nustatytus reikalavimus ir pareigas.

3. 4b straipsnyje nustatyti su bendrosios paskirties DI sistemomis susiję reikalavimai ir pareigos netaikomi labai mažoms, mažosioms ir vidutinėms įmonėms, jei tos įmonės neturi įmonių partnerių arba susijusių įmonių, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB dėl labai mažų, mažųjų ir vidutinių įmonių apibrėžties priedo 3 straipsnyje.

VI ANTRAŠTINĖ DALIS

VALDYMAS

1 SKYRIUS

EUROPOS DIRBTINIO INTELEKTO VALDYBA

56 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. Europos duomenų apsaugos priežiūros pareigūnas dalyvauja stebėtojo teisėmis. Komisija taip pat dalyvauja Valdybos posėdžiuose, tačiau 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.

2a. Kiekvieną atstovą valstybė narė skiria trejų metų laikotarpiui, kuris gali būti pratęstas vieną kartą.

2aa. Valstybės narės užtikrina, kad jų atstovai Valdyboje:

   i) savo valstybėje narėje turėtų atitinkamą kompetenciją ir įgaliojimus, kad galėtų aktyviai prisidėti prie 58 straipsnyje nurodytų Valdybos užduočių vykdymo;

   ii) būtų paskirti kaip ryšių su Valdyba palaikymo kontaktiniai asmenys ir, kai tinkama, atsižvelgiant į valstybių narių poreikius, kaip ryšių su suinteresuotaisiais subjektais palaikymo kontaktiniai asmenys;

iii) būtų įgalioti palengvinti savo valstybės narės nacionalinių kompetentingų institucijų veiklos nuoseklumo ir koordinavimo užtikrinimą, kiek tai susiję su šio reglamento įgyvendinimu, be kita ko, renkant atitinkamus duomenis ir informaciją, kad jos galėtų vykdyti savo užduotis Valdyboje.

3. Paskirti valstybių narių atstovai Valdybos darbo tvarkos taisykles priima dviejų trečdalių balsų dauguma.

Darbo tvarkos taisyklėse visų pirma nustatomos atrankos proceso tvarka, įgaliojimų trukmė ir pirmininko užduočių specifikacijos, balsavimo tvarka ir Valdybos bei jos pogrupių veiklos organizavimas.

Valdyba įsteigia nuolatinį pogrupį, kuris veikia kaip suinteresuotųjų subjektų platforma ir pataria Valdybai visais su šio reglamento įgyvendinimu susijusiais klausimais, be kita ko, dėl įgyvendinimo ir deleguotųjų aktų rengimo. Šiuo tikslu dalyvauti šio pogrupio veikloje kviečiamos organizacijos, atstovaujančios DI sistemų tiekėjų ir naudotojų, įskaitant MVĮ ir startuolius, interesams, taip pat pilietinės visuomenės organizacijos, paveiktų asmenų atstovai, tyrėjai, standartizacijos organizacijos, notifikuotosios įstaigos, laboratorijos ir bandymų bei eksperimentavimo infrastruktūros atstovai. Valdyba įsteigia du nuolatinius pogrupius, kad rinkos priežiūros institucijoms ir notifikuojančiosioms institucijoms būtų suteikta platforma bendradarbiauti ir keistis informacija atitinkamai su rinkos priežiūra ir notifikuotosiomis įstaigomis susijusiais klausimais.

Valdyba prireikus gali sudaryti kitus nuolatinius ar laikinuosius pogrupius konkretiems klausimams nagrinėti. Kai tinkama, pirmesnėje pastraipoje nurodyti suinteresuotieji subjektai stebėtojų teisėmis gali būti kviečiami į tokius pogrupius arba į konkrečius tų pogrupių posėdžius.

3a. Valdybos veikla organizuojama ir ji veikia taip, kad būtų užtikrintas jos veiklos objektyvumas ir nešališkumas.

4. Valdybai pirmininkauja vienas iš valstybių narių atstovų. Pirmininko prašymu Komisija sušaukia posėdžius ir rengia darbotvarkę atsižvelgdama į Valdybos užduotis pagal šį reglamentą ir darbo tvarkos taisykles. Komisija teikia administracinę ir analitinę paramą Valdybos veiklai pagal šį reglamentą.

57 straipsnis

[išbraukta]

58 straipsnis

Valdybos užduotys

Valdyba konsultuoja Komisiją ir valstybes nares ir joms padeda, kad būtų palengvintas nuoseklus ir veiksmingas šio reglamento taikymas. Šiuo tikslu Valdyba visų pirma gali:

a) rinkti technines ir su reglamentavimu susijusias ekspertines žinias bei geriausią praktiką ir jomis dalytis su valstybėmis narėmis;

b) prisidėti derinant valstybių narių administracinę praktiką, be kita ko, susijusią su nukrypti nuo 47 straipsnyje nurodytų atitikties vertinimo procedūrų leidžiančia nuostata, apribotų bandomųjų reglamentavimo aplinkų veikimu ir bandymu realiomis sąlygomis, kaip nurodyta 53, 54 ir 54a straipsniuose;

c) Komisijos prašymu arba savo iniciatyva skelbti rekomendacijas ir rašytines nuomones visais aktualiais klausimais, susijusiais su šio reglamento įgyvendinimu ir nuosekliu bei veiksmingu jo taikymu, įskaitant:

   i) technines specifikacijas arba esamus standartus, susijusius su III antraštinės dalies 2 skyriuje nustatytais reikalavimais,

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

iii) rekomendacinių dokumentų, įskaitant rekomendacijas dėl 71 straipsnyje nurodytų administracinių baudų nustatymo, rengimą;

d) konsultuoti Komisiją dėl galimo poreikio iš dalies keisti III priedą pagal 4 ir 7 straipsnius, atsižvelgiant į atitinkamus turimus faktinius duomenis ir naujausius technologinius pokyčius;

e) konsultuoti Komisiją rengiant deleguotąjį arba įgyvendinimo aktą pagal šį reglamentą;

f) prireikus bendradarbiauti su atitinkamomis ES įstaigomis, ekspertų grupėmis ir tinklais, visų pirma gaminių saugos, kibernetinio saugumo, konkurencijos, skaitmeninių ir žiniasklaidos paslaugų, finansinių paslaugų, kriptovaliutų, vartotojų apsaugos, duomenų ir pagrindinių teisių apsaugos srityse;

g) padėti ir teikti atitinkamas konsultacijas Komisijai rengiant 58a straipsnyje nurodytas gaires arba prašyti parengti tokias gaires;

h) padėti rinkos priežiūros institucijoms atlikti savo darbą ir, bendradarbiaujant ir susitarus su atitinkamomis rinkos priežiūros institucijomis, skatinti ir remti tarpvalstybinius rinkos priežiūros tyrimus, be kita ko, susijusius su sisteminio pobūdžio rizikos, kuri gali kilti dėl DI sistemų, atsiradimu;

i) prisidėti vertinant valstybių narių darbuotojų, dalyvaujančių įgyvendinant šį reglamentą, mokymo poreikius;

j) konsultuoti Komisiją tarptautiniais su dirbtiniu intelektu susijusiais klausimais.

1A SKYRIUS

KOMISIJOS GAIRĖS

58a straipsnis

Komisijos gairės dėl šio reglamento įgyvendinimo

1. Valstybių narių ar Valdybos prašymu arba savo iniciatyva Komisija paskelbia gaires dėl šio reglamento praktinio įgyvendinimo, visų pirma dėl:

   i) 8–15 straipsniuose nurodytų reikalavimų taikymo;

   ii) 5 straipsnyje nurodytos draudžiamos praktikos;

   iii) nuostatų, susijusių su esminiais pakeitimais, praktinio įgyvendinimo;

   iv) 6 straipsnio 3 dalyje nurodytų vienodų sąlygų praktinio įgyvendinimo, įskaitant pavyzdžius, susijusius su III priede nurodytomis didelės rizikos DI sistemomis;

   v) 52 straipsnyje nustatytų skaidrumo pareigų praktinio įgyvendinimo;

   vi) šio reglamento sąsajų su kitais atitinkamais Sąjungos teisės aktais, be kita ko, kiek tai susiję su jų vykdymo užtikrinimo nuoseklumu.

Skelbdama tokias gaires, Komisija ypač daug dėmesio skiria MVĮ, įskaitant startuolius, vietos valdžios institucijų ir sektorių, kuriems šis reglamentas gali daryti didžiausią poveikį, poreikiams.

2 SKYRIUS

NACIONALINĖS KOMPETENTINGOS INSTITUCIJOS

59 straipsnis

Nacionalinių kompetentingų institucijų skyrimas

1. [išbraukta]

2. Šio reglamento tikslais kiekviena valstybė narė kaip nacionalines kompetentingas institucijas įsteigia arba jomis paskiria bent vieną notifikuojančiąją instituciją ir bent vieną rinkos priežiūros instituciją. Šių nacionalinių kompetentingų institucijų veikla organizuojama taip, kad būtų užtikrinti jų veiklos ir užduočių objektyvumo ir nešališkumo principai. Su sąlyga, kad laikomasi šių principų, atsižvelgiant į valstybės narės organizacinius poreikius tokią veiklą ir užduotis gali vykdyti viena ar kelios paskirtos institucijos.

3. Valstybės narės informuoja Komisiją apie paskirtą (-as) instituciją (-as).

4. Valstybės narės užtikrina, kad nacionalinėms kompetentingoms institucijoms būtų suteikta pakankamai finansinių išteklių, techninės įrangos ir aukštos kvalifikacijos žmogiškųjų išteklių jų užduotims pagal šį reglamentą veiksmingai vykdyti.

5. Ne vėliau kaip *[vieni metai po šio reglamento įsigaliojimo]*, o vėliau – likus šešiems mėnesiams iki 84 straipsnio 2 dalyje nurodyto termino valstybės narės informuoja Komisiją apie nacionalinių kompetentingų institucijų finansinių išteklių, techninės įrangos bei žmogiškųjų išteklių būklę ir įvertina jų tinkamumą. Komisija šią informaciją perduoda Valdybai aptarti ir galimoms rekomendacijoms pateikti.

6. Komisija padeda nacionalinėms kompetentingoms institucijoms keistis patirtimi.

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

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

VII ANTRAŠTINĖ DALIS

III PRIEDE IŠVARDYTŲ DIDELĖS RIZIKOS DI SISTEMŲ ES DUOMENŲ BAZĖ

60 straipsnis

III priede išvardytų didelės rizikos DI sistemų ES duomenų bazė

1. Komisija, bendradarbiaudama su valstybėmis narėmis, sukuria ir tvarko ES duomenų bazę, kurioje laikoma 2 dalyje nurodyta informacija, susijusi su III priede nurodytomis ir pagal 51 bei 54a straipsnius užregistruotomis didelės rizikos DI sistemomis. Nustatydama tokios duomenų bazės funkcines specifikacijas, Komisija konsultuojasi su DI valdyba.

2. VIII priedo I dalyje išvardytus duomenis jų registravimo metu į ES duomenų bazę įveda atitinkamai tiekėjai, įgaliotieji atstovai ir atitinkami naudotojai. VIII priedo II dalies 1–11 punktuose išvardytus duomenis pagal 51 straipsnį į ES duomenų bazę įveda tiekėjai arba, kai taikytina, įgaliotasis atstovas. VIII priedo II dalies 12 punkte nurodyti duomenys automatiškai generuojami duomenų bazėje, remiantis atitinkamų naudotojų pagal 51 straipsnio 2 dalį pateikta informacija. VIIIa priede išvardytus duomenis pagal 54a straipsnį į duomenų bazę įveda galimi tiekėjai arba tiekėjai.

3. [išbraukta]

4. ES duomenų bazėje nesaugoma jokių asmens duomenų, išskyrus VIII priede išvardytą informaciją, ir ji nedaro poveikio 70 straipsniui.

5. Komisija yra ES duomenų bazės valdytoja. Ji teikia tiekėjams, galimiems tiekėjams ir naudotojams tinkamą techninę ir administracinę paramą.

5a. ES duomenų bazėje esanti pagal 51 straipsnį užregistruota informacija yra prieinama visuomenei. Pagal 54a 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 ir visuomenei.

VIII ANTRAŠTINĖ DALIS

PRIEŽIŪRA PO PATEIKIMO RINKAI, DALIJIMASIS INFORMACIJA IR RINKOS PRIEŽIŪRA

1 SKYRIUS

PRIEŽIŪRA PO PATEIKIMO RINKAI

61 straipsnis

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

1. Tiekėjai nustato priežiūros po pateikimo rinkai sistemą ir ją dokumentuoja tokiu būdu, kuris yra proporcingas didelės rizikos DI sistemos keliamai rizikai.

2. Kad tiekėjas galėtų įvertinti, ar DI sistemos per visą jų gyvavimo ciklą atitinka III antraštinės dalies 2 skyriuje nustatytus reikalavimus, priežiūros po pateikimo rinkai sistema renka, dokumentuoja ir analizuoja atitinkamus duomenis, kuriuos gali pateikti naudotojai arba kurie gali būti renkami naudojantis kitais informacijos apie didelės rizikos DI sistemų veiksmingumą šaltiniais. Ši pareiga neapima DI sistemų naudotojų, kurie yra teisėsaugos institucijos, neskelbtinų operatyvinių duomenų.

3. Priežiūros po pateikimo rinkai sistema grindžiama priežiūros po pateikimo rinkai planu. Priežiūros po pateikimo rinkai planas yra vienas iš IV priede nurodytų techninių dokumentų. Komisija priima įgyvendinimo aktą, kuriame nustatomos išsamios nuostatos dėl priežiūros po pateikimo rinkai plano šablono ir į planą įtrauktinų elementų sąrašo.

4. Didelės rizikos DI sistemų, kurioms taikomi II priedo A skirsnyje nurodyti teisės aktai, atveju, jeigu pagal tuos teisės aktus priežiūros po pateikimo rinkai sistema ir planas jau yra nustatyti, laikoma, kad pakanka pagal tuos teisės aktus parengtų priežiūros po pateikimo rinkai dokumentų, su sąlyga, kad naudojamas 3 dalyje nurodytas šablonas.

Pirma 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 SKYRIUS

DALIJIMASIS INFORMACIJA APIE RIMTUS INCIDENTUS

62 straipsnis

Pranešimas apie rimtus incidentus

1. DI sistemas Sąjungos rinkai pateikiantys tiekėjai valstybių narių, kuriose įvyko rimtas incidentas, rinkos priežiūros institucijoms praneša apie visus tuos incidentus.

Toks pranešimas turi būti 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 sužino apie rimtą incidentą.

2. Gavusi pranešimą, susijusį 3 straipsnio 44 punkto c papunktyje nurodytu rimtu incidentu, atitinkama rinkos priežiūros institucija informuoja 64 straipsnio 3 dalyje nurodytas nacionalines valdžios institucijas ar įstaigas. Siekdama palengvinti 1 dalyje nustatytų pareigų laikymąsi Komisija parengia specialias gaires. Tos gairės pateikiamos ne vėliau kaip per 12 mėnesių nuo šio reglamento įsigaliojimo.

3. III priedo 5 punkte nurodytų didelės rizikos DI sistemų, kurias rinkai pateikė arba pradėjo naudoti tiekėjai, kurie yra finansų įstaigos, kurioms pagal Sąjungos finansinių paslaugų teisės aktus taikomi reikalavimai, susiję su jų vidaus valdymu, tvarka ar procesais, atveju turi būti pranešama tik apie 3 straipsnio 44 punkto c papunktyje nurodytus rimtus incidentus.

4. Didelės rizikos DI sistemų, kurios yra priemonių saugos komponentai arba kurios pačios yra priemonės, kurioms taikomas Reglamentas (ES) 2017/745 ir Reglamentas (ES) 2017/746, atveju turi būti pranešama tik apie 3 straipsnio 44 punkto c papunktyje nurodytus rimtus incidentus ir apie juos pranešama valstybių narių, kuriose įvyko tas incidentas, šiuo tikslu pasirinktai nacionalinei kompetentingai institucijai.

3 SKYRIUS

VYKDYMO UŽTIKRINIMAS

63 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. Tačiau siekiant veiksmingai užtikrinti šio reglamento vykdymą laikoma, kad:

   a) nuorodos į ekonominės veiklos vykdytoją pagal Reglamentą (ES) 2019/1020 apima visus šio reglamento 2 straipsnyje nurodytus veiklos vykdytojus;

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

2. Vykdydamos savo pareigas pranešti pagal Reglamento (ES) 2019/1020 34 straipsnio 4 dalį, rinkos priežiūros institucijos praneša Komisijai apie atitinkamos pagal šį reglamentą vykdomos rinkos priežiūros veiklos rezultatus.

3. Didelės rizikos DI sistemų, susijusių su gaminiais, kuriems taikomi II priedo A skirsnyje išvardyti teisės aktai, atveju šio reglamento tikslais rinkos priežiūros institucija yra pagal tuos teisės aktus paskirta institucija, atsakinga už rinkos priežiūros veiklą, arba pagrįstomis aplinkybėmis ir su sąlyga, kad bus užtikrintas veiksmų koordinavimas, valstybės narės nurodyta kita atitinkama institucija.

Šio reglamento 65, 66, 67 ir 68 straipsniuose nurodytos procedūros netaikomos DI sistemoms, susijusioms su gaminiais, kuriems taikomi II priedo A skirsnyje išvardyti teisės aktai, kai tokiuose teisės aktuose jau numatytos procedūros, kurių tikslas yra toks pat. Tokiu atveju taikomos sektorių procedūros.

4. Didelės rizikos DI sistemų, kurias rinkai pateikia arba pradeda naudoti arba finansų įstaigos, reglamentuojamos Sąjungos finansinių paslaugų teisės aktais, atveju šio reglamento tikslais rinkos priežiūros institucija yra atitinkama nacionalinė institucija, atsakinga už tų įstaigų finansinę priežiūrą pagal tuos teisės aktus, jeigu DI sistemos pateikimas rinkai, pradėjimas naudoti arba naudojimas yra tiesiogiai susijęs su tų finansinių paslaugų teikimu.

Nukrypstant nuo pirmesnės pastraipos, pagrįstomis aplinkybėmis ir su sąlyga, kad bus užtikrintas veiksmų koordinavimas, šio reglamento tikslais valstybė narė gali rinkos priežiūros institucija paskirti kitą atitinkamą instituciją.

Nacionalinės rinkos priežiūros institucijos, prižiūrinčios reguliuojamas kredito įstaigas, reglamentuojamos Direktyva 2013/36/ES, kurios dalyvauja bendrame priežiūros mechanizme (BPM), nustatytame Tarybos reglamentu (ES) Nr. 1204/2013, 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.

5. 1 punkto a papunktyje išvardytų didelės rizikos DI sistemų atveju, jei sistemos naudojamos teisėsaugos tikslais, III priedo 6, 7 ir 8 punktuose valstybės narės šio reglamento tikslais rinkos priežiūros institucijomis paskiria nacionalines institucijas, kurios prižiūri teisėsaugos, sienų kontrolės, imigracijos, prieglobsčio ar teisminių institucijų veiklą, arba kompetentingas duomenų apsaugos priežiūros institucijas pagal Direktyvą (ES) 2016/680 arba Reglamentą (ES) 2016/679. Rinkos priežiūros veikla jokiu būdu nedaro poveikio teisminių institucijų nepriklausomumui ar ja kitaip nesikišama į jų veiklą, kai jos vykdo teismines funkcijas.

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

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

8. Nedarant poveikio pagal Reglamentą (ES) 2019/1020 nustatytiems įgaliojimas, kai aktualu, ir neviršijant to, kas būtina rinkos priežiūros institucijų užduotims atlikti, tiekėjas šioms įstaigoms suteikia 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.

9. Prieiga prie didelės rizikos DI sistemos pirminio kodo rinkos priežiūros institucijoms suteikiama gavus motyvuotą prašymą ir tik tada, kai įvykdomos visos šios sąlygos:

a) prieiga prie pirminio kodo yra būtina siekiant įvertinti didelės rizikos DI sistemos atitiktį III antraštinės dalies 2 skyriuje nustatytiems reikalavimams ir

b) bandymo ir (arba) audito procedūros ir tikrinimai, pagrįsti tiekėjo pateiktais duomenimis ir dokumentais, buvo išnagrinėti arba pasirodė esantys nepakankami.

10. Visa rinkos priežiūros institucijų gauta informacija ir dokumentai tvarkomi laikantis 70 straipsnyje nustatytų konfidencialumo pareigų.

11. Skundus atitinkamai rinkos priežiūros institucijai gali pateikti bet kuris fizinis ar juridinis asmuo, turintis pagrindo manyti, kad buvo pažeistos šio reglamento nuostatos.

Pagal Reglamento (ES) 2019/1020 11 straipsnio 3 dalies e punktą ir 7 dalies a punktą į skundus atsižvelgiama rinkos priežiūros veiklos tikslais ir jie nagrinėjami laikantis rinkos priežiūros institucijų tuo tikslu nustatytų specialių procedūrų.

63a straipsnis

Rinkos priežiūros institucijų vykdoma bandymo realiomis sąlygomis priežiūra

1. Rinkos priežiūros institucijos turi kompetenciją ir įgaliojimus užtikrinti, kad bandymas realiomis sąlygomis atitiktų šį reglamentą.

2. Kai bandymas realiomis sąlygomis atliekamas DI sistemų, kurios prižiūrimos DI srities apribotoje bandomojoje reglamentavimo aplinkoje pagal 54 straipsnį, atžvilgiu, rinkos priežiūros institucijos, vykdydamos DI srities apribotos bandomosios reglamentavimo aplinkos priežiūros funkciją, patikrina, ar laikomasi 54a straipsnio nuostatų. Tos institucijos gali atitinkamai leisti, kad tiekėjas arba galimas tiekėjas atliktų bandymą realiomis sąlygomis nukrypdamas nuo 54a straipsnio 4 dalies f ir g punktuose nustatytų sąlygų.

3. Jei galimas tiekėjas, tiekėjas arba bet kuri trečioji šalis rinkos priežiūros instituciją yra informavę apie rimtą incidentą arba jei ji turi kitų priežasčių manyti, kad nevykdomos 54a ir 54b 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 naudotojas (-ai) pakeistų bet kurį bandymo realiomis sąlygomis aspektą.

4. Jeigu rinkos priežiūros institucija priima šio straipsnio 3 dalyje nurodytą sprendimą arba pateikia prieštaravimą, kaip tai suprantama 54a straipsnio 4 dalies b punkte, sprendime arba prieštaravime nurodomos jo priežastys ir sąlygos, kurių laikydamasis tiekėjas arba galimas tiekėjas gali sprendimą arba prieštaravimą užginčyti.

5. Kai taikytina, kai rinkos priežiūros institucija priima šio straipsnio 3 dalyje nurodytą sprendimą, ji praneša to sprendimo motyvus kitų valstybių narių, kuriose ta DI sistema buvo išbandyta pagal bandymų planą, rinkos priežiūros institucijoms.

64 straipsnis

Pagrindines teises saugančių institucijų įgaliojimai

1. [išbraukta]

2. [išbraukta]

3. Nacionalinės valdžios institucijos arba įstaigos, prižiūrinčios, kaip laikomasi pareigų pagal Sąjungos teisę dėl pagrindinių teisių, įskaitant teisę nebūti diskriminuojamu, apsaugos, kai naudojamos III priede nurodytos didelės rizikos DI sistemos, arba užtikrinančios tų pareigų laikymąsi, turi teisę prašyti visų pagal šį reglamentą parengtų ar saugomų dokumentų ir gauti prie jų prieigą, kai prieiga prie tų dokumentų yra būtina pareigoms pagal jų įgaliojimus vykdyti neperžengiant jų jurisdikcijos ribų. Atitinkama valdžios institucija ar įstaiga apie tokį prašymą informuoja atitinkamos valstybės narės rinkos priežiūros instituciją.

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

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

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

65 straipsnis

Nacionalinio lygmens riziką keliančioms DI sistemoms taikoma procedūra

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

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

   Jeigu atlikdama vertinimą rinkos priežiūros institucija nustato, kad DI sistema neatitinka šiame reglamente nustatytų reikalavimų ir pareigų, ji nepagrįstai nedelsdama reikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų reikiamų taisomųjų veiksmų, kad užtikrintų DI sistemos atitiktį, pašalintų DI sistemą iš rinkos arba ją atšauktų per laikotarpį, kurį ji gali nustatyti.

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

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

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

5. Jeigu per 2 dalyje nurodytą laikotarpį su DI sistema susijusios veiklos vykdytojas nesiima tinkamų taisomųjų veiksmų, rinkos priežiūros institucija imasi visų tinkamų laikinųjų priemonių, kad būtų uždraustas arba apribotas DI sistemos tiekimas jos nacionalinei rinkai, gaminys būtų pašalintas iš rinkos arba atšauktas. Apie tokias priemones ta institucija 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 kilmė, įtariamos neatitikties ir keliamos rizikos pobūdis, taikomų nacionalinių priemonių pobūdis ir trukmė, taip pat atitinkamo veiklos vykdytojo pateikti argumentai. Visų pirma rinkos priežiūros institucijos nurodo, ar neatitiktis sietina su viena ar daugiau iš šių priežasčių:

-a) nesilaikoma 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo;

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

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

c) nesilaikoma 52 straipsnyje nustatytų nuostatų;

d) bendrosios paskirties DI sistemos neatitinka 4a straipsnyje nurodytų reikalavimų ir pareigų.

7. Valstybių narių, išskyrus procedūrą inicijavusią valstybę narę, rinkos priežiūros institucijos nepagrįstai nedelsdamos informuoja Komisiją ir kitas valstybes nares apie visas priemones, kurių ėmėsi, ir pateikia visą turimą papildomą informaciją, susijusią su atitinkamos DI sistemos neatitiktimi, o jei nesutinka su nacionaline priemone, apie kurią pranešta – savo prieštaravimus.

8. Jeigu per tris mėnesius nuo 5 dalyje nurodyto pranešimo gavimo nei valstybė narė, nei Komisija nepareiškia prieštaravimų dėl laikinosios priemonės, kurios ėmėsi valstybė narė, ta priemonė laikoma pagrįsta. Tai nedaro poveikio atitinkamo veiklos vykdytojo procesinėms teisėms pagal Reglamento (ES) 2019/1020 18 straipsnį. Jeigu nesilaikoma 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo, šios dalies pirmame sakinyje nurodytas laikotarpis sutrumpinamas iki 30 dienų.

9. Tuomet visų valstybių narių rinkos priežiūros institucijos užtikrina, kad atitinkamai DI sistemai nepagrįstai nedelsiant būtų taikomos tinkamos ribojamosios priemonės, pvz., gaminys būtų pašalintas iš rinkos.

66 straipsnis

Sąjungos apsaugos procedūra

1. Jeigu per tris mėnesius nuo 65 straipsnio 5 dalyje nurodyto pranešimo gavimo arba tuo atveju, kai nesilaikoma 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo, per 30 dienų kuri nors valstybė narė pareiškia prieštaravimų dėl priemonės, kurios ėmėsi kita valstybė narė, 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 9 mėnesius arba tuo atveju, kai nesilaikoma 5 straipsnyje nurodyto su dirbtiniu intelektu susijusios praktikos draudimo, per 60 dienų nuo 65 straipsnio 5 dalyje nurodyto pranešimo gavimo dienos nusprendžia, ar nacionalinė priemonė yra pagrįsta. Apie tokį sprendimą ji praneša atitinkamai valstybei narei. Apie tokį sprendimą Komisija informuoja ir visas kitas valstybes nares.

2. Jei Komisija mano, kad priemonė, kurios ėmėsi atitinkamos valstybės narės rinkos priežiūros institucija, yra pagrįsta, visų valstybių narių rinkos priežiūros institucijos užtikrina, kad dėl atitinkamos DI sistemos būtų imtasi tinkamų ribojamųjų priemonių, pavyzdžiui, nepagrįstai nedelsiant DI sistema būtų pašalinta iš jų rinkos, ir atitinkamai informuoja Komisiją. Jei Komisija mano, kad nacionalinė priemonė yra nepagrįsta, atitinkamos valstybės narės rinkos priežiūros institucija priemonę pašalina ir apie tai 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.

67 straipsnis

Riziką keliančios reikalavimus atitinkančios didelės rizikos arba bendrosios paskirties DI sistemos

1. Jeigu atlikusi vertinimą pagal 65 straipsnį valstybės narės rinkos priežiūros institucija nustato, kad, nors didelės rizikos arba bendrosios paskirties DI sistema atitinka šio reglamento reikalavimus, ji kelia riziką žmonių sveikatai ar saugai arba pagrindinėms teisėms, ji reikalauja, kad atitinkamas veiklos vykdytojas nepagrįstai nedelsdamas imtųsi visų tinkamų priemonių užtikrinti, kad rinkai pateikta arba pradėta naudoti atitinkama DI sistema nebekeltų tokios rizikos, pašalintų DI sistemą iš rinkos arba ją atšauktų per laikotarpį, kurį ji gali nustatyti.

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

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

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

5. Savo sprendimą Komisija skiria atitinkamoms valstybėms narėms ir informuoja visas kitas valstybes nares.

68 straipsnis

Oficiali neatitiktis

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

   a) atitikties ženklu paženklinta pažeidžiant 49 straipsnį;

   b) nebuvo ženklinama atitikties ženklu;

   c) neparengta ES atitikties deklaracija;

   d) ES atitikties deklaracija parengta netinkamai;

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

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

68a straipsnis

Sąjungos gaminių bandymų įstaigos dirbtinio intelekto srityje

1. Komisija pagal Reglamento (ES) 2019/1020 21 straipsnį paskiria vieną ar daugiau Sąjungos gaminių bandymų įstaigų dirbtinio intelekto srityje.

2. Nedarant poveikio Reglamento (ES) 2019/1020 21 straipsnio 6 dalyje nurodytų Sąjungos gaminių bandymų įstaigų veiklai, 1 dalyje nurodytos Sąjungos gaminių bandymų įstaigos Valdybos arba rinkos priežiūros institucijų prašymu taip pat teikia nepriklausomas technines ar mokslines konsultacijas.

68b straipsnis

Centrinis nepriklausomų ekspertų rezervas

1. DI valdybos prašymu Komisija įgyvendinimo aktu priima nuostatas dėl centrinio nepriklausomų ekspertų rezervo, skirto pagal šį reglamentą atliekamai vykdymo užtikrinimo veiklai remti, sukūrimo, administravimo ir finansavimo.

2. Ekspertus atrenka Komisija ir jie įtraukiami į centrinį rezervą remiantis naujausiomis mokslinėmis ar techninėmis ekspertinėmis žiniomis dirbtinio intelekto srityje, tinkamai atsižvelgiant į technines sritis, kurioms taikomi šiame reglamente nustatyti reikalavimai ir pareigos, ir į rinkos priežiūros institucijų veiklą pagal Reglamento (ES) 2019/1020 11 straipsnį. Rezervo ekspertų skaičių Komisija nustato atsižvelgdama į būtinus poreikius.

3. Ekspertai gali atlikti šias užduotis:

a) rinkos priežiūros institucijų prašymu teikti joms konsultacijas ir padėti jų darbe;

b) talkinti atliekant tarpvalstybinius rinkos priežiūros tyrimus, nurodytus 58 straipsnio h punkte, nedarant poveikio rinkos priežiūros institucijų įgaliojimams;

c) teikti konsultacijas ir padėti Komisijai vykdyti savo pareigas, susijusias su pagal 66 straipsnį nustatyta apsaugos sąlyga.

4. Ekspertai savo užduotis vykdo nešališkai, objektyviai ir užtikrina informacijos ir duomenų, gautų vykdant savo užduotis ir veiklą, konfidencialumą. Kiekvienas ekspertas parengia interesų deklaraciją, kuri skelbiama viešai. Komisija nustato sistemas ir procedūras, skirtas aktyviai valdyti galimus interesų konfliktus ir užkirsti jiems kelią.

5. Gali būti reikalaujama, kad valstybės narės sumokėtų mokesčius už ekspertų konsultacijas ir paramą. Mokesčių struktūrą ir dydį, taip pat atlygintinų išlaidų dydį ir struktūrą Komisija nustato 1 dalyje nurodytu įgyvendinimo aktu, atsižvelgdama į tinkamo šio reglamento įgyvendinimo tikslus, išlaidų efektyvumą ir būtinybę užtikrinti galimybę visoms valstybėms narėms veiksmingai naudotis ekspertų paslaugomis.

6. Komisija sudaro palankesnes sąlygas valstybėms narėms prireikus laiku pasinaudoti ekspertų paslaugomis ir užtikrina, kad Sąjungos gaminių bandymų įstaigų pagal 68a straipsnį ir ekspertų pagal šį straipsnį vykdomos paramos veiklos derinimas būtų organizuojamas veiksmingai ir suteiktų kuo didesnės pridėtinės vertės.

IX ANTRAŠTINĖ DALIS

ELGESIO KODEKSAI

69 straipsnis

Savanoriško konkrečių reikalavimų taikymo elgesio kodeksai

1. Komisija ir valstybės narės padeda rengti elgesio kodeksus, kuriais siekiama skatinti savanoriškai kuo geriau taikyti vieną ar daugiau šio reglamento III antraštinės dalies 2 skyriuje nustatytų reikalavimų DI sistemoms, išskyrus didelės rizikos DI sistemas, atsižvelgiant į turimus techninius sprendimus, kuriais sudaromos sąlygos taikyti tokius reikalavimus.

2. Komisija ir valstybės narės padeda rengti elgesio kodeksus, kuriais siekiama skatinti savanorišką konkrečių reikalavimų, susijusių, pavyzdžiui, su aplinkosauginiu tvarumu, be kita ko, kiek tai susiję su efektyviu energijos vartojimu grindžiamu programavimu, neįgaliesiems skirta prieiga, suinteresuotųjų subjektų dalyvavimu projektuojant bei kuriant DI sistemas ir kūrimo grupių įvairove, taikymą visoms DI sistemoms, remiantis aiškiais tikslais ir tų tikslų pasiekimui įvertinti skirtais pagrindiniais veiklos rodikliais. Komisija ir valstybės narės, kai tinkama, taip pat padeda rengti savanoriškai taikytinus elgesio kodeksus dėl naudotojų pareigų, susijusių su DI sistemomis.

3. Savanoriškai taikytinus elgesio kodeksus gali rengti atskiri DI sistemų tiekėjai arba jiems atstovaujančios organizacijos, arba ir vieni, ir kiti, be kita ko, įtraukdami naudotojus, suinteresuotuosius subjektus ir jiems atstovaujančias organizacijas, arba, kai tinkama, naudotojai, kiek tai susiję su jų pareigomis. Elgesio kodeksai gali būti taikomi vienai ar daugiau DI sistemų, atsižvelgiant į atitinkamų sistemų numatytosios paskirties panašumą.

4. Komisija ir valstybės narės, skatindamos ir padėdamos rengti šiame straipsnyje nurodytus elgesio kodeksus, atsižvelgia į konkrečius MVĮ tiekėjų, įskaitant startuolius, interesus ir poreikius.

X ANTRAŠTINĖ DALIS

KONFIDENCIALUMAS IR SANKCIJOS

70 straipsnis

Konfidencialumas

1. Šį reglamentą taikančios nacionalinės kompetentingos institucijos, notifikuotosios įstaigos, Komisija, Valdyba ir visi kiti fiziniai ar juridiniai asmenys pagal Sąjungos arba nacionalinę teisę įdiegia tinkamas technines ir organizacines priemones, kuriomis būtų užtikrintas informacijos ir duomenų, kuriuos jie gavo vykdydami savo užduotis ir veiklą, konfidencialumas, kad visų pirma būtų apsaugoti:

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

b) veiksmingas šio reglamento įgyvendinimas, visų pirma susijęs su patikrinimais, tyrimais arba auditu;

c) visuomenės ir nacionalinio saugumo interesai;

d) baudžiamojo ar administracinio proceso vientisumas;

e) pagal Sąjungos arba nacionalinę teisę įslaptintos informacijos vientisumas.

2. Nedarant poveikio 1 daliai, informacija, kuria konfidencialiai tarpusavyje keičiasi nacionalinės kompetentingos institucijos ir nacionalinės kompetentingos institucijos bei Komisija, neatskleidžiama iš anksto nepasikonsultavus su ją pateikusia nacionaline kompetentinga institucija ir naudotoju, kai III priedo 1, 6 ir 7 punktuose nurodytas didelės rizikos DI sistemas naudoja teisėsaugos, sienų kontrolės, imigracijos ar prieglobsčio institucijos, jei toks atskleidimas keltų grėsmę visuomenės ir nacionalinio saugumo interesams. Ši pareiga keistis 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 ir 7 punktuose, tiekėjos, IV priede nurodyti techniniai dokumentai laikomi tų institucijų patalpose. Tos institucijos užtikrina, kad, pateikusios prašymą, atitinkamai 63 straipsnio 5 ir 6 dalyse nurodytos rinkos priežiūros institucijos galėtų nedelsdamos susipažinti su dokumentais arba gauti jų kopijas. Susipažinti su tais dokumentais ar jų kopijomis leidžiama tik rinkos priežiūros institucijos darbuotojams, turintiems atitinkamo lygio asmens patikimumo pažymėjimą.

3. 1 ir 2 dalys nedaro poveikio Komisijos, valstybių narių ir atitinkamų jų institucijų, taip pat notifikuotųjų įstaigų teisėms ir pareigoms keistis informacija bei platinti įspėjimus, be kita ko, tarpvalstybinio bendradarbiavimo kontekste, taip pat atitinkamų šalių pareigoms teikti informaciją pagal valstybių narių baudžiamąją teisę.

71 straipsnis

Sankcijos

1. Laikydamosi šiame reglamente nustatytų sąlygų, valstybės narės nustato taisykles dėl sankcijų, įskaitant administracines baudas, taikytinų už šio reglamento pažeidimus, ir imasi visų būtinų priemonių užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Jomis visų pirma atsižvelgiama į MVĮ tiekėjų, įskaitant startuolius, dydį bei interesus ir jų ekonominį gyvybingumą. Jomis taip pat atsižvelgiama į tai, ar DI sistema naudojama asmeninės neprofesinės veiklos kontekste.

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

3. Už bet kurio iš 5 straipsnyje nurodytų su dirbtiniu intelektu susijusios praktikos draudimų nesilaikymą skiriamos iki 30 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra bendrovė, iki 6 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų). MVĮ, įskaitant startuolius, atveju šios baudos sudaro iki 3 proc. jų pasaulinės praėjusių finansinių metų metinės apyvartos.

4. Iki 20 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra bendrovė, iki 4 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų) skiriamos už toliau išdėstytų nuostatų, susijusių su veiklos vykdytojais ar notifikuotosiomis įstaigomis, pažeidimus:

-a) tiekėjų pareigų pagal 4b ir 4c straipsnius;

a) tiekėjų pareigų pagal 16 straipsnį;

b) tam tikrų kitų asmenų pareigų pagal 23a straipsnį;

c) įgaliotųjų atstovų pareigų pagal 25 straipsnį;

d) importuotojų pareigų pagal 26 straipsnį;

e) platintojų pareigų pagal 27 straipsnį;

f) naudotojų pareigų pagal 29 straipsnio 1–6a dalis;

g) notifikuotųjų įstaigų reikalavimų ir pareigų pagal 33 straipsnį, 34 straipsnio 1, 3 bei 4 dalis ir 34a straipsnį;

h) tiekėjams ir naudotojams taikomų skaidrumo pareigų pagal 52 straipsnį.

MVĮ, įskaitant startuolius, atveju šios baudos sudaro iki 2 proc. jų pasaulinės praėjusių finansinių metų metinės apyvartos.

5. Už neteisingos, neišsamios ar klaidinančios informacijos pateikimą notifikuotosioms įstaigoms ir nacionalinėms kompetentingoms institucijoms atsakant į jų prašymą taikomos iki 10 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra bendrovė, iki 2 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų). MVĮ, įskaitant startuolius, atveju šios baudos sudaro iki 1 proc. jų pasaulinės praėjusių finansinių metų metinės apyvartos.

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

a) pažeidimo pobūdį, rimtumą, trukmę ir jo pasekmes;

aa) tai, ar pažeidimas padarytas tyčia ar dėl aplaidumo;

ab) visus veiksmus, kurių veiklos vykdytojas ėmėsi, kad ištaisytų pažeidimą ir sumažintų galimą neigiamą jo poveikį;

b) tai, ar kitos rinkos priežiūros institucijos kitose valstybėse narėse jau yra skyrusios administracines baudas tam pačiam veiklos vykdytojui už tą patį pažeidimą;

ba) tai, ar kitos institucijos jau yra skyrusios administracines baudas tam pačiam veiklos vykdytojui už kitų Sąjungos ar nacionalinės teisės pažeidimus, kai tokie pažeidimai padaryti dėl tos pačios veiklos arba neveikimo, kurie yra svarbus šio Akto pažeidimas;

c) pažeidimą padariusio veiklos vykdytojo dydį, metinę apyvartą ir rinkos dalį;

d) kitas atsakomybę sunkinančias ar švelninančias aplinkybes, susijusias su konkrečiu atveju, pavyzdžiui, gautą finansinę naudą arba nuostolius, kurių buvo tiesiogiai ar netiesiogiai išvengta dėl pažeidimo.

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

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

9. Rinkos priežiūros institucijos naudojimuisi įgaliojimais pagal šį straipsnį taikomos atitinkamos procedūrinės garantijos laikantis Sąjungos ir valstybės narės teisės, įskaitant veiksmingas teismines teisių gynimo priemones ir tinkamą procesą.

72 straipsnis

Administracinės baudos Sąjungos institucijoms, agentūroms ir įstaigoms

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

   a) pažeidimo pobūdį, rimtumą, trukmę ir jo pasekmes;

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

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

2. Už bet kurio iš 5 straipsnyje nurodytų su dirbtinio intelekto praktika susijusių draudimų nesilaikymą skiriamos iki 500 000 EUR dydžio administracinės baudos.

3. Už DI sistemos neatitiktį bet kuriems pagal šį reglamentą nustatytiems reikalavimams ar pareigoms, išskyrus nustatytus 5 ir 10 straipsniuose, skiriamos iki 250 000 EUR dydžio administracinės baudos.

4. Prieš priimdamas sprendimus pagal šį straipsnį, Europos duomenų apsaugos priežiūros pareigūnas suteikia Sąjungos institucijai, agentūrai ar įstaigai, dėl kurios jis pradėjo procesą, galimybę būti išklausytai su galimu pažeidimu susijusiais klausimais. Europos duomenų apsaugos priežiūros pareigūnas savo sprendimus grindžia tik tais elementais ir aplinkybėmis, dėl kurių atitinkamos šalys galėjo pateikti 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, laikomos Sąjungos bendrojo biudžeto pajamomis.

XI ANTRAŠTINĖ DALIS

DELEGUOTIEJI ĮGALIOJIMAI IR KOMITETO PROCEDŪRA

73 straipsnis

Įgaliojimų delegavimas

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

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

Likus ne mažiau kaip devyniems mėnesiams iki 5 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 7 straipsnio 1 dalyje, 7 straipsnio 3 dalyje, 11 straipsnio 3 dalyje, 43 straipsnio 5 bei 6 dalyse ir 48 straipsnio 5 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Jis įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

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

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

74 straipsnis

Komiteto procedūra

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

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

XII ANTRAŠTINĖ DALIS

BAIGIAMOSIOS NUOSTATOS

75 straipsnis

Reglamento (EB) Nr. 300/2008 pakeitimas

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

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

_____

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

76 straipsnis

Reglamento (ES) Nr. 167/2013 pakeitimas

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

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

_____

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

77 straipsnis

Reglamento (ES) Nr. 168/2013 pakeitimas

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

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

_____

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

78 straipsnis

Direktyvos 2014/90/ES pakeitimas

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

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

_____

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

79 straipsnis

Direktyvos (ES) 2016/797 pakeitimas

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

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

_____

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

80 straipsnis

Reglamento (ES) 2018/858 pakeitimas

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

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

_____

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

81 straipsnis

Reglamento (ES) 2018/1139 pakeitimas

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

1) 17 straipsnis papildomas šia dalimi:

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

_____

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

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) YYY/XX [dėl dirbtinio intelekto], atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.“;

3) 43 straipsnis papildomas šia dalimi:

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

4) 47 straipsnis papildomas šia dalimi:

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

5) 57 straipsnis papildomas šia dalimi:

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

6) 58 straipsnis papildomas šia dalimi:

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

82 straipsnis

Reglamento (ES) 2019/2144 pakeitimas

Reglamento (ES) 2019/2144 11 straipsnis papildomas šia 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) YYY/XX [dėl dirbtinio intelekto]*, atsižvelgiama į to reglamento III antraštinės dalies 2 skyriuje nustatytus reikalavimus.

_____

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

83 straipsnis

Rinkai jau pateiktos ar pradėtos naudoti DI sistemos

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

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

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

84 straipsnis

Vertinimas ir peržiūra

1. [išbraukta]

1b. Komisija kas 24 mėnesius nuo šio reglamento įsigaliojimo iki įgaliojimų delegavimo laikotarpio pabaigos įvertina poreikį iš dalies pakeisti III priede pateiktą sąrašą. To vertinimo rezultatus ji pateikia Europos Parlamentui ir Tarybai.

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

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

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

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

4. Iki [*treji metai po 85 straipsnio 2 dalyje nurodytos šio reglamento taikymo pradžios dienos*] ir vėliau kas ketverius metus, kai tinkama, Komisija įvertina savanoriškų elgesio kodeksų poveikį ir veiksmingumą skatinant III antraštinės dalies 2 skyriuje nustatytų reikalavimų taikymą DI sistemoms, išskyrus didelės rizikos DI sistemas, ir galbūt kitų papildomų reikalavimų taikymą DI sistemoms, be kita ko, kiek tai susiję su aplinkosauginiu tvarumu.

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

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

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

85 straipsnis

Įsigaliojimas ir taikymas

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

2. Šis reglamentas taikomas nuo [36 mėnesiai po šio reglamento įsigaliojimo].

3. Nukrypstant nuo 2 dalies:

   a) III antraštinės dalies 4 skyrius ir VI antraštinė dalis taikomi nuo [dvylika mėnesių po šio reglamento įsigaliojimo];

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

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas / Pirmininkė	*Pirmininkas / Pirmininkė*

I PRIEDAS

[išbraukta]

II 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

1. 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).

2. 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);

3. 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);

4. 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);

5. 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);

6. 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);

7. 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);

8. 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.

III PRIEDAS

6 STRAIPSNIO 3 DALYJE NURODYTOS DIDELĖS RIZIKOS DI SISTEMOS

Kiekvienoje iš 1–8 punktuose išvardytų sričių konkrečiai nurodytos DI sistemos laikomos didelės rizikos DI sistemomis pagal 6 straipsnio 3 dalį:

1. Biometriniai duomenys:

   a) nuotolinio biometrinio tapatybės nustatymo sistemos.

2. Ypatingos svarbos infrastruktūra:

   a) DI sistemos, kurias numatoma naudoti kaip saugos komponentus valdant ir eksploatuojant ypatingos svarbos skaitmeninę infrastruktūrą, užtikrinant kelių eismą ir vandens, dujų, šilumos ir elektros energijos tiekimą.

3. Švietimas ir profesinis mokymas:

   a) DI sistemos, kurias numatoma naudoti siekiant suteikti prieigą fiziniams asmenims prie švietimo ir profesinio mokymo įstaigų ar programų visais lygmenimis, į jas priimti arba paskirti;

   b) DI sistemos, kurias numatoma naudoti mokymosi rezultatams vertinti, įskaitant atvejus, kai tie rezultatai naudojami siekiant valdyti fizinių asmenų mokymosi procesą švietimo ir profesinio mokymo įstaigose ar programose visais lygmenimis.

4. Užimtumas, darbuotojų valdymas ir galimybė dirbti savarankiškai:

   a) DI sistemos, kurias numatoma naudoti fizinių asmenų įdarbinimui arba atrankai, visų pirma siekiant teikti tikslinius darbo skelbimus, analizuoti ir filtruoti darbo prašymus ir vertinti kandidatus;

b) DI sistemos, kurias numatoma naudoti priimant sprendimus dėl paaukštinimo arba sutartinių darbo santykių nutraukimo, siekiant paskirstyti užduotis remiantis individualiu elgesiu arba asmenybės bruožais ar savybėmis ir 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, kurias numatoma naudoti valdžios institucijose arba jų vardu siekiant įvertinti fizinių asmenų tinkamumą gauti esminės viešosios paramos išmokas ir paslaugas, taip pat teikti, sumažinti, panaikinti arba susigrąžinti tokias išmokas;

b) DI sistemos, kurias numatoma naudoti siekiant įvertinti fizinių asmenų kreditingumą arba nustatyti jų kredito reitingą, išskyrus atvejus, kai DI sistemas savo reikmėms pradeda naudoti tiekėjai, kurie yra mažosios ir vidutinės įmonės, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB priede;

c) DI sistemos, kurias numatoma naudoti teikiant arba nustatant prioritetines teiktinas skubias pirmosios pagalbos paslaugas, įskaitant ugniagesių ir medicininės pagalbos paslaugas;

d) DI sistemos, kurias numatoma naudoti siekiant įvertinti su fiziniais asmenimis susijusią riziką ir kainodarą gyvybės bei sveikatos draudimo atveju, išskyrus atvejus, kai DI sistemas savo reikmėms pradeda naudoti tiekėjai, kurie yra mažosios ir vidutinės įmonės, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB priede.

6. Teisėsauga:

a) DI sistemos, kurias numatoma naudoti teisėsaugos institucijose arba jų vardu siekiant įvertinti riziką, ar fizinis asmuo gali padaryti nusikaltimą arba pakartotinai padaryti nusikaltimą, arba riziką, kad fizinis asmuo gali tapti nusikalstamų veikų auka;

b) DI sistemos, kurias numatoma naudoti teisėsaugos institucijose arba jų vardu kaip poligrafus ir panašias priemones arba siekiant nustatyti fizinio asmens emocinę būklę;

c) [išbraukta]

d) DI sistemos, kurias numatoma naudoti teisėsaugos institucijose arba jų vardu, siekiant įvertinti įrodymų patikimumą tiriant nusikalstamas veikas arba vykdant baudžiamąjį persekiojimą už jas;

e) DI sistemos, kurias numatoma naudoti teisėsaugos institucijose arba jų vardu, siekiant nuspėti faktinį arba galimą nusikalstamos veikos padarymą ar tokios nusikalstamos veikos pakartotinį padarymą, remiantis 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;

f) DI sistemos, kurias numatoma naudoti teisėsaugos institucijose arba jų vardu, siekiant profiliuoti fizinius asmenis, kaip nurodyta Direktyvos (ES) 2016/680 3 straipsnio 4 dalyje, išaiškinant ar tiriant nusikalstamas veikas arba vykdant baudžiamąjį persekiojimą už jas.

g) [išbraukta]

7. Migracija, prieglobstis ir sienų kontrolės valdymas:

a) DI sistemos, kurias numatoma naudoti kompetentingose valdžios institucijose arba jų vardu kaip poligrafus ir panašias priemones arba siekiant nustatyti fizinio asmens emocinę būklę;

b) DI sistemos, kurias numatoma naudoti kompetentingose valdžios institucijose arba jų vardu, siekiant įvertinti riziką, įskaitant saugumo riziką, nelegalios migracijos riziką arba riziką sveikatai, kurią kelia fizinis asmuo, ketinantis atvykti į valstybės narės teritoriją arba į ją atvykęs;

c) [išbraukta]

d) DI sistemos, kurias numatoma naudoti kompetentingose valdžios institucijose arba jų vardu, siekiant išnagrinėti prašymus suteikti prieglobstį, išduoti vizą ir leidimus gyventi ir susijusius skundus, susijusius su fizinių asmenų tinkamumu prašyti suteikti pabėgėlio statusą.

8. Teisingumo vykdymas ir demokratiniai procesai:

a) DI sistemos, kurias numatoma naudoti teisminėje institucijoje arba jos vardu, siekiant aiškinti faktus arba teisę ir taikyti teisę konkretiems faktų rinkiniams.

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, asmenį (-is), kuriantį (-čius) sistemą, sistemos sukūrimo datą ir versiją;

   b) tai, kaip DI sistema sąveikauja arba, kai taikytina, gali būti naudojama, kad sąveikautų su aparatine arba programine įranga, kuri nėra pačios DI sistemos sudedamoji dalis;

   c) atitinkamos programinės įrangos arba aparatinės programinės įrangos versijas ir su versijos atnaujinimu susijusį bet kokį reikalavimą;

   d) visų DI sistemų pateikimo rinkai arba pradėjimo naudoti formų aprašymą (pvz., programinės įrangos paketai, įmontuoti į aparatinę įrangą, parsisiunčiami, API ir t. t.);

   e) aparatinės įrangos, kurią naudojant numatoma naudoti DI sistemą, aprašymą;

   f) nuotraukas arba iliustracijas, kuriose matomi išorės požymiai, ženklinimas ir šių gaminių vidaus sandara, jeigu DI sistema yra gaminių komponentas;

   g) naudotojui skirtas naudojimo instrukcijas ir, kai tinkama, įdiegimo instrukcijos;

2. išsamus DI sistemos ir jos kūrimo proceso elementų aprašymas, įskaitant:

   a) metodus ir etapus, susijusius su DI sistemos kūrimu, įskaitant, kai tinkama, 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 dizaino sprendimus, įskaitant loginį pagrindą ir prielaidas, taip pat dėl asmenų ar asmenų grupių, kurių atžvilgiu numatoma naudoti sistemą; pagrindinius klasifikacijos sprendimus; tai, ką siekiama optimizuoti sistema, ir įvairių parametrų svarbą; numatomų sistemos rezultatų aprašymą; sprendimus apie bet kokį galimą kompromisą dėl techninių sprendimų, kurie buvo priimti siekiant laikytis III antraštinės dalies 2 skyriuje nustatytų reikalavimų;

c) sistemos struktūros aprašymą, kuriame paaiškinama, kaip programinės įrangos komponentai prijungiami prie vienas kito arba kaip papildo vienas kitą ir kaip jie apskritai įtraukiami į visą procesą; kompiuterių išteklius, kurie naudojami DI sistemai kurti, mokyti, bandyti ir validuoti;

d) kai tinkama, duomenų reikalavimus, nustatytus duomenų lapuose, kuriuose aprašoma mokymo metodika ir būdai, ir naudojamus mokymo duomenų rinkinius, įskaitant bendrą šių duomenų rinkinių aprašymą, informaciją apie jų kilmę, taikymo sritį ir pagrindines charakteristikas; tai, kaip duomenys buvo gauti ir atrinkti; ženklinimo procedūras (pvz., prižiūrimo mokymosi), duomenų valymo metodiką (pvz., išskirčių nustatymas);

e) žmogaus atliekamos priežiūros priemonių, reikalingų pagal 14 straipsnį, vertinimą, įskaitant techninių priemonių, kurios reikalingos siekiant padėti naudotojams interpretuoti DI sistemų išvedinius pagal 13 straipsnio 3 dalies d punktą, vertinimą;

f) kai taikytina, išsamų iš anksto nustatytų DI sistemos ir jos efektyvaus veikimo pakeitimų aprašymą, įskaitant visą atitinkamą informaciją, susijusią su techniniais sprendimais, kurie pritaikyti taip, kad užtikrintų nuolatinę DI sistemos atitiktį atitinkamiems III antraštinės dalies 2 skyriuje 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, patikimumui, kibernetiniam saugumui ir atitikčiai kitiems susijusiems reikalavimams, nustatytiems III antraštinės dalies 2 skyriuje, taip pat galimam diskriminaciniam poveikiui įvertinti; bandymų žurnalus ir visas bandymų ataskaitas, kuriose nurodoma data ir kurias pasirašo atsakingi asmenys, taip pat atsižvelgiant į f punkte nurodytus iš anksto nustatytus pakeitimus;

3. išsami informacija apie DI sistemos stebėseną, veikimą ir kontrolę, visų pirma atsižvelgiant į: jos pajėgumus ir efektyvaus veikimo apribojimus, įskaitant konkretiems asmenims arba asmenų grupėms, kurių atžvilgiu numatoma naudoti sistemą, taikomus tikslumo laipsnius ir bendrą tikėtiną tikslumo lygį, atsižvelgiant į numatytąją paskirtį; numatomas 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 nustatytas technines priemones, siekiant padėti naudotojams interpretuoti DI sistemų išvedinius; kai tinkama, įvesties duomenų specifikacijas;

4. išsamus rizikos valdymo sistemos aprašymas pagal 9 straipsnį;

5. atitinkamų sistemos pakeitimų, padarytų tiekėjo per jos gyvavimo ciklą, aprašymas;

6. 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, priimtų siekiant laikytis III antraštinės dalies 2 skyriuje nurodytų reikalavimų, aprašymas, įskaitant kitų taikomų susijusių standartų ir techninių specifikacijų sąrašą;

7. ES atitikties deklaracijos kopija;

8. išsamus sistemos, taikomos vertinant DI sistemos efektyvų veikimą atliekant priežiūrą po pateikimo rinkai pagal 61 straipsnį, aprašymas, įskaitant 61 straipsnio 3 dalyje nurodytą priežiūros po pateikimo rinkai planą.

V PRIEDAS
ES ATITIKTIES DEKLARACIJA

48 straipsnyje nurodytoje ES atitikties deklaracijoje pateikiama visa toliau nurodyta informacija:

1. DI sistemos pavadinimas ir tipas ir bet kuri papildoma vienareikšmiška nuoroda, sudaranti sąlygas identifikuoti DI sistemą ir užtikrinti jos atsekamumą;

2. tiekėjo arba, jei taikoma, jo įgaliotojo atstovo pavadinimas (vardas ir pavardė) ir adresas;

3. patvirtinimas, kad ES atitikties deklaracija išduota tik tiekėjo atsakomybe;

4. pareiškimas, kad atitinkama DI sistema atitinka šį reglamentą ir, jei taikoma, kitus atitinkamus Sąjungos teisės aktus, pagal kuriuos numatyta išduoti ES atitikties deklaraciją;

5. nuoroda į bet kuriuos naudojamus susijusius darniuosius standartus arba bet kurią kitą bendrąją specifikaciją, dėl kurios deklaruojama atitiktis;

6. kai taikoma, notifikuotosios įstaigos pavadinimas ir identifikacinis numeris, atliktos atitikties vertinimo procedūros aprašymas ir išduoto sertifikato identifikaciniai duomenys;

7. deklaracijos išdavimo vieta ir data, ją pasirašiusio asmens vardas, pavardė ir pareigos bei 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 2–4 punktais pagrįsta atitikties vertinimo procedūra.

2. Tiekėjas patvirtina, kad nustatyta kokybės valdymo sistema atitinka 17 straipsnio reikalavimus.

3. Tiekėjas nagrinėja techniniuose dokumentuose pateiktą informaciją, kad įvertintų DI sistemos atitiktį atitinkamiems III antraštinės dalies 2 skyriuje išvardytiems esminiams reikalavimams.

4. Tiekėjas taip pat patikrina, ar 61 straipsnyje nurodytas DI sistemos projektavimo ir plėtojimo 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 patvirtina, kad pakeista kokybės valdymo sistema ir toliau atitinka 3.2 punkte nurodytus reikalavimus, arba priima sprendimą, kad 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 nurodomas (pateikiamas):

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, programų sąsajas (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, kad sudarytų sąlygas tinkamai įvertinti DI sistemos atitiktį III antraštinės dalies 2 skyriuje nustatytiems reikalavimams. Visais atvejais, kai notifikuotosios įstaigos netenkina tiekėjo atlikti bandymai, notifikuotoji įstaiga, kai tinkama, tiesiogiai atlieka tinkamus bandymus.

4.5. Prieiga prie DI sistemos pirminio kodo notifikuotosioms įstaigoms suteikiama gavus pagrįstą prašymą ir tik tada, kai įvykdomos visos šios sąlygos:

a) prieiga prie pirminio kodo yra būtina siekiant įvertinti didelės rizikos DI sistemos atitiktį III antraštinės dalies 2 skyriuje nustatytiems reikalavimams ir

b) bandymo ir (arba) audito procedūros ir tikrinimai, pagrįsti tiekėjo pateiktais duomenimis ir dokumentais, buvo išnagrinėti arba pasirodė esantys nepakankami.

4.6. Apie sprendimą pranešama tiekėjui arba jo įgaliotajam atstovui. Pranešime pateikiamos techninių dokumentų vertinimo išvados ir motyvuotas sprendimas dėl įvertinimo.

Jeigu DI sistema atitinka III antraštinės dalies 2 skyriuje nustatytus reikalavimus, notifikuotoji įstaiga išduoda techninių dokumentų vertinimo 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 antraštinės dalies 2 skyriuje nustatytų reikalavimų, notifikuotoji įstaiga atsisako išduoti ES 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 DI sistemos atitikties vertinimo, sistema turės būti pakartotinai mokoma. Šiuo atveju notifikuotosios įstaigos pagrįstame sprendime dėl vertinimo, kuriuo atsisakoma išduoti ES techninių dokumentų įvertinimo sertifikatą, nurodomos konkrečios aplinkybės, susijusios su duomenų, naudotų mokant DI sistemą, kokybe, visų pirma su reikalavimų nesilaikymu susijusios priežastys.

4.7. Bet kurį DI sistemos pakeitimą, kuris galėtų turėti įtakos DI sistemos atitikčiai reikalavimams arba jos numatytajai paskirčiai, tvirtina ES 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 padarytus pakeitimus. Numatomus pakeitimus įvertina notifikuotoji įstaiga, kuri nusprendžia, ar dėl tų pakeitimų reikia atlikti naują atitikties vertinimą pagal 43 straipsnio 4 dalį ir ar į juos galima atsižvelgti papildant ES techninių dokumentų įvertinimo sertifikatą. Pastaruoju atveju notifikuotoji įstaiga įvertina pakeitimus, praneša tiekėjui apie savo sprendimą ir, jei pakeitimai patvirtinami, pateikia jam ES 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 įvykdytų patvirtintos kokybės valdymo sistemos sąlygas.

5.2. Vertinimo tikslais tiekėjas leidžia notifikuotajai įstaigai patekti į patalpas, kuriose projektuojamos, kuriamos 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. Atlikdama šiuos auditus, notifikuotoji įstaiga gali atlikti papildomus DI sistemos, dėl kurios buvo išduotas ES techninių dokumentų įvertinimo sertifikatas, bandymus.

VIII PRIEDAS

INFORMACIJA, KURIĄ TURI PATEIKTI VEIKLOS VYKDYTOJAI, REGISTRUODAMI DIDELĖS RIZIKOS DI SISTEMAS PAGAL 51 STRAIPSNĮ

Tiekėjai, įgaliotieji atstovai ir naudotojai, kurie yra valdžios institucijos, agentūros ar įstaigos, pateikia I dalyje nurodytą informaciją. Tiekėjai arba, kai taikytina, įgaliotieji atstovai užtikrina, kad II dalies 1–11 punktuose nurodyta informacija apie jų didelės rizikos DI sistemas būtų išsami, teisinga ir nuolat atnaujinama. II dalies 12 punkte nurodyta informacija automatiškai generuojama duomenų bazėje.

I dalis. Informacija, susijusi su veiklos vykdytojais (registruojantis veiklos vykdytojais)

-1. Veiklos vykdytojo tipas (tiekėjas, įgaliotasis atstovas arba naudotojas);

1. Tiekėjo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

2. kai informaciją pateikia kitas asmuo veiklos vykdytojo vardu – to asmens pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys,

II dalis. Su didelės rizikos DI sistema susijusi informacija

1. Tiekėjo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

2. kai taikytina, įgaliotojo atstovo pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys;

3. DI sistemos prekybinis pavadinimas ir bet kuri papildoma vienareikšmiška nuoroda, sudaranti sąlygas identifikuoti DI sistemą ir užtikrinti jos atsekamumą;

4. DI sistemos numatytosios paskirties aprašymas;

5. DI sistemos statusas (pateikta rinkai arba naudojama; nebeteikiama rinkai / nebenaudojama, atšaukta);

6. notifikuotosios įstaigos išduoto sertifikato rūšis, numeris ir galiojimo pabaigos data ir, kai taikytina, tos notifikuotosios įstaigos pavadinimas arba identifikacinis numeris;

7. kai taikytina, 6 punkte nurodyto sertifikato skenuota kopija;

8. valstybės narės, kuriose DI sistema pateikiama arba buvo pateikiama rinkai, pradėta naudoti arba tapo prieinama Sąjungoje;

9. 48 straipsnyje nurodytos ES atitikties deklaracijos kopija;

10. elektroninės naudojimo instrukcijos;

11. URL, kaip papildoma informacija (neprivaloma);

12. Naudotojų pavadinimas (vardas ir pavardė), adresas ir kontaktiniai duomenys.

VIIIa PRIEDAS

INFORMACIJA, KURIĄ REIKIA PATEIKTI REGISTRUOJANT III PRIEDE IŠVARDYTAS DIDELĖS RIZIKOS DI SISTEMAS, KIEK TAI SUSIJĘ SU BANDYMU REALIOMIS SĄLYGOMIS PAGAL 54a STRAIPSNĮ

Turi būti pateikiama ir po to nuolat atnaujinama toliau nurodyta informacija, susijusi su bandymu realiomis sąlygomis, kuris turi būti užregistruotas pagal 54a straipsnį:

1. Visoje Sąjungoje taikomas vienintelis unikalusis bandymo realiomis sąlygomis identifikacinis numeris;

2. Tiekėjo arba galimo tiekėjo ir naudotojų, 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.

IX PRIEDAS

SĄJUNGOS TEISĖS AKTAI DĖL DIDELĖS APIMTIES IT SISTEMŲ LAISVĖS, SAUGUMO IR TEISINGUMO ERDVĖJE

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) Pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 767/2008, Reglamentas (EB) Nr. 810/2009, Reglamentas (ES) 2017/2226, Reglamentas (ES) 2016/399, Reglamentas XX/2018 [Sąveikumo reglamentas] ir Sprendimas 2004/512/EB ir panaikinamas Tarybos sprendimas 2008/633/TVR, COM(2018) 302 final. Turi būti atnaujinta teisės aktų leidėjams priėmus reglamentą (2021 m. balandžio / gegužės mėn.).

3. Sistema EURODAC

a) Iš dalies pakeistas pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO dėl biometrinių duomenų lyginimo sistemos EURODAC sukūrimo siekiant veiksmingai taikyti Reglamentą (ES) XXX/XXX [Reglamentas dėl prieglobsčio ir migracijos valdymo] ir Reglamentą (ES) XXX/XXX [Perkėlimo į ES reglamentas] siekiant 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 reglamentai (ES) 2018/1240 ir (ES) 2019/818, COM(2020) 614 final.

4. Atvykimo ir išvykimo sistema

a) 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).

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

a) 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 (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 (OL L 135, 2019 5 22, p. 85).