TRINITI JUREX
TALLINN RIGA VILNIUS

EUROPOS SĄJUNGOS SKAITMENINĖ PERTVARKA

2025 m. Kovas

TRINITI JUREX
TALLINN RIGA VILNIUS

Turinys

TRINITI JUREX
TALLINN RIGA VILNIUS

I DALIS.
Kibernetinis saugumas

Šioje dalyje aptarsime 3 pagrindinius Europos Sąjungos teisės aktus, formuojančius kibernetinio saugumo reikalavimus:

1. TIS2 direktyva – teisės aktas, skirtas svarbių infrastruktūrų ir paslaugų kibernetiniam saugumui užtikrinti, stiprinant rizikų valdymą ir kibernetinio saugumo priemonių taikymą. Ši direktyva nustato minimalias kibernetinio saugumo priemones, kurias turi įdiegti ypatingos svarbos sektoriuose veikiantys vieši ir privatūs subjektai, veikiantys tokiose srityse, kaip energetika, transportas, sveikata ir finansai.

2. Kibernetinio atsparumo aktas – šis teisės aktas siekia užtikrinti, kad visi skaitmeniniai produktai ir paslaugos Europos rinkoje atitiktų griežtus kibernetinio saugumo standartus. Aktas įpareigoja gamintojus užtikrinti, jog jų kuriami produktai būtų atsparūs kibernetinėms grėsmėms per visą jų gyvavimo ciklą.

3. Skaitmeninės veiklos atsparumo finansų sektoriuje reglamentas - reglamentas skirtas finansų sektoriaus veiklos tęstinumui ir kibernetiniam atsparumui užtikrinti. Jis numato privalomas taisykles finansų įstaigoms, kurios privalo užtikrinti savo technologijų sistemų saugumą ir galimybę atsilaikyti prieš kibernetinius išpuolius.

TRINITI JUREX
TALLINN RIGA VILNIUS

TIS2 Direktyva

Direktyva dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje sąjungoje užtikrinti (es) 2022/2555

Pagrindinis TIS2 tikslas - įdiegti aukšto lygio kibernetinio saugumo standartą visoje Europos Sąjungoje ir padidinti bendrą kibernetinio saugumo lygį. Ši direktyva yra nukreipta į ypatingos svarbos sektoriuose veikiančių viešųjų ir privačiųjų subjektų kibernetinį atsparumą. Direktyvoje pateikiamos konkrečios priemonės, susijusios su kibernetinio saugumo rizikos valdymu.

TIS2 direktyva įsigaliojo 2023 m. sausio 16 d., o Europos Sąjungos valstybės narės iki 2024 m. spalio 17 d. turėjo perkelti TIS2 direktyvą į nacionalinę teisę ir paskelbti su ja susijusią reikalingą informaciją.

TAIKYMAS

TIS2 direktyva taikoma organizacijoms, kurios yra skirstomos į didelės svarbos ir ypatingos svarbos sektorių subjektus, atsižvelgiant į jų svarbos mastą pagal sektoriaus rūšį, teikiamas paslaugas ir dydį.

Didelės svarbos sektoriai: energija (elektros energija, centralizuotas šildymas ir vėsinimas, nafta, dujos ir vandenilis); transportas (oro, geležinkelių, vandens ir kelių); bankininkystė; finansų rinkų infrastruktūra; sveikata; geriamasis vanduo; nuotekos; skaitmeninė infrastruktūra; IKT paslaugų valdymas; viešasis administravimas ir kosmosas.

Kiti ypatingos svarbos sektoriai: pašto ir kurjerių paslaugos; atliekų tvarkymas; chemikalų gamyba, produkcija ir platinimas; maisto gamyba, perdirbimas ir platinimas; medicinos prietaisų, kompiuterių ir elektronikos, mašinų ir įrangos, motorinių transporto priemonių, priekabų ir puspriekabių bei kitos transporto įrangos gamyba; skaitmeninių paslaugų teikėjai (internetinės prekyvietės, interneto paieškos sistemos ir socialinių tinklų paslaugų platformos) ir mokslinių tyrimų organizacijos.

TIS 2 direktyva įpareigoja nacionalines valstybes skirstyti subjektus pagal jų teikiamų paslaugų reikšmę visuomenės sveikatai, viešajam saugumui, visuomenės saugumui bei riziką, kuri kyla dėl šių paslaugų sutrikimų.

ĮGYVENDINIMAS LIETUVOJE

Šios direktyvos reikalavimai buvo perkelti į Lietuvos Respublikos kibernetinio saugumo įstatymą ir jį lydinčius teisės aktus.

Vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu, kibernetinio saugumo subjektu, kuriam taikomi perkelti TIS2 reikalavimai, tampama nuo įmonės įregistravimo Kibernetinio saugumo informacinėje sistemoje.

Galite pasitikrinti, ar Jūsų įmonė nepateko į sistemą čia.

Nacionalinis kibernetinio saugumo centras

Svarbu atkreipti dėmesį, kad netiesiogiai Lietuvos Respublikos kibernetinio saugumo įstatymo reikalavimai taikomi ir informacinių technologijų ir tinklų paslaugas teikiančioms įmonėms, kurios šias paslaugas teikia kibernetinio saugumo subjektams.

Į Kibernetinio saugumo informacinę sistemą įtrauktoms įmonėms numatytas pereinamasis laikotarpis:

- 12 mėn. organizacinių reikalavimų įgyvendinimui.
- 24 mėn. techninių reikalavimų įgyvendinimui.

Nacionalinis kibernetinio saugumo centras paskirtas priežiūros institucija.

PAGRINDINIAI REIKALAVIMAI

Kibernetinio saugumo rizikos valdymo priemonės: visiems subjektams nustatyti įpareigojimai įgyvendinti tinkamas technines, organizacines ir operatyvines saugumo priemones. Šios priemonės apima rizikų analizę, incidentų valdymą, veiklos tęstinumo užtikrinimą ir tiekimo grandinės saugumą.

Pranešimų apie incidentus teikimas: TIS2 direktyva nustato etapais grindžiamą incidentų pranešimo mechanizmą, kurį sudaro:

- Ankstyvasis perspėjimas - pradinis pranešimas per 24 val. nuo incidento nustatymo.
- Incidento pranešimas - detalesnė informacija turi būti pateikta per 72 val.
- Galutinė ataskaita - išsami informacija turi būti pateikta per 1 mėn. nuo incidento užbaigimo.

Lietuvoje apie incidentus privaloma pranešti Nacionaliniam kibernetinio saugumo centrui.

Valdymo ir atitikties užtikrinimas: įmonės turi prisiimti atsakomybę už kibernetinio saugumo reikalavimų vykdymą, užtikrinant, kad jų organizacijos laikytųsi direktyvą įgyvendinančių teisės aktų nuostatų.

BAUDOS

Lietuvos Respublikos kibernetinio saugumo įstatyme nustatyti maksimalūs baudų dydžiai už teisės aktuose nustatytų reikalavimų nesilaikymą ar trukdymą priežiūros institucijoms, įskaitant jų pasitelkiamus subjektus, atlikti joms priskirtas funkcijas:

1. Esminiam subjektui – iki 10 mln. eur arba iki 2 procentų juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė.

2. Svarbiam subjektui – iki 7 mln. eur arba iki 1,4 procento juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė.

3. Biudžetinei įstaigai, kuri yra esminis subjektas – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė kaip 60 000 eur.

4. Biudžetinei įstaigai, kuri yra svarbus subjektas – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė kaip 30 000 eur.

Pažeidimai skirstomi į pavojingus, vidutinio pavojingumo ir nedidelio pavojingumo ir atitinkamai pagal tai bus nustatomas skiriamos baudos dydis:

1. Iki 100 procentų aukščiau nurodytos maksimalios baudos, jeigu pažeidimas yra laikomas pavojingu pažeidimu.
2. Iki 50 procentų aukščiau nurodytos maksimalios baudos, jeigu pažeidimas yra laikomas vidutinio pavojingumo pažeidimu.
3. Iki 10 procentų aukščiau nurodytos maksimalios baudos, jeigu pažeidimas yra laikomas nedidelio pavojingumo pažeidimu.

TRINITI JUREX
TALLINN RIGA VILNIUS

Kibernetinio atsparumo aktas

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

Pagrindinis Kibernetinio atsparumo akto (KAA) tikslas - suderinti taisykles ir standartus, taikomus pateikiant rinkai produktus ar programinę įrangą su skaitmeniniu komponentu. Juo siekiama sukurti kibernetinio saugumo standartų sistemą, kuri reglamentuotų tokių produktų planavimą, projektavimą, kūrimą ir techninę priežiūrą, o įsipareigojimų būtų laikomasi kiekviename etape. Numatyta pareiga rūpintis tokiais produktais visą jų gyvavimo trukmę.

KAA įsigaliojo 2024 m. lapkričio 20 d. Akte nustatytas pereinamasis laikotarpis, numatantis, kad gamintojai turi trejų metų laikotarpį (iki 2027 m.), užtikrinti savo produktų atitiktį KAA reikalavimams.

TAIKYMAS

Kibernetinio atsparumo aktas tiesiogiai taikomas verslo subjektams, tokiems kaip gamintojai, programinės įrangos kūrėjai, platintojai, importuotojai ir kiti verslo subjektai (pvz., perpardavinėtojai), kurie tiekia skaitmeninius produktus Europos Sąjungos rinkai.

PAGRINDINIAI REIKALAVIMAI

Saugumo standartai - KAA nustato būtinus kibernetinio saugumo reikalavimus sujungtiems įrenginiams (pvz., IoT) ir programinei įrangai, siekiant užtikrinti, kad įmonės įdiegtų tinkamas saugumo priemones produktų gyvavimo ciklo metu.

Rizikos valdymas - gamintojai privalo vykdyti kibernetinio saugumo rizikos analizę ir valdymą. Tai apima rizikos nustatymą, jos mažinimą ir grėsmių stebėjimą produktų gyvavimo laikotarpiu.

Saugumo testavimas - privalomi produktų saugumo bandymai prieš juos pateikiant rinkai. Tai užtikrins, kad produktai atitiktų Europos Sąjungos saugumo reikalavimus ir būtų atsparūs galimoms grėsmėms.

Aptikimo ir reagavimo priemonės - turi būti užtikrinta galimybė aptikti pažeidimus ir į juos reaguoti.

Atitikties deklaracijos - gamintojai privalo užtikrinti, kad jų produktai atitinka KAA reikalavimus ir pateikti atitikties deklaraciją. Jei produktas neatitinka reikalavimų, numatomos sankcijos.

Informavimas apie pažeidžiamumus - kibernetinio saugumo incidentai ir nustatyti pažeidžiamumai turi būti laiku pranešami atitinkamoms institucijoms, siekiant užtikrinti veiksmingą kibernetinio saugumo incidentų valdymą.

BAUDOS

KAA numatytos griežtos administracinės baudos už įvairius pažeidimus, įskaitant:

- Baudos už esminių reikalavimų pažeidimus: iki 15 mln. eurų arba 2,5 % metinių pajamų.
- Baudos už neteisingos informacijos pateikimą: iki 5 mln. eurų arba 1 % metinių pasaulinių pajamų.
- Baudos už kitus pažeidimus: iki 10 mln. eurų arba 2 % metinių pasaulinių pajamų.

TRINITI JUREX
TALLINN RIGA VILNIUS

Skaitmeninės veiklos atsparumo finansų sektoriuje reglamentas

2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl finansų sektoriaus skaitmeninio operacinio atsparumo ir kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 (DORA)

Pagrindinis DORA tikslas – sustiprinti Europos Sąjungos finansų sektoriaus skaitmeninės veiklos atsparumą, užtikrinant veiksmingą informacinių ir ryšių technologijų (toliau - IRT) rizikos valdymą bei incidentų valdymo sistemų veikimą. Kadangi finansų sektorius vis labiau priklauso nuo IRT priemonių ir paslaugų teikėjų, didėja ir trečiųjų šalių keliamų rizikų pavojus. Finansų sektoriaus subjektai, tokie kaip bankai, draudimo bendrovės, elektroninių pinigų ir mokėjimo įstaigos, investicinės įmonės ir kiti, dažnai remiasi IRT paslaugų teikėjais, kurie nėra tiesiogiai prižiūrimi ar jiems taikomi tie patys reguliavimo reikalavimai kaip finansų rinkos dalyviams. Netinkamai valdoma IRT rizika gali sutrikdyti finansinių paslaugų teikimą, sukelti domino efektą kitoms finansų institucijoms ir net paveikti visą ekonomiką. Todėl DORA siekia užtikrinti, kad finansų įstaigos turėtų stiprias incidentų valdymo, rizikos vertinimo bei ataskaitų teikimo sistemas, kurios padėtų joms išlikti atsparioms skaitmeninėje aplinkoje ir efektyviai reaguoti į kibernetinius incidentus. DORA nustato vieningą skaitmeninės veiklos atsparumo reguliavimo sistemą visose Europos Sąjungos valstybėse narėse, įpareigodama finansų sektoriaus subjektus užtikrinti, kad jie būtų pajėgūs atlaikyti, reaguoti ir atsigauti po bet kokių su IRT susijusių sutrikimų ar grėsmių.

TAIKYMAS

Nuo 2025 m. sausio 17 d. DORA taikoma:

- kredito įstaigoms;
- mokėjimo įstaigoms, įskaitant mokėjimo įstaigas, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366;
- informavimo apie sąskaitas paslaugų teikėjams;
- elektroninių pinigų įstaigoms, įskaitant elektroninių pinigų įstaigas, kurioms taikoma išimtis pagal Direktyvą 2009/110/EB;
- investicinėms įmonėms;
- kriptoturto paslaugų teikėjams, turintiems veiklos leidimą pagal Europos Parlamento ir Tarybos reglamentą dėl kriptoturto rinkų, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1093/2010 ir (ES) Nr. 1095/2010 ir direktyvos 2013/36/ES bei (ES) 2019/1937, ir su turtu susietų žetonų emitentams;
- centriniams vertybinių popierių depozitoriumams;
- pagrindinėms sandorio šalims;
- prekybos vietoms;
- sandorių duomenų saugykloms;
- alternatyvaus investavimo fondų valdytojams;
- valdymo įmonėms;
- duomenų teikimo paslaugų teikėjams;
- draudimo ir perdraudimo įmonėms;
- draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams;
- profesinių pensijų įstaigoms;
- kredito reitingų agentūroms;
- ypatingos svarbos lyginamųjų indeksų administratoriams;
- sutelktinio finansavimo paslaugų teikėjams;
- pakeitimo vertybiniais popieriais duomenų saugykloms;
- IRT paslaugas teikiančioms trečiosioms šalims.

PAGRINDINIAI REIKALAVIMAI

IRT rizikos valdymas – finansų sektoriaus subjektai turi sukurti ir įdiegti veiksmingas sistemas, leidžiančias identifikuoti, vertinti ir valdyti IRT keliamas grėsmes bei užtikrinti nuolatinį jų stebėjimą.

Operacinio atsparumo testavimas – finansų sektoriaus subjektai įpareigoti reguliariai atlikti įvairaus sudėtingumo testus, įskaitant pažangius kibernetinio saugumo testavimo metodus, siekiant įvertinti savo pasirengimą valdyti galimus technologinius sutrikimus.

Incidentų valdymas ir pranešimų teikimas – finansų sektoriaus subjektai privalo turėti aiškią incidentų valdymo sistemą, privalo užtikrinti greitą reagavimą į IRT sutrikimus bei pranešti priežiūros institucijoms apie reikšmingus kibernetinius incidentus ir grėsmes.

Trečiųjų šalių rizikos valdymas – finansų subjektai turi įvertinti IRT paslaugų teikėjų keliamą riziką ir užtikrinti, kad šie partneriai atitiktų saugumo reikalavimus. Kritiniams IRT paslaugų teikėjams turi būti taikoma papildoma priežiūra.

Informacijos dalijimasis – DORA skatina finansų rinkos subjektus keistis informacija apie kibernetines grėsmes, siekiant stiprinti bendrą sektoriaus atsparumą ir sumažinti galimų incidentų poveikį.

Siekiant šių reikalavimų veiksmingo įgyvendinimo, finansų sektoriaus subjektams reikia ne tik peržiūrėti savo strategijas, valdymo modelius ir veiklos procesus, bet ir užtikrinti aukščiausio lygio vadovų įsitraukimą bei nuoseklų naujų priemonių integravimą į kasdienę veiklą.

Lietuvoje IRT incidentų bei kibernetinių grėsmių ataskaitos teikiamos Lietuvos bankui. Papildomai siūlome paskaityti straipsnį:

2025 metus pradėsime su DORA: Ar esate pasiruošę naujiems iššūkiams?

BAUDOS

Gali būti taikomos:

1. Taisomosios priemonės, pavyzdžiui, reikalavimas nutraukti neteisėtą veiklą arba sustabdyti tam tikras praktikas.

2. Viešų pranešimų apie padarytus pažeidimus paskelbimas, kuriuose būtų nurodomas pažeidimo pobūdis ir fizinio arba juridinio asmens tapatybė.

3. Nacionalinėje teisėje nustatytos administracinės nuobaudos. Valstybės narės gali priimti sprendimą nenustatyti taisyklių dėl administracinių nuobaudų ar taisomųjų priemonių už pažeidimus, už kuriuos pagal jų nacionalinę teisę skiriamos baudžiamosios sankcijos.

Periodinės baudos dydis, apskaičiuojamas nuo sprendime dėl periodinės baudos skyrimo nustatytos dienos, gali sudaryti iki 1 % ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies vidutinės dienos pasaulinės apyvartos ankstesniais finansiniais metais.

SVARBU:

Krašto apsaugos ministerija kviečia mažas ir vidutines įmones pasinaudoti Europos Sąjungos finansavimo galimybėmis ir teikti paraiškas, kurios leis sustiprinti jų kibernetinį atsparumą.

Galima prašyti mažiausia finansinės paramos lėšų suma – 30 000 eur.

Galima prašyti didžiausia finansinės paramos lėšų suma – 60 000 eur.

Paraiška pildoma ir teikiama lietuvių kalba elektronine forma, naudojantis paraiškų teikimo sistema Submittable. Paraiškų vertinimą organizuoja Central Project Management Agency.

Paraiškų pateikimo terminas: iki 2025 m. balandžio 4 d. 23:59 val.

Daugiau informacijos rasite čia.

Labai mažų, mažų ir vidutinių įmonių kibernetinio atsparumo didinimas

TRINITI JUREX
TALLINN RIGA VILNIUS

II DALIS.
Duomenų reglamentavimas

Šioje dalyje bus aptarti pagrindiniai Europos Sąjungos teisės aktai, formuojantys skaitmeninių paslaugų ir duomenų valdymo strategiją.

1. Duomenų aktas – nustato teisinę sistemą, skatinančią duomenų dalijimąsi ir naudojimą Europos Sąjungoje. Jis orientuotas į duomenų prieinamumo didinimą ir vartotojų teisių užtikrinimą.

2. Skaitmeninių paslaugų aktas – reglamentuoja interneto platformų atsakomybę ir sąlygas, kaip jos tvarko turinį, siekiant užtikrinti vartotojų saugumą internete.

3. Skaitmeninių rinkų aktas - užtikrina naudotojams geresnes paslaugas ir sąžiningesnes kainas, kartu skatinant inovacijas bei sudarant palankesnes sąlygas technologijų startuoliams augti.

4. Dirbtinio intelekto aktas – reguliuoja dirbtinio intelekto sistemų kūrimą ir naudojimą, kad būtų užtikrinta, jog jos būtų saugios ir etiškos.

TRINITI JUREX
TALLINN RIGA VILNIUS

Duomenų aktas

2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentu (ES) 2023/2854 dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių, kuriuo iš dalies keičiami Reglamentas (ES) 2017/2394 ir Direktyva (ES) 2020/1828

Pagrindinis Duomenų akto tikslas - stiprinti Europos Sąjungos valstybių duomenų ekonomiką. Juo siekiama, kad duomenys, ypač gamybiniai, būtų lengviau prieinami ir patogiau naudojami, skatinant duomenimis grindžiamas inovacijas bei gerinant duomenų prieinamumą visoje Europos Sąjungoje. Akte nustatytos aiškios duomenų naudojimo ir dalijimosi jais taisyklės, užtikrinančios teisingą duomenų vertės paskirstymą suinteresuotosioms šalims.

Duomenų aktas įsigaliojo 2024 m. sausio 11 d. ir bus pradėtas taikyti 2025 m. rugsėjo 12 d.

TAIKYMAS

Duomenų aktas taikomas susietųjų gaminių gamintojams ir susijusių paslaugų teikėjams, kurie siūlo savo produktus Europos Sąjungos rinkoje, nepriklausomai nuo jų įsisteigimo vietos. Jis taip pat apima naudotojus Europos Sąjungoje, kurie naudoja šiuos gaminius ar paslaugas, ir duomenų turėtojus, kurie suteikia prieigą prie duomenų Europos Sąjungoje, nesvarbu, kur jie įsisteigę.

Reglamentas taikomas ir duomenų gavėjams Europos Sąjungoje, kurie gauna prieigą prie duomenų, bei debesijos ir kitų duomenų tvarkymo paslaugų teikėjams, dirbantiems su klientais Europos Sąjungoje. Be to, jis apima duomenų erdvių dalyvius, išmaniųjų sutarčių kūrėjus ir pardavėjus, kurie prisideda prie duomenų dalijimosi sistemų.

Šiuo aktu siekiama užtikrinti sąžiningą duomenų prieinamumą ir paskirstymą tarp visų suinteresuotųjų šalių.

PAGRINDINIAI REIKALAVIMAI

Prieiga prie duomenų – naudotojai turi teisę gauti prieigą prie jų naudojamų prijungtų įrenginių ir susijusių paslaugų generuojamų duomenų. Jie taip pat gali suteikti prieigą pasirinktiems trečiųjų šalių paslaugų teikėjams.

Sąžiningos sąlygos duomenų dalijimuisi – duomenų turėtojai turi taikyti sąžiningas, pagrįstas ir nediskriminacines sąlygas dalijantis duomenimis su kitais ūkio subjektais, užtikrinant skaidrią ir proporcingą kompensaciją.

Privatumo ir saugumo užtikrinimas – Duomenų aktas reglamentuoja ne asmens duomenų apsaugą ir nustato mechanizmus, kurie riboja neleistiną trečiųjų šalių prieigą prie Europos Sąjungos valdomų duomenų. Asmens duomenims ir toliau taikomas Bendrasis duomenų apsaugos reglamentas.

Verslo ir valdžios institucijų prieiga – viešojo sektoriaus institucijos ypatingomis aplinkybėmis gali reikalauti prieigos prie tam tikrų duomenų iš privačių įmonių, jei tai būtina visuomenės interesams užtikrinti, pavyzdžiui, ekstremalių situacijų metu.

Sąveikumo standartai – duomenų perdavimas tarp skirtingų sistemų ir paslaugų teikėjų turi būti kuo sklandesnis. Duomenų aktas nustato sąveikumo standartus, ypač debesijos paslaugoms, kad būtų lengviau keisti paslaugų teikėjus ir užtikrinti duomenų perkėlimą.

Tiesioginė ir netiesioginė prieiga – naudotojai turi teisę tiesiogiai ar per tarpininkus pasiekti duomenis, kuriuos generuoja jų naudojami įrenginiai ar paslaugos.

Saugumo ir prekybos paslapčių apsauga – nors duomenų turėtojai privalo dalytis duomenimis sąžiningomis sąlygomis, jie gali riboti prieigą, jei tai kelia pavojų jų saugumui ar konfidencialiai informacijai, tačiau tokie ribojimai turi būti pagrįsti.

Neteisėtos prieigos kontrolė – trečiųjų šalių (už Europos Sąjungos ribų) valdžios institucijos ir įmonės negali tiesiogiai reikalauti prieigos prie Europos Sąjungoje esančių duomenų, nebent tam yra aiškus teisinis pagrindas pagal Europos Sąjungos teisę.

Ginčų sprendimas – Duomenų aktas nustato priemones, kurios padeda spręsti ginčus tarp naudotojų, duomenų turėtojų ir gavėjų, jei kyla nesutarimų dėl duomenų prieigos ar naudojimo sąlygų.

Standartinės sutarčių sąlygos – Duomenų akte nustatyta, kad Europos Komisija parengs standartines sutarčių sąlygas, kurios padės įmonėms – ypač mažoms ir vidutinėms – užtikrinti aiškias ir sąžiningas duomenų naudojimo sąlygas.

BAUDOS

Duomenų akto reikalavimų nesilaikymas gali užtraukti baudą, kurios dydį kiekviena valstybė narė nustatys iki 2025 m. rugsėjo 12 d. Visgi Europos duomenų inovacijų valdyba koordinuos ir rekomenduos, kaip vienodinti baudas visoje Europos Sąjungoje, kad būtų užtikrinta aukšta nuoseklumo kokybė.

Valstybinė duomenų apsaugos inspekcija galės skirti baudą pagal Bendrojo duomenų apsaugos reglamento nuostatas (iki 20 mln. eurų arba 4 % įmonės metinių pajamų) dėl pažeidimų, susijusių su:

- verslo subjektų duomenų dalijimusi su vartotojais;
- verslo subjektų tarpusavio dalijimusi duomenimis;
- duomenų turėtojų, įpareigotų pagal Europos Sąjungos teisę suteikti prieigą prie duomenų, pareigų nevykdymu;
- duomenų prieigos suteikimu viešojo sektoriaus institucijoms, Europos Komisijai, Europos Centriniam Bankui ir Europos Sąjungos įstaigoms išimtinio poreikio pagrindu.

Europos duomenų apsaugos priežiūros pareigūnas taip pat turės teisę skirti administracines baudas už pažeidimus, susijusius su duomenų prieigos suteikimu viešojo sektoriaus institucijoms, Europos Komisijai, Europos Centriniam Bankui ir Europos Sąjungos įstaigoms išimtinio poreikio pagrindu.

TRINITI JUREX
TALLINN RIGA VILNIUS

Skaitmeninių paslaugų aktas

2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB

Pagrindinis Skaitmeninių paslaugų akto (toliau SPA) tikslas – sukurti saugesnę ir skaidresnę interneto aplinką, nustatant aiškias taisykles internetinėms platformoms ir socialinės žiniasklaidos tinklams. SPA įpareigoja šias platformas aktyviai kovoti su neteisėtu turiniu, neapykantą kurstančia kalba ir dezinformacija, taip pat užtikrinti vartotojų teisių apsaugą. Be to, SPA stiprina internetinių paslaugų teikėjų atsakomybę, skatindamas didesnį skaidrumą ir atskaitomybę – tai apima aiškius ataskaitų teikimo ir priežiūros mechanizmus. Kartu SPA sudaro palankesnes sąlygas inovacijoms ir konkurencingumui Europos Sąjungos vidaus rinkoje, suteikdamas verslui aiškias taisykles ir užtikrindamas vienodas sąlygas skaitmeninėje erdvėje.

TAIKYMAS

SPA tiesiogai visose Europos Sąjungos šalyes (įskaitant Lietuvą) taikomas nuo 2024 m. vasario 17 d. Kai kurios taisyklės, susijusios su labai didelėmis internetinėmis platformomis, kurias naudoja daugiau nei 10 % iš 450 mln. Europos Sąjungos naudotojų, ir labai didelėmis internetinėms paieškos sistemomis, kurias naudoja daugiau nei 10 % iš 450 mln. Europos Sąjungos naudotojų, taikomos nuo 2022 m. lapkričio 16 d., įskaitant prievoles teikti ataskaitas, atlikti nepriklausomus auditus, dalintis duomenimis ir taisyklės, susijusios su priežiūra (įskaitant mokesčių), tyrimais ir stebėsena.

SPA taikomas tarpininkavimo paslaugoms, siūlomoms paslaugos gavėjams, kurių įsisteigimo vieta yra Europos Sąjungoje arba kurie yra Europos Sąjungoje, neatsižvelgiant į tai, kur yra tų tarpininkavimo paslaugų teikėjų įsisteigimo vieta. Į SPA taikymo sritį patenka:

- Tarpininkavimo paslaugos, suteikiančios tinklo infrastruktūrą: interneto prieigos paslaugų teikėjai ir domenų vardų registruotojai (įskaitant prieglobos paslaugas);
- Prieglobos paslaugos, pavyzdžiui, debesijos ir saityno prieglobos paslaugos (įskaitant interneto platformas);
- Interneto platformos, suburiančios pardavėjus ir vartotojus, pavyzdžiui, elektroninės prekyvietės, programėlių parduotuvės, bendradarbiaujamosios ekonomikos platformos ir socialinės žiniasklaidos platformos;
- Labai didelės interneto platformos ir paieškos sistemos, kadangi kelia ypač didelę neteisėto turinio sklaidos ir žalos visuomenei riziką. Šioms platformoms numatytos specialios taisyklės.

PAGRINDINIAI REIKALAVIMAI

Kova su neteisėtu turiniu internete, įskaitant nelegalias prekes ir paslaugas, siekiant užtikrinti griežtesnę kontrolę ir didesnį skaidrumą. Vartotojams turi būti suteikta daugiau informacijos apie jiems rodomą reklamą bei galimybė lengvai pažymėti neteisėtą turinį, neapykantą kurstančią kalbą ar dezinformaciją. Platformos turi bendradarbiauti su „patikimais pranešėjais“, kad neteisėtas turinys būtų greičiau atpažįstamas ir pašalinamas. Taip pat nustatomi aiškūs įpareigojimai dėl prekiautojų atsekamumo internetinėse prekyvietėse, siekiant užkirsti kelią nesąžiningai ar pavojingai prekybai.

Vartotojų ir pilietinės visuomenės įgalinimas. Vartotojams turi būti suteikta galimybė užginčyti turinio modifikavimo sprendimus ir reikalauti žalos atlyginimo, pasitelkiant ginčų nagrinėjimo mechanizmus ar teisinius skundus. Valdžios institucijos ir mokslininkai turi turėti prieigą prie svarbiausių duomenų iš didžiųjų platformų, kad galėtų geriau įvertinti internete kylančias rizikas.

Be to, didinamas skaidrumas algoritmų veikimo srityje, suteikiant daugiau aiškumo apie tai, kaip vartotojams rekomenduojamas turinys ar produktai.

Rizikos vertinimas ir mažinimas. Labai didelės interneto platformos ir paieškos sistemos įpareigojamos užkirsti kelią piktnaudžiavimui jų paslaugomis bei atlikti nepriklausomą savo rizikos valdymo sistemų auditą. Taip pat turi būti užtikrinta, kad šios sistemos galėtų greitai ir veiksmingai reaguoti į visuomenės saugumui ar visuomenės sveikatai kylančias grėsmes. Be to, turi būti įdiegtos papildomos vaikų apsaugos priemonės ir nustatyti apribojimai neskelbtinų asmens duomenų naudojimui tikslinei reklamai.

Sustiprinama visų tarpininkavimo paslaugų teikėjų priežiūra. Kiekvienoje Europos Sąjungos valstybėje narėje svarbų vaidmenį atliks nepriklausomi skaitmeninių paslaugų koordinatoriai, o bendrą priežiūrą koordinuos Europos skaitmeninių paslaugų valdyba. Be to, Europos Komisija turi papildomus priežiūros įgaliojimus, skirtus labai didelėms interneto platformoms ir paieškos sistemoms, siekiant užtikrinti didesnį jų atsakomybės lygį ir skaidrumą.

Skaitmeninių paslaugų koordinatorius Lietuvoje - Lietuvos Respublikos ryšių reguliavimo tarnyba.

Lietuvoje SPA reikalavimų įgyvendinimo priežiūrą vykdo kompetentingos institucijos – Valstybinė vartotojų teisių apsaugos tarnyba, Valstybinė duomenų apsaugos inspekcija bei Žurnalistų etikos inspektoriaus tarnyba.

BAUDOS

Iki 6 % atitinkamo tarpininkavimo paslaugų teikėjo metinės pasaulinės apyvartos praėjusiais finansiniais metais – už SPA nustatytos pareigos nevykdymą.

Periodinės baudos suma gali būti iki 5 % atitinkamo tarpininkavimo paslaugų teikėjo vidutinės pasaulinės apyvartos per dieną ar pajamų per dieną praėjusiais finansiniais metais, apskaičiuojant nuo atitinkamame sprendime nurodytos datos.

1 % atitinkamo tarpininkavimo paslaugų teikėjo ar asmens metinių pajamų ar pasaulinės apyvartos praėjusiais finansiniais metais - už neteisingos, neišsamios ar klaidinančios informacijos pateikimą, atsakymo nepateikimą arba neteisingos, neišsamios ar klaidinančios informacijos neištaisymą ir nepateikimą patikrinimui.

TRINITI JUREX
TALLINN RIGA VILNIUS

Skaitmeninių rinkų aktas

Europos Parlamento ir Tarybos reglamentas (ES) 2022/1925 2022 m. rugsėjo 14 d. dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828

Pagrindinis Skaitmeninių rinkų akto (toliau – SRA) tikslas – prisidėti prie tinkamo vidaus rinkos veikimo nustatant suderintas taisykles, kuriomis visoms įmonėms visoje Europos Sąjungoje užtikrinamos atviros konkurencijai ir sąžiningos skaitmeninio sektoriaus rinkos, kuriose veikia prieigos valdytojai, veikiantys verslo klientų ir galutinių naudotojų naudai. SRA užtikrina naudotojams geresnes paslaugas ir sąžiningesnes kainas, kartu skatinant inovacijas bei sudarant palankesnes sąlygas technologijų startuoliams augti. Verslo naudotojai įgyja daugiau galimybių pasiekti vartotojus ir pasiūlyti platesnį pasirinkimą, o didžiosios platformos privalo laikytis griežtų reikalavimų, kad būtų užkirstas kelias nesąžiningai praktikai didelėse interneto platformose.

TAIKYMAS

SRA taikomas nuo 2023 m. gegužės 2 d.

SRA nustato taisykles prieigos valdytojams, t.y. pagrindines platformos paslaugas teikiančioms įmonėms, kurioms yra suteiktas prieigos valdytojo statusas. Prieigos valdytojo statusas suteikiamas, jeigu įmonė:

- Daro didelį poveikį vidaus rinkai. Laikoma, kad įmonė atitinka šį reikalavimą, jeigu jos pasiekta metinė apyvarta Europos Sąjungoje yra lygi arba ne mažesnė nei 7,5 mlrd. EUR kiekvienais iš pastarųjų trejų finansinių metų arba kai jos vidutinė rinkos kapitalizacija arba jos tikroji rinkos vertė yra bent 75 mlrd. EUR per paskutinius finansinius metus, ir ji teikia tą pačią pagrindinę platformos paslaugą bent trijose valstybėse narėse.

- Teikia pagrindinę platformos paslaugą, kuria naudodamiesi verslo klientai gali pasiekti galutinius naudotojus. Laikoma, kad įmonė atitinka šį reikalavimą, jeigu ji teikia pagrindinę platformos paslaugą, kuria praėjusiais finansiniais metais per mėnesį naudojosi ne mažiau nei 45 mln. aktyvių galutinių naudotojų, įsisteigusių ar esančių Europos Sąjungoje, ir kasmet naudojasi ne mažiau nei 10 000 aktyvių verslo klientų, įsisteigusių Europos Sąjungoje, identifikuotų ir apskaičiuotų naudojant SRA priede išdėstytą metodiką ir rodiklius.

- Užima įsitvirtinusios ir ilgalaikės rinkos dalyvės poziciją arba numatoma, kad tokią poziciją užims artimiausiu metu. Laikoma, kad įmonė atitinka šį reikalavimą, jeigu ne mažiau nei 45 mln. aktyvių galutinių naudotojų, įsisteigusių ar esančių Europos Sąjungoje, ir kasmet naudojasi ne mažiau nei 10 000 aktyvių verslo klientų, įsisteigusių Europos Sąjungoje, identifikuotų ir apskaičiuotų naudojant SRA priede išdėstytą metodiką ir rodiklius, riba buvo pasiekta kiekvienais iš praėjusių trejų finansinių metų.

Jeigu pagrindinės platformos paslaugas teikianti įmonė pasiekia visas nustatytas ribas, ji nedelsiant ir bet kuriuo atveju per 2 mėnesius nuo tada, kai pasiekiamos šios ribos, apie tai praneša Uropos Komisijai ir pateikia jai atitinkamą informaciją.

Pagrindinės platformos paslaugos yra bet kuri iš šių paslaugų:

- internetinės tarpininkavimo paslaugos;
- interneto paieškos sistema;
- internetinės socialinių tinklų paslaugos;
- dalijimosi vaizdo medžiaga platformos paslaugos;
- su numeriu nesiejamo asmenų tarpusavio ryšio paslaugos;
- operacinės sistemos;
- saityno naršyklės;
- virtualieji asistentai;
- debesijos kompiuterijos paslaugos;
- internetinės reklamos paslaugos, įskaitant reklamos tinklų, reklamos mainų ir visas kitas reklamos tarpininkavimo paslaugas, kurias teikia įmonė, teikianti bet kurią iš aukščiau išvardytų pagrindinių platformos paslaugų.

Kai didelė interneto bendrovė pripažįstama prieigos valdytoja, ji privalo pradėti laikytis SRA taisyklių per šešis mėnesius.

PAGRINDINIAI REIKALAVIMAI

Prieigos valdytojai privalo užtikrinti sąžiningesnę ir atviresnę skaitmeninę rinką, suteikdami verslo naudotojams daugiau teisių ir galimybių. Jie turi leisti trečiosioms šalims tam tikrais atvejais sąveikauti su jų paslaugomis. Verslo naudotojai turi gauti prieigą prie duomenų, kuriuos surinko naudodamiesi platforma, o taip pat gali laisvai reklamuoti savo produktus ir sudaryti sutartis su klientais už prieigos valdytojo platformos ribų. Be to, prieigos valdytojai privalo suteikti reklamą talpinančioms įmonėms priemones ir informaciją, leidžiančią nepriklausomai patikrinti savo skelbimus.

Prieigos valdytojams taikomi griežti draudimai, siekiant užtikrinti sąžiningą konkurenciją ir vartotojų teisių apsaugą. Jie negali palankiau vertinti savo pačių siūlomas paslaugas ir produktus nei panašius trečiųjų šalių pasiūlymus platformoje.

Taip pat draudžiama sekti naudotojus už pagrindinės prieigos valdytojų platformos ribų ir tvarkyti surinktus duomenis tikslinės reklamos tikslais be aiškaus sutikimo. Kūrėjams turi būti leidžiama naudoti trečiųjų šalių mokėjimo platformų programėles pardavimams. Be to, prieigos valdytojams yra draudžiama iš anksto įdiegti tam tikras programas arba neleisti naudotojams jų lengvai pašalinti.

Siekiant užtikrinti sklandų SRA įgyvendinimą, buvo priimti specialūs įgyvendinimo aktai (pvz., įgyvendinimo reglamentas (ES) 2023/814 ir du jo priedai), detalizuojantys prieigos valdytojų paskyrimo ir priežiūros procedūras.

SRA vykdymą prižiūri Europos Komisija, kuriai padeda patariamasis komitetas ir aukšto lygio grupė.

BAUDOS

Iki 10 % prieigos valdytojo bendros pasaulinės apyvartos praėjusiais finansiniais metais, jeigu Europos Komisija konstatuoja, kad prieigos valdytojas tyčia arba per aplaidumą nevykdo savo pareigų, priemonių ar kitų įsipareigojimų, kurie nustatyti kaip teisiškai privalomi pagal SRA.

Iki 20 % jo bendros pasaulinės apyvartos praėjusiais finansiniais metais, už tokį patį ar panašų SPA numatytos pareigos pažeidimą, susijusį su ta pačia pagrindine platformos paslauga, kaip praėjusių 8 metų laikotarpiu priimtame sprendime dėl reikalavimų nesilaikymo užfiksuotas jo padarytas pažeidimas.

Europos Komisija gali priimti įgyvendinimo aktą, kuriuo tokiam prieigos valdytojui nustatomos bet kokios elgesio ar struktūrinės taisomosios priemonės, kurios turi būti proporcingos ir būtinos tam, kad būtų užtikrintas veiksmingas SRA laikymasis, pavyzdžiui, uždrausti prieigos valdytojui ribotą laikotarpį vykdyti koncentraciją, kaip tai suprantama Reglamento (EB) Nr. 139/2004 3 straipsnyje.

Europos Komisija gali priimti sprendimą, kuriuo įmonėms, įskaitant, kai taikytina, prieigos valdytojus, ir įmonių asociacijoms būtų skirtos periodinės baudos periodiškai mokėti iki 5 % vidutinės dienos pasaulinės apyvartos praėjusiais finansiniais metais, skaičiuojamos nuo tame sprendime nurodytos dienos, kad juos priverstų vykdyti priemones ar laikytis kitų pareigų.

TRINITI JUREX
TALLINN RIGA VILNIUS

Dirbtinio intelekto aktas

2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828

Dirbtinio intelekto akto tikslas – sukurti suderintą teisinę sistemą, užtikrinančią, kad dirbtinio intelekto sistemos („DI sistemos“) būtų kuriamos ir naudojamos saugiai, etiškai ir nepažeidžiant pagrindinių teisių. Aktas siekia skatinti patikimą, į žmogų orientuoto dirbtinio intelekto kūrimą ir naudojimą Europos Sąjungos vidaus rinkoje, kartu užtikrinant aukštą saugumo, pagrindinių teisių apsaugą, palengvinti inovacijas. Dirbtinio intelekto aktas užtikrina, kad europiečiai galėtų pasitikėti dirbtinio intelekto teikiamomis galimybėmis.

TAIKYMAS

DI sistemų teikėjams (nepriklausomai nuo to, ar jie yra įsteigti ar įsikūrę Europos Sąjungoje, ar trečiojoje šalyje), jeigu jie teikia DI sistemas Europos Sąjungos rinkai.

DI sistemų naudotojams (turintiems įsisteigimo vietą arba įsikūrusiems Europos Sąjungoje).

Teikėjams ir naudotojams (turintiems savo įsisteigimo vietą arba įsikūrusiems trečiojoje šalyje), jeigu DI sistemos sukurtas rezultatas naudojamas Europos Sąjungoje.

DI sistemų importuotojams ir platintojams

Produktų gamintojams (pateikiantiems į Europos Sąjungos rinką arba pradedantiems naudoti DI sistemą kartu su savo produktu ir savo vardu arba po savo prekės ženklu)

Dirbtinio intelekto akto reikalavimai įsigalioja ir taikomi etapais.

Pagrindiniai etapai:

2025 m. vasario 2 d.:

- Įsigalioja draudžiamų praktikų draudimas (II skyrius).
- Pradedamos taikyti dirbtinio intelekto („DI“) raštingumo taisyklės (4 straipsnis).

2025 m. rugpjūčio 2 d.

- Įsigalioja nacionalinių institucijų paskyrimo nuostatos (III skyriaus 4 skirsnis).
- Pradedami taikyti reikalavimai bendrosios paskirties DI modeliams (V skyrius).
- Įsigalioja priežiūros nuostatos (ES ir nacionaliniu lygmeniu) (VII skyrius).
- Pradedamos taikyti konfidencialumo ir sankcijų taisyklės (išskyrus susijusias su bendrosios paskirties DI modeliais) (XII skyrius).

2026 m. rugpjūčio 2 d.

- Pradedamos taikyti visos kitos DI akto nuostatos (nebent pačiame akte nurodytos vėlesnės datos).

PAGRINDINIAI REIKALAVIMAI

Rizikos klasifikavimas ir atitikties užtikrinimas – DI sistemos skirstomos į rizikos kategorijas (žemos, ribotos, didelės ir nepriimtinos rizikos), kiekvienai jų taikomi skirtingi reikalavimai.

Nepriimtinos rizikos DI sistemas draudžiama tiekti į ES rinką ir jas naudoti. Visos DI sistemos, kurios kelia aiškią grėsmę žmonių saugumui ir teisėms, yra uždraustos nuo 2025 m. vasario 2 d. Dirbtinio intelekto aktas draudžia šias praktikas:

- Manipuliatyvias arba apgaulingas DI praktikas;
- Išnaudojančias asmenų pažeidžiamumą;
- Socialinį reitingavimą;
- Rizikos vertinimą polinkio nusikalsti prognozėms;
- Veido atvaizdų betikslis rinkimą ir duomenų bazių kūrimą;
- Emocijų atpažinimą darbo vietoje ir švietimo įstaigose;
- Biometrinę kategorizaciją;
- Realaus laiko biometrinę identifikaciją, vykdomą teisėsaugos tikslais.

Detaliau su draudimais galite susipažinti mūsų straipsnyje

Draudžiamos dirbtinio intelekto praktikos

Reikalavimai didelės rizikos DI sistemų teikėjams ir naudotojams – keliami aukšti reikalavimai šių sistemų teikėjams ir naudotojams.

Pavyzdžiui, didelės rizikos DI sistemos teikėjas privalo:

- Sukurti rizikos valdymo sistemą;
- Užtikrinti tinkamą duomenų valdymą;
- Parengti techninę dokumentaciją;
- Parengti instrukcijas naudotojams;
- Užtikrinti, kad DI sistema būtų pateikta atitinkamai atitikties vertinimo procedūrai;
- Parengti ES atitikties deklaraciją;
- Laikytis ES duomenų bazės registracijos reikalavimų;
- Ir t.t.

Skaidrumas ir informavimas – didelės rizikos DI sistemų teikėjai turi pateikti informaciją apie šių sistemų veikimą šių sistemų naudotojams. Taip pat DI sistemų, kurios tiesiogiai sąveikauja su žmonėmis, teikėjai turi užtikrinti, kad asmenys suprastų, kad jie sąveikauja su DI, o ne su kitu žmogumi.

Žmonių kontrolė – Dirbtinio intelekto akte numatytas reikalavimas didelės rizikos DI sistemų teikėjams kurti didelės rizikos DI sistemas taip, kad žmonės galėtų išlaikyti tam tikrą kontrolę ir intervencijos galimybes, ypač kai kyla pavojus pagrindinėms teisėms.

Raštingumas – DI sistemų teikėjai ir naudotojai privalo užtikrinti, kad visi, kurie tvarko ir naudoja DI sistemas jų vardu, turėtų pakankamą dirbtinio intelekto raštingumo lygį.

Stebėsena ir auditas – institucijos turi teisę atlikti DI sistemų patikras, kad užtikrintų teisės aktų laikymąsi ir surinktų atitikties įrodymus.

BAUDOS

1. 35 mln. eurų arba iki 7 % bendros metinės pasaulinės apyvartos už praėjusius finansinius metus, priklausomai nuo to, kuri suma yra didesnė, jei pažeidžiami reikalavimai dėl nepriimtinos rizikos DI sistemų neteikimo į ES rinką ir nenaudojimo.

2. 15 mln. eurų arba iki 3% bendros metinės pasaulinės apyvartos už praėjusius finansinius metus, priklausomai nuo to, kuri suma yra didesnė, jei pažeidžiami pagrindiniai įsipareigojimai, susiję su didelės rizikos DI sistemų reikalavimais.

3. 7.5 mln. eurų arba iki 1% bendros metinės pasaulinės apyvartos už praėjusius finansinius metus, priklausomai nuo to, kuri suma yra didesnė, už neteisingos, neišsamios ar klaidinančios informacijos teikimą notifikuotosioms įstaigoms arba nacionalinėms kompetentingoms institucijoms.

TRINITI JUREX
TALLINN RIGA VILNIUS

III DALIS.
Prieinamumo reglamentavimas

Šioje dalyje bus aptarta Prieinamumo direktyvos perkėlimas į Lietuvos teisinę sistemą.

2019 m. balandžio 17 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/882 dėl gaminių ir paslaugų prieinamumo reikalavimų.

Pagrindinis Prieinamumo direktyvos tikslas - gerinti prieigą prie pagrindinių gaminių ir paslaugų asmenims su negalia ir kitiems funkcinių sutrikimų turintiems asmenims, įskaitant ir vyresnio amžiaus asmenis.

TAIKYMAS

Prieinamumo direktyvos reikalavimai perkelti į Lietuvos Respublikos gaminių ir paslaugų prieinamumo reikalavimų įstatymą.

Įstatymo reikalavimai taikomi visoms įmonėms, išskyrus tik labai mažas įmones, kurios teikia paslaugas.

Įmonės gali taikyti neproporcingos naštos institutą, kuris reiškia, kad prieinamumo reikalavimai taikomi tik tokia apimtimi, kad dėl šių reikalavimų laikymosi: i) nereikėtų daryti esminio gaminio ar paslaugos pagrindinio pobūdžio pakeitimo arba ii) nebūtų sukelta neproporcinga našta atitinkamiems ekonominės veiklos vykdytojams. Įmonės privalo dokumentuoti neproporcingos naštos vertinimą. Tokią ataskaitą jos turi saugoti 5 metus po to, kai gaminys rinkai buvo paskutinį kartą patiektas, arba po to, kai paslauga buvo suteikta paskutinį kartą.

Išimtis dėl neproporcingos naštos vertinimo ataskaitos rengimo taikoma tik gamyba užsiimančioms labai mažoms įmonėms, t. y., jos neturi rengti neproporcingos naštos vertinimo ataskaitos, jeigu gamyba užsiimanti labai maža įmonė nusprendžia nesilaikyti vieno ar kelių prieinamumo reikalavimų, tačiau priežiūros institucija turi teisę paprašyti pateikti faktus, susijusius su neproporcingos naštos vertinimu.

Labai maža įmonė – įmonė, kurioje dirba mažiau kaip 10 darbuotojų ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų:

1) įmonės metinės pajamos neviršija 2 mln. eurų;
2) įmonės balanse nurodyto turto vertė neviršija 2 mln. eurų.

Įstatymas įsigalios 2025 m. birželio 28 d.

PAGRINDINIAI REIKALAVIMAI

Pateikiama informacija ar paslaugos prieinamos visiems asmenims. Tai reiškia, kad informacija turi būti pateikta taip, kad ją būtų galima suvokti ir naudoti naudojant įvairius formatų ir pojūčių derinius (pvz., garsinę, vizualinę, tekstinę informaciją). Prieinamumas taip pat apima atitinkamus techninius ir dizaino sprendimus, užtikrinančius, kad informacija būtų aiškiai suprantama, tinkamai pateikta skirtingais būdais, ir užtikrintų, kad naudotojai galėtų ją pasiekti nepaisant jų fizinių ar technologinių galimybių.

Informacija būtų lengvai suvokiama visiems žmonėms, nepriklausomai nuo jų individualių galimybių, ir tam tikslui naudojami universalūs dizaino principai ir techninės priemonės.

Jeigu paslaugų teikimo metu naudojami gaminiai, tai tiems gaminiams taip pat taikomi šie reikalavimai.

Pavyzdžiui, instrukcijos gali būti skelbiamos interneto svetainėje ir turi atitikti tokius reikalavimus: turi būti pateikiamos daugiau nei viena jusle atpažįstamu, suprantamu, suvokiamu būdu, tinkamo šrifto dydžio ir tipo, užtikrinant pakankamą kontrastą bei tarpus, galinčios būti transformuojamos į alternatyvius formatus, o netekstinis turinys turi būti pateikiamas su alternatyviu aprašymu.

BAUDOS

Ekonominės veiklos vykdytojui (gamintojui, įgaliotajam atstovui (jei gamintojas įsisteigęs ne Europos Sąjungoje), importuotojui, platintojui ar paslaugų teikėjui) už įstatymo pažeidimus:

1. Nuo 500 iki 2 500 eurų - pateikusiam ar tiekiančiam rinkai prieinamumo reikalavimų neatitinkantį gaminį, suteikusiam ar teikiančiam prieinamumo reikalavimų neatitinkančią paslaugą.

2. Nuo 1 000 iki 6 000 eurų - nepaisančiam priežiūros institucijos draudimo ar ribojimo pateikti ir tiekti rinkai prieinamumo reikalavimų neatitinkančius gaminius.

3. Nuo 2 500 iki 15 000 eurų - jeigu prieinamumo reikalavimų neatitinkantys gaminiai ar paslaugos yra padarę žalos vartotojo sveikatai.

Autoriai

Aurelija Rutkauskaitė

Partnerė, advokatė,
IT, duomenų apsaugos ir privatumo komandos vadovė
aurelija.rutkauskaite@triniti jurex.lt

Greta Bujutė

Vyr. teisininkė

Jolita Supranavičiūtė

Teisininkė

Deivydas Nikartas

Teisininkas

TRINITI JUREX
TALLINN RIGA VILNIUS

Pasiūlymas!

Labas!

Ar žinai, kad savo prekių ženklą ar dizainą gali registruoti pigiau, nes iki 75% žyminio mokesčio kompensuos ES paramos fondas?

Mes parengsime paraišką paramai gauti ir padėsime su registracija Lietuvoje, ES ar kitoje valstybėje.

Susidomėjai – susisiek!

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE