Domenų industriją įtakojančių teisės aktų pokyčiai

Laura Subačienė| Interneto paslaugų centras / DOMREG
Kauno technologijos universitetas

2024-12-03

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555
2022 m. gruodžio 14 d. dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148

TIS 2 direktyva

(https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32022L2555)

2024 m. spalio 18 d. atnaujintas Kibernetinio saugumo įstatymas

(https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr?positionInSearchResults=0&searchModelUUID=aa20dd5b-faff-427e-a55c-464a37633a72)

DOM REG [.lt]

2024 m. spalio 17 d.

Komisijos įgyvendinimo reglamentas (ES) 2024/2690,

kuriuo nustatomos Direktyvos (ES) 2022/2555 taikymo taisyklės, susijusios su kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais ir išsamesniu atvejų, kuriais incidentas laikomas dideliu, apibūdinimu, skirtais DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams

https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32024R2690

2024 m. lapkričio 6 d.

Vyriausybės nutarimas “Dėl Kibernetinio saugumo įstatymo įgyvendinimo”

(https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/22f960219fff11ef9db2c9aaf9c67042?positionInSearchResults=6&searchModelUUID=aa20dd5b-faff-427e-a55c-464a37633a72)

- **Nacionalinis kibernetinių incidentų valdymo planas;**
- **Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodika;**
- **Kibernetinio saugumo reikalavimų aprašas.**

DOM REG [.lt]

Aktualios sąvokos

Aukščiausio lygio domenų vardų registravimo paslaugas teikiantis subjektas – subjektas, atsakingas už aukščiausio lygio domeno administravimą, apimantį domenų vardų registraciją tame domene ir techninį jo veikimą, įskaitant vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp domenų vardų serverių, neatsižvelgiant į tai, ar visas tas operacijas atlieka pats subjektas, ar dalis jų yra užsakomosios paslaugos. Subjektas nėra laikomas aukščiausio lygio domenų vardų registravimo paslaugas teikiančiu subjektu, jeigu aukščiausio lygio domenų vardus naudoja tik savo reikmėms.

Domenų vardų registravimo paslaugas teikiantis subjektas – subjektas arba jo vardu veikiantis subjektas, teikiantys domenų vardų registravimo paslaugas, įskaitant privatumo ar įgaliotojo tarpininkavimo registravimo paslaugų teikėją arba perpardavėją.

Domenų vardų sistema – sistema, kurioje hierarchiškai suskirstyti domenų vardai, kurioje galima identifikuoti interneto paslaugas ir išteklius ir kurioje sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis siekiant gauti išteklius.

Domenų vardų sistemos paslaugų teikėjas – subjektas, kuris teikia viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba patikimas domenų vardų keitimo paslaugas trečiosioms šalims, išskyrus šakninių domenų vardų serverių paslaugas.

DOM REG [.lt]

Kitos sąvokos

Duomenų centro paslauga – duomenų centro teikiama paslauga, kuri apima informacinių technologijų ir tinklo įrangos centralizuotą pritaikymą, eksploatavimą ir tarpusavio junglumo palaikymą, duomenų saugojimo, tvarkymo ir perdavimo paslaugų teikimą ir visos energijos paskirstymo ir aplinkos kontrolės įrangos ir infrastruktūros užtikrinimą.

Elektroninės informacijos prieglobos paslaugos – paslaugos, kurios sudaro paslaugos gavėjo pateiktos elektroninės informacijos saugojimą jo prašymu.

Interneto duomenų srautų mainų taškas – tinklo įrenginys, per kurį siekiant palengvinti interneto duomenų srautų mainus, sujungiamos daugiau nei dvi atskiros autonominės sistemos. Interneto duomenų srautų mainų taškas sujungia tik autonomines sistemas, jį naudojant nebūtina, kad interneto duomenų srautai, kuriais keičiasi autonominių sistemų pora, būtų perduodami per trečią autonominę sistemą, be to, jis nekeičia ir netrikdo tokių srautų.

DOM REG [.lt]

NKSC informuoja subjektą apie jo priskyrimą preliminariam kibernetinio saugumo subjektų sąrašui

Subjektas per dešimt darbo dienų nuo pranešimo gavimo dienos patvirtina pateiktų duomenų teisingumą

Iki 2025 m. balandžio 17 d.

Kibernetinio saugumo subjektai įtraukiami į esminių ir svarbių subjektų sąrašą ir Kibernetinio saugumo subjektų Registrą

Iki 2026 m. balandžio 17 d.

Kibernetinio saugumo subjektai privalo atitikti organizacinius reikalavimus

Iki 2027 m. balandžio 17 d.

Kibernetinio saugumo subjektai privalo atitikti techninius reikalavimus

Kas 3 metai

Savarankiškai atliekamas auditas

DOM REG [.lt]

Kibernetinio saugumo subjektų registre kaupiami duomenys apie kibernetinio saugumo subjektus:

- kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinė forma, ekonominės veiklos sritis (sritys) ir rūšis (rūšys), pagrindinės buveinės adresas;
- kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);
- teikiamos paslaugos ir (ar) vykdomos veiklos, atitinkančios nurodytus kriterijus;
- naudojami interneto protokolo (IP) adresai;
- valstybės, kuriose kibernetinio saugumo subjektas teikia paslaugas ir (ar) vykdo veiklą;
- paslaugų teikimui ar veiklai reikšmingos tinklų ir informacinės sistemos.

Galimybė pasitikrinti apie savo organizacijos patekimo į Registrą tikimybę NKSC interneto svetainėje adresu:
https://www.nksc.lt/kssregistras/

Kibernetinio saugumo subjektai

ESMINIAI

SVARBŪS

! KS subjektai įgyja pareigas, nustatytas KS subjektams, tik nuo jų įregistravimo Kibernetinio saugumo informacinėje sistemoje.

DOM REG .lt

Esminiai KS subjektai

Subjektai, teikiantys **aukščiausio lygio domeno vardų registravimo paslaugas**

Subjektai, teikiantys **domenų vardų sistemos (toliau – DNS) paslaugas**, išskyrus šakninių vardų serverių operatorius

Svarbūs KS subjektai

Subjektai, teikiantys **domenų vardų registravimo paslaugas**

! Jeigu subjektas atitinka bent vieną kriterijų, pagal kurį identifikuojamas esminis subjektas, laikoma, kad subjektas yra esminis subjektas nepriklausomai nuo jo atitikties svarbaus subjekto kriterijams.

DOM REG [.lt]

Kibernetinio saugumo reikalavimai

1) kibernetinio saugumo rizikos analizės, tinklų ir informacinių sistemų kibernetinio saugumo politiką;

2) už kibernetinį saugumą atsakingų asmenų ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas;

3) kibernetinių incidentų valdymą;

4) veiklos tęstinumą;

5) tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;

6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą;

7) politiką ir procedūras, skirtas kibernetinio saugumo reikalavimų veiksmingumui įvertinti;

8) kibernetinės higienos praktiką ir reguliarius kibernetinio saugumo mokymus;

9) kriptografijos ir šifravimo naudojimo politiką ir procedūras;

10) žmogiškųjų išteklių saugumą, prieigos prie tinklų ir informacinių sistemų kontrolės politiką ir turto valdymą;

11) kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą;

12) kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų naudotojų, administratorių, kibernetinio saugumo subjektų tiekėjų, jų subtiekėjų ir kitų ūkio subjektų teisių ir prieigos prie kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų ir (ar) skaitmeninių duomenų suteikimo ir valdymo politiką;

13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus kibernetinio saugumo reikalavimus, nustatytus atsižvelgiant į identifikuotas atskirų sektorių kibernetinio saugumo rizikas.

DOM REG [.lt]

Kibernetinio saugumo reikalavimai

Kibernetinio saugumo subjekto vadovas privalo paskirti **kibernetinio saugumo vadovą** ir **saugos įgaliotinį**.

Kibernetinio saugumo subjektui **leidžiama iš tiekėjo įsigyti paslaugas**, kurių metu būtų vykdomos už kibernetinį saugumą atsakingų asmenų funkcijos.

Šie reikalavimai netaikomi, jei kibernetinio saugumo subjektas yra **fizinis asmuo**.

Kibernetinio saugumo **subjekto valdymo organų nariai, vadovas** privalo ne rečiau kaip **kartą per 2 metus išklausyti kibernetinio saugumo mokymus** ir **užtikrinti kibernetinio saugumo subjekto darbuotojų nuolatinį švietimą kibernetinio saugumo srityje**.

Kibernetinio saugumo **subjektai ne rečiau kaip kartą per 3 metus atlieka kibernetinio saugumo auditą** pagal NKSC patvirtintą metodiką.

Kibernetinio saugumo subjektai privalo užtikrinti **tiekimo grandinės saugumą**.
Kibernetinio saugumo subjektai **privalės reikalauti ir įsitikinti**, jog tiekėjai atitinka kibernetinio saugumo reikalavimus, pavyzdžiui, turi incidentų valdymo planus, atitinkamus saugumo sertifikatus, įvykus kibernetiniam incidentui bendradarbiaus su kibernetinio saugumo subjektu ir pan.

DOM REG [.lt]

Reikalavimai domenų paslaugų teikimui

ALD vardų registro paslaugas teikiantys subjektai ir domenų vardų registravimo paslaugas teikiantys subjektai, **privalo**:

Kaupti informaciją, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius asmenis:

a) domeno vardą;

b) domeno registracijos datą;

c) domeno vardo turėtojo juridinio asmens pavadinimą ar fizinio asmens vardą ir pavardę, kontaktinius duomenis (elektroninio pašto adresas, ryšio numeris);

d) domeno vardą administruojančio kontaktinio asmens elektroninio pašto adresą ir ryšio numerį, jei jie skiriasi nuo domeno vardo turėtojo duomenų;

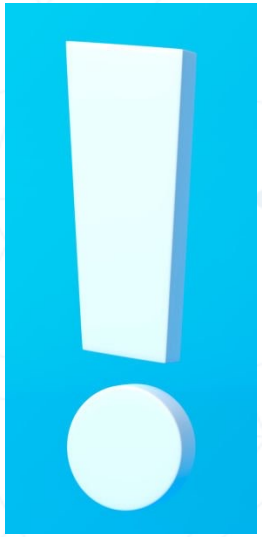
DOM REG [.lt]

Reikalavimai domenų paslaugų teikimui

ALD vardų registro paslaugas teikiantys subjektai ir domenų vardų registravimo paslaugas teikiantys subjektai, **privalo**:

- taikyti politiką ir procedūras, įskaitant tikrinimo procedūras, kuriomis užtikrinama, kad domenų vardų registracijos duomenų bazėje būtų **pateikiama tiksli ir išsami informacija**;
- **skelbti** šią politiką ir procedūras **viešai savo interneto svetainėse** ar, jeigu jos neturi, kitomis visuomenės informavimo priemonėmis;
- ne vėliau kaip **per 72 valandas po domeno vardo užregistravimo** momento **paskelbti viešai savo interneto svetainėse** ar, jeigu jos neturi, kitomis visuomenės informavimo priemonėmis **domeno vardo registracijos duomenis**, kurie nėra asmens duomenys;
- **gavę teisėtus ir pagrįstus teisėtos prieigos** prie domenų vardų registracijos duomenų, kurie yra asmens duomenys, prašančių subjektų **prašymus**, pagal taikomą duomenų atskleidimo politiką ir procedūras **suteikti prieigą prie konkrečių domenų vardų registracijos duomenų**. Atsakymai prašančiam subjektui pateikiami ne vėliau kaip per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą;
- siekdami **nedubliuoti domenų vardų registracijos duomenų rinkimo**, bendradarbiauti tarpusavyje.

DOM REG [.lt]



Iš kibernetinio saugumo subjektų grupės išskiriama **specialiųjų subjektų** grupė:

- **DNS paslaugų teikėjai;**
- **aukščiausio lygio domenų vardų registravimo paslaugas teikiantys subjektai;**

- debesijos paslaugų teikėjai;
- duomenų centrų paslaugų teikėjai;
- paskirstytojo turinio teikimo tinklo paslaugų teikėjai;
- valdomų paslaugų teikėjai;
- valdomų kibernetinio saugumo paslaugų teikėjai;
- elektroninės prekyvietės paslaugų teikėjai;
- interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjai.

DOM REG [.lt]

Specialusis subjektas nuo patekimo į **KS subjektų registrą momento**, privalės **užtikrinti** savo naudojamų tinklų ir informacinių sistemų atitiktį **tik Europos Komisijos įgyvendinimo reglamente (ES) 2024/2690** nurodytoms **kibernetinio saugumo rizikos valdymo priemonėms.**

Reglamentas (ES) 2024/2690 nenustato pereinamojo laikotarpio terminų

Reikalavimai kibernetinio saugumo rizikos valdymo priemonėms **bus privalomi** nuo specialiojo subjekto patekimo į Kibernetinio saugumo subjektų registrą momento (t.y. nuo **2025-04-17**).

DOM REG [.lt]

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) rengia Reglamento (ES) 2024/2690, **įgyvendinimo gaires**.

Šiose gairėse bus siekiama pateikti:

- papildomus patarimus ir rekomendacijas, į ką atsižvelgti įgyvendinant vieną ar kitą reikalavimą, ir išsamesnius paaiškinimus apie teisės akto tekste vartojamas sąvokas ir terminus;
- įrodymų, kuriais remiantis galima bus įvertinti, ar reikalavimas įvykdytas, pavyzdžius;
- lenteles, kuriose Europos Komisijos įgyvendinimo reglamente nustatyti reikalavimai bus susieti su Europos ir tarptautiniais standartais bei nacionaliniais teisės aktais.

Tam tikrus Reglamente nustatytus techninius ir metodinius reikalavimus atitinkami subjektai turėtų taikyti, **kai tikslinga**, **kai taikytina** ir **tiek, kiek įmanoma**.

Tais atvejais, kai atitinkamas subjektas mano, kad taikyti tam tikrus nustatytus techninius ir metodinius reikalavimus jo atveju nėra tikslinga, taikytina ar įmanoma, jis turėtų dokumentuose **suprantamai užfiksuoti** su tuo susijusius savo argumentus.

Vykdydamos priežiūrą, nacionalinės kompetentingos institucijos **gali atsižvelgti** į tai, kiek laiko atitinkamiems subjektams reikia kibernetinio saugumo rizikos valdymo priemonių techniniams ir metodiniams reikalavimams įgyvendinti.

DOM REG [.lt]

Kibernetinių incidentų valdymas

- **Pareiga esminiams ir svarbiems** subjektams **pranešti NKSC** ne tik apie **didelį kibernetinį incidentą**, bet ir **apie kitus** kibernetinius incidentus.
- Informaciją apie kibernetinius incidentus subjektai NKSC galės pranešti **įprastais būdais** (el. paštu, internetinėje NKSC svetainėje, telefonu).
- NKSC jau pradėjo kurti naują centralizuotą **Nacionalinę kibernetinių incidentų valdymo platformą**, kuri palengvins ir automatizuos informacijos pateikimą, o ateityje taps pagrindiniu informacijos apie kibernetinius incidentus pateikimo kanalu.

Vadovaujantis „vieno langelio“ principu, organizacijos galės pateikti informaciją apie incidentą, o platformoje šią informaciją galės pamatyti ir efektyviai koordinuoti NKSC, Lietuvos policija, Valstybinė duomenų apsaugos inspekcija, kitos kompetentingos institucijos, kibernetinio saugumo subjektų saugumo operacijų centrai.

Duomenys apie kibernetinius incidentus, reikalingi institucijų tyrimams atlikti, išskyrus ikiteisminio tyrimo duomenis, bus teikiami ir tvarkomi Platformoje.

DOM REG [.lt]

Didelis kibernetinis incidentas

(pagal KSĮ)

Kibernetinis **incidentas laikomas dideliu** bent vienu iš šių atvejų:

1) jeigu dėl kibernetinio incidento atitinkamas **subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų;**

2) jeigu dėl kibernetinio incidento atitinkamas **subjektas patyrė arba gali patirti didelių finansinių nuostolių**;

3) jeigu kibernetinis incidentas **paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą**.

DOM REG [.lt]

Didelis kibernetinis incidentas

(pagal KSĮ)

1. Jeigu dėl kibernetinio incidento atitinkamas **subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų (ir yra bent vienas iš šių kriterijų):**

- paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje Europos Sąjungos arba NATO šalyje;
- tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;
- paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);
- paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys;
- kibernetinio saugumo subjektas nebegali užtikrinti teisės aktuose jo veiklai nustatytų reikalavimų įgyvendinimo;
- prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija;
- per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas.

2. Jeigu dėl kibernetinio incidento atitinkamas **subjektas patyrė arba gali patirti didelių finansinių nuostolių**;

- kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur,
- arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

3. Jeigu kibernetinis incidentas **paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą** :

- galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;
- galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur;
- sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.

DOM REG .lt

Europos Komisijos įgyvendinimo Reglamente (ES) 2024/2690 taip pat apibrėžti išsamesni atvejai, kuriais remiantis kibernetinis incidentas laikomas dideliu, todėl specialusis subjektas, pranešdamas apie incidentus, **turi laikytis tiek nacionalinių teisės aktų**, tiek **Reglamento (ES) 2024/2690 reikalavimų**.

Didelis kibernetinis incidentas

(pagal Reglamentą 2024/2690)

Kibernetinis **incidentas laikomas dideliu** bent vienu iš šių atvejų:

a) finansiniai praradimai > 500 000 EUR arba > 5% atitinkamo subjekto metinės apyvartos;

b) incidentas sukėlė arba gali sukelti komercinių paslapčių atskleidimą;

c) incidentas sukėlė arba gali sukelti fizinio asmens mirtį;

d) įvykis padarė arba gali padaryti **didelę žalą fizinio asmens sveikatai**;

e) prie tinklų ir informacinių sistemų **įgyta piktavališka ir neteisėta prieiga, kuria naudojantis galima smarkiai sutrikdyti veiklą;**

f) **jei per šešis mėnesius įvyko bent dukart**, juos sieja ta pati pagrindinė priežastis ir sudėti kartu jie atitinka a punkte nustatytą kriterijų;

g) **ARBA incidentas atitinka vieną ar daugiau iš nustatytų kriterijų:**

DOM REG [.lt]

Su **ALD vardų registrais** susiję dideli incidentai:

- patikimo domenų vardų keitimo **paslauga** yra visiškai **neprieinama**;
- patikimo domenų vardų keitimo paslaugos **atsako į DNS užklausas** vidutinė trukmė ilgiau nei vieną valandą **viršija 10 sekundžių**;
- **pažeistas** su aukščiausio lygio domeno techniniu veikimu susijusių **saugomų, perduodamų ar tvarkomų duomenų vientisumas, konfidencialumas ar autentiškumas**.

Su DNS paslaugų teikėjais susiję dideli incidentai:

- rekursinio arba patikimo domenų vardų keitimo **paslauga** yra visiškai **neprieinama ilgiau kaip 30 minučių;**
- rekursinio arba patikimo domenų vardų keitimo paslaugos **atsako į DNS užklausas** vidutinė trukmė ilgiau nei vieną valandą **viršija 10 sekundžių**;
- **pažeistas** su patikimo domenų vardų keitimo paslaugos teikimu susijusių **saugomų, perduodamų ar tvarkomų duomenų vientisumas, konfidencialumas ar autentiškumas**, išskyrus atvejus, kai dėl netinkamos konfigūracijos neteisingi yra mažiau kaip 1 000 DNS paslaugų teikėjo administruojamų domenų vardų, sudarančių ne daugiau kaip 1 % DNS paslaugų teikėjo administruojamų domenų vardų, duomenys.

DOM REG [.lt]

Pranešimas apie didelį kibernetinį incidentą

Nedelsiant, bet **ne vėliau kaip per 24 valandas** nuo sužinojimo apie didelį kibernetinį incidentą	→	**Ankstyvasis perspėjimas**
Nedelsiant, bet **ne vėliau kaip per 72 valandas** nuo sužinojimo apie didelį kibernetinį incidentą	→	**Pranešimas apie kibernetinį incidentą, pradinis vertinimas, įsilaužimo įrodymų nurodymas**
Per NKSC **nurodytą terminą** pateikimo	→	**Tarpinė atitinkamų atnaujintų padėties duomenų ataskaita**
Ne vėliau kaip **per vieną mėnesį** nuo pranešimo apie kibernetinį incidentą	→	**Pažangos** *arba* **Galutinė ataskaita**

DOM REG [.lt]

Kibernetinių incidentų valdymo organizavimas

Kibernetinių incidentų valdymo organizavimą kibernetinio saugumo subjekto lygmeniu **užtikrina kibernetinio saugumo subjektas.**

Kibernetinių incidentų valdymas organizuojamas pagal kibernetinio saugumo subjekto patvirtintą **kibernetinių incidentų valdymo planą.**

Kibernetinių incidentų valdymo organizavimo funkcijas kibernetinio saugumo vadovas paskiria **Saugumo operacijų centrui – SOC.**

SOC funkcijos **negali būti pavestos** kibernetinio saugumo subjekto arba paslaugų teikėjo darbuotojui, atsakingam už tinkamą to kibernetinio saugumo subjekto tinklų ir (ar) informacinių sistemų veiklą.

DOM REG [.lt]

Kibernetinio saugumo subjektų pažeidimai

NKSC atlieka kibernetinio saugumo subjektų **atitikties Kibernetinio saugumo įstatymo reikalavimams, patikrinimus.**

Pažeidimai skirstomi į:

- **pavojingus,**
- **vidutinio pavojingumo,**
- **nedidelio pavojingumo.**

NKSC gali skirti **baudas** kibernetinio saugumo subjektams, kurių dydis skiriasi:

Esminiams subjektams
nustatoma bauda iki **10 000 000 Eur** arba iki **2 proc.** juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri yra didesnė

Svarbiems subjektams
nustatoma bauda iki **7 000 000 Eur** arba iki **1,4 proc.** juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri yra didesnė

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

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

Juridinių asmenų vadovams
ar kitiems atsakingiems asmenims nustatoma bauda už Kibernetinio saugumo įstatyme nustatytų reikalavimų pažeidimą nuo **250** iki **3000 Eur**, o nusižengimas, padarytas pakartotinai, užtraukia baudą nuo **2000** iki **6000 Eur**

DOM REG .lt

Ačiū!

DOM REG .lt