TEISĖ IR KIBERNETINĖ SAUGA:

KAIP RASTI BENDRĄ VARDIKLĮ IR NEPASIKLYSTI REIKALAVIMŲ GAUSOJE?

MIGLĖ PETKEVIČIENĖ

2024 m. spalio 16 d.

BLOGA ŽINIA:
DIDĖJANTI REGULIACINĖ NAŠTA

Ellex

SVARBIAUSI TEISĖS AKTAI

BDAR

Taikomas JA ir FA, kurie versdamiesi profesine / ūkine veikla, renka, saugo ar kitaip tvarko asmens duomenis

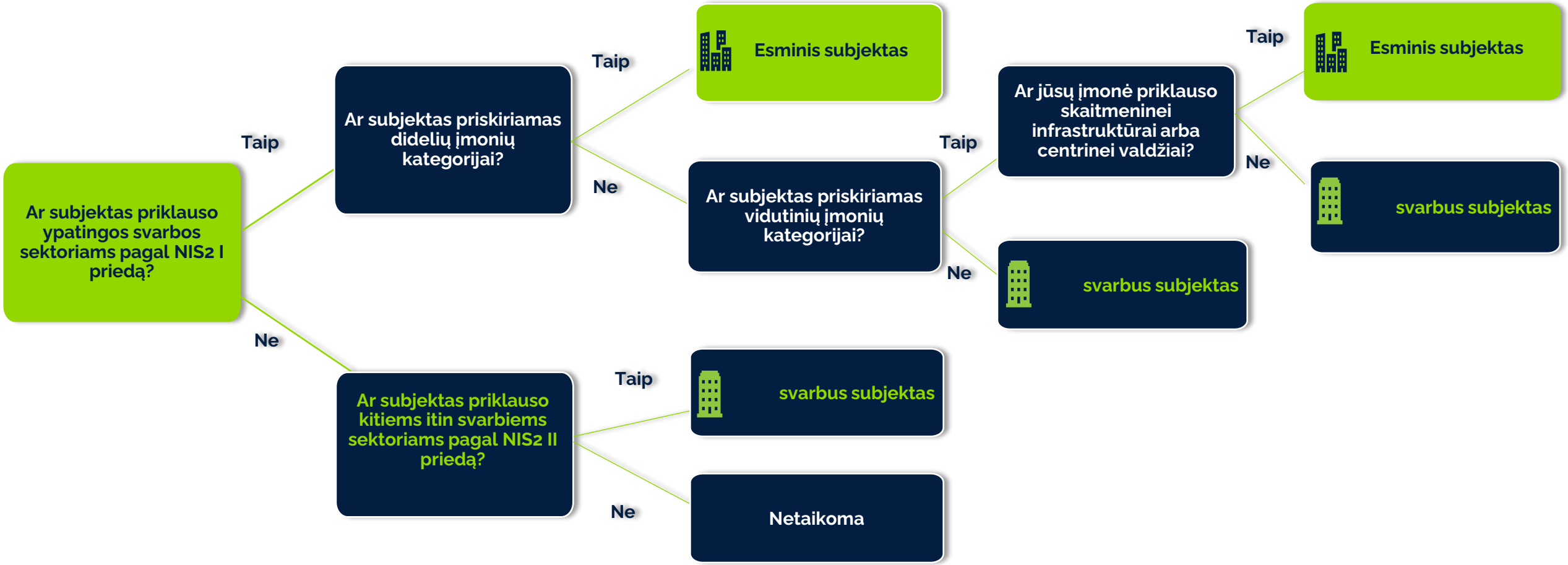
NIS2

Taikomas esminiams ir svarbiems subjektams kaip tai suprantama pagal kibernetinio saugumo įstatymą

DORA

Taikomas finansų sektoriuje veikiantiems subjektams. DORA turi taikymo pirmenybę prieš NIS2 finansų sektoriuje

ESMINIŲ IR SVARBIŲ SUBJEKTŲ ATPAŽINIMAS



Keletas I priede nurodytų ypatingos svarbos sektoriai:

Energija Transportas Bankininkystė Finansų rinkos infrastruktūros objektai Sveikatos priežiūra IRT paslaugų valdymas; Viešasis administravimas

Keletas II priede nurodytų itin svarbių sektorių:

Pašto ir kurjerių paslaugos Atliekų tvarkymas Cheminių medžiagų gamyba ir platinimas Maisto gamyba, perdirbimas ir platinimas Gamyba Skaitmeninių paslaugų teikėjai

Ellex

NIS2:

ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

Ellex

ORGANIZACIJA =
ŽMOGAUS KŪNAS

Ellex

KELIAS Į ATITIKTĮ:
SPRAGŲ NUSTATYMAS IR JŲ UŽPILDYMAS

Ellex

GERA ŽINIA: NIS2.LEGAL

KAS YRA NIS2?

Šis įrankis buvo sukurtas siekiant padėti Lietuvoje veikiančioms organizacijoms pačioms įsivertinti savo atitikties TIS2 direktyvos (angl. NIS2) lygį bei didinti organizacijų kibernetinio saugumo brandą. Klausimyno pildymo metu visas progresas ir rezultatai saugomi tik naudotojo kompiuteryje. Šis įrankis turi du pasirinkimus – Bazinį klausimyną (rekomenduojama pildyti vadovams bei CISO) ir Išplėstinį klausimyną (rekomenduojame pildyti kartu su IT ir kibernetinio saugumo specialistais). Klausimyno pabaigoje galėsite atlikti rezultatų eksportavimą į .pdf dokumentą ir, jei pageidaujate, pasidalinti rezultatais su įrankio kūrėjais „Ellex Valiūnas“ ir „Santa Monica Networks“, kad galėtume padėti įgyvendinti minėtus reikalavimus. Konfidencialumą garantuojame.

PAGRINDINIAI PATARIMAI

- **Nuolatinis imuniteto stiprinimas:**
  - Vitaminai, gerosios bakterijos, grūdinimasis

  Kitaip tariant:
  - Tinkamas pasirengimas, įsilaužimų testavimas, nuolatinė dokumentų, tvarkų ir turimų įrankių peržiūra ir atnaujinimas

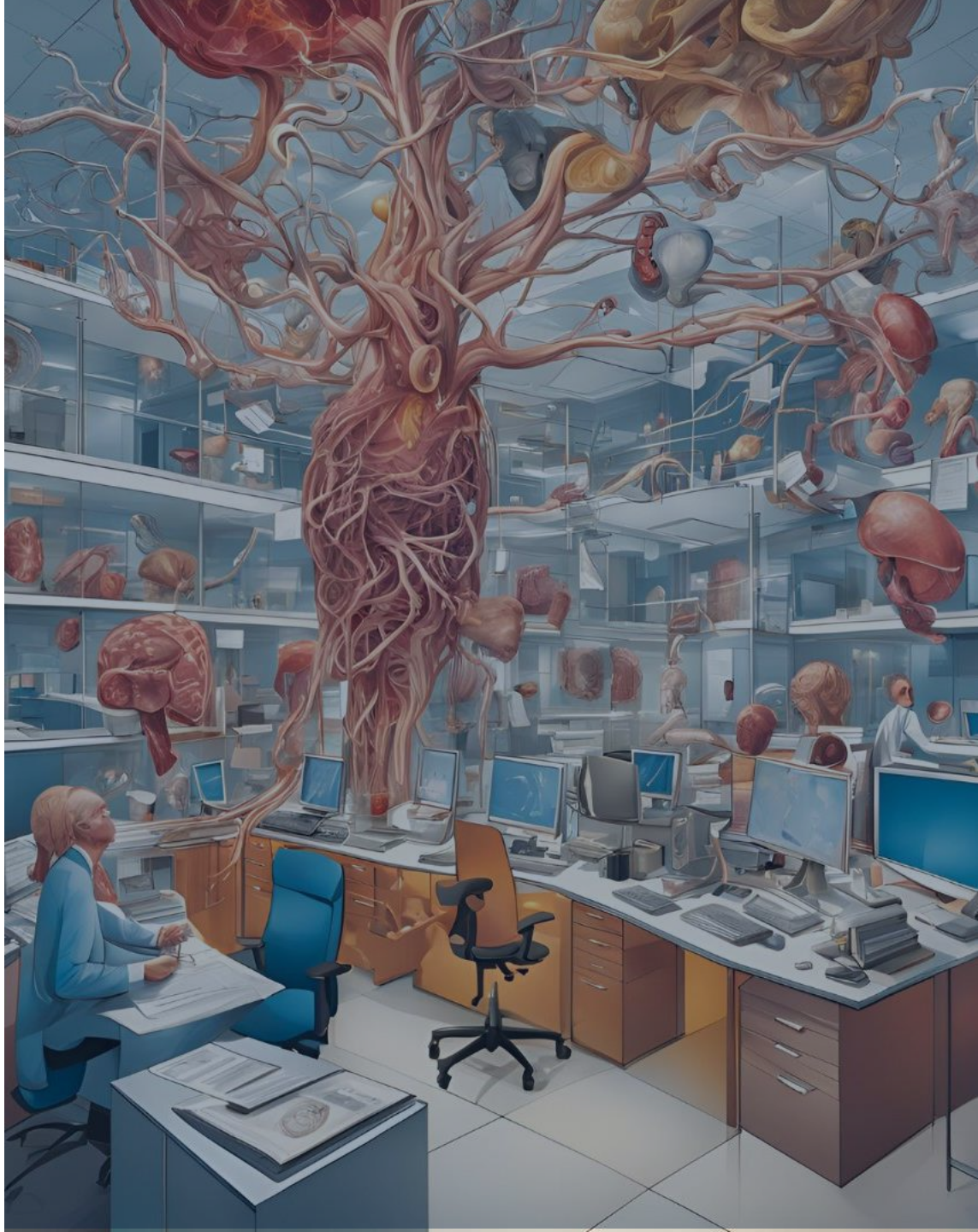
- **Sveiki įpročiai:**
  - Sveika mityba, sportas, geras miegas

  Kitaip tariant:
  - Mokymai, mokymai ir dar kartą mokymai

- **Savalaikė ir adekvati reakcija į negalavimus:**
  - Nuo kokios temperatūros / kokiems simptomams pasireiškus skubame pas gydytoją?

  Kitaip tariant:
  - Kokiais atvejais eskaluojame situaciją ir kreipiamės į teisininkus profesionalios pagalbos?

Ellex



AČIŪ!

MIGLĖ PETKEVIČIENĖ
Partnerė
Duomenų apsaugos, kibernetinės saugos ir atitikties komandos vadovė

T: +370 640 41055

E: migle.petkeviciene@ellex.legal

Kas patenka į NIS2 taikymo sritį?

Formulė: **Sektorius** (NIS2 1+2 priedai) + **Dydis**

Subjekto dydis	Esminis	Svarbus	Nepatenka į taikymo sritį
Didelis	Jei nurodytas pirmame priede	Jei nurodytas antrame priede	x
Vidutinis	gali būti esminė, jei: • vienintelė paslauga; • reikšmingas poveikis; • sisteminė rizika; • esminė visuomenei; • jei nusprendė valstybė narė.	Visuomet	x
Mažas	gali būti esminė, jei: • vienintelė paslauga; • reikšmingas poveikis; • sisteminė rizika; • esminė visuomenei; • jei nusprendė valstybė narė.	Gali būti laikoma svarbiu subjektu jei valstybė narė nuspręs	Dažniausiai

Į TIS1 taikymo sritį pateko: ~400 subjektų
Planuojama, kad į NIS2 taikymo sritį pateks: ~**22.000 subjektų** (Šaltinis)

Ellex

Sektorius	Subsektorius	Atsakinga institucija	Subjekto rūšis	Jurisdikcija	Didelis subjektas: 1) **dirba ≥ 250 darbuotojų** ir: a) **metinės pajamos ≥ 50 mln. EUR** arba b) **balanse nurodyto turto vertė ≥ 43 mln. EUR**	Vidutinis subjektas: 1) **dirba ≥ 50 darbuotojų** ir: a) **metinės pajamos ≥ 10 mln. EUR** arba b) **balanse nurodyto turto vertė ≥ 10 mln. EUR**	Maži ir labai maži subjektai: 1) **dirba ≤ 50 (maži) ≤ 10 (labai maži) darbuotojų** ir: a) **metinės pajamos ≤ 10 (maži) ≤ 2 (labai maži) mln. EUR** arba b) **balanse nurodyto turto vertė ≤ 10 (maži) ≤ 2 (labai maži) mln. EUR**
					Subjekto dydžiai yra apibrėžti Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatyme		
I priedas: YPATINGOS SVARBOS SEKTORIAI							
1. Energetika	Elektra	ENMIN	Elektros energijos įmonės	Valstybės narės (VN), kurioje įsisteigę	**ESMINIS** subjektas	**SVARBUS** subjektas nebent identifikuotas kaip ESMINIS subjektas pagal šiuos kriterijus: b) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, teikėjas valstybėje narėje; c) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai; d) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį; e) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje nacionaliniu ar regioniniu lygmeniu; TOLIAU TEKSTE: **SVARBUS** subjektas nebent identifikuotas kaip ESMINIS subjektas	**NETAIKOMA**, nebent identifikuotas kaip ESMINIS subjektas arba SVARBUS subjektas pagal šiuos kriterijus: b) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, teikėjas valstybėje narėje; c) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai; d) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį; e) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje nacionaliniu ar regioniniu lygmeniu; TOLIAU TEKSTE: **NETAIKOMA**, nebent identifikuotas kaip ESMINIS subjektas arba SVARBUS subjektas
		ENMIN	Skirstymo sistemos operatoriai				
		ENMIN	Perdavimo sistemos operatoriai				
		ENMIN	Gamintojai				
		ENMIN	Paskirtieji elektros energijos rinkos operatoriai				
		ENMIN	Elektros energijos rinkos dalyviai				
		ENMIN	Įkrovimo prieigos operatoriai, atsakingi už įkrovimo prieigos, kuri naudojama įkrovimo paslaugai galutiniams naudotojams teikti, taip pat ir judumo paslaugų teikėjo vardu bei jo pavedimu, valdymą ir eksploatavimą				
	Centralizuotas šilumos ir vėsumos tiekimas	ENMIN	Centralizuoto šilumos tiekimo arba centralizuoto vėsumos tiekimo operatoriai				
	Nafta	ENMIN	Naftotiekių operatoriai				
		ENMIN	Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai				
		ENMIN	Centrinės atsargų saugyklos				
	Dujos	ENMIN	Tiekimo įmonės				
		ENMIN	Skirstymo sistemos operatoriai				
		ENMIN	Perdavimo sistemos operatoriai				
		ENMIN	Laikymo sistemų operatoriai				
		ENMIN	SGD sistemos operatoriai				
		ENMIN	Gamtinių dujų įmonės				
		ENMIN	Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai				
	Vandenilis	ENMIN	Vandenilio gamybos, laikymo ir perdavimo operatoriai				
2. Transportas	Oro transportas	SUMIN	Oro vežėjai				
		SUMIN	Oro uosto valdymo organai				
		SUMIN	Skrydžių valdymo operatoriai				
	Geležinkelių transportas	SUMIN	Infrastruktūros valdytojai				
		SUMIN	Geležinkelio įmonės				
	Vandens transportas	SUMIN	Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės				
		SUMIN	Uostų, įskaitant jų uosto įrenginius, direkcijos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius				
		SUMIN	Laivų eismo tarnybų operatoriai				
	Kelių transportas	SUMIN	Kelių direkcijos, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis				
		SUMIN	Intelektinių transporto sistemų operatoriai				
3. Bankininkystė		FINMIN	Kredito įstaigos				
4. Finansų rinkų infrastruktūros objektai		FINMIN	Prekybos vietų operatoriai				
		FINMIN	Pagrindinės sandorio šalys				
5. Sveikatos priežiūra		SAM	Sveikatos priežiūros paslaugų teikėjai				
		SAM	ES etaloninės laboratorijos				
		SAM	Subjektai, vykdantys vaistų, mokslinių tyrimų ir kūrimo veiklą				
		SAM	Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus				
		SAM	Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas)				

II priedas: KITI ITIN SVARBŪS SEKTORIAI						
1. Pašto ir kurjerių paslaugos		SUMIN	Pašto paslaugų teikėjai, įskaitant kurjerių paslaugų tiekėjus	VN, kurioje įsisteigę	**SVARBUS** subjektas nebent identifikuotas kaip **ESMINIS** subjektas	**NETAIKOMA**, nebent identifikuotas kaip **ESMINIS** subjektas arba **SVARBUS** subjektas
2. Atliekų tvarkymas		AM	Atliekas tvarkančios įmonės, išskyrus įmones, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas			
3. Cheminių medžiagų gamyba ir platinimas		AM	Cheminės medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės ir gaminius iš tų medžiagų ar mišinių gaminančios įmonės			
4. Maisto gamyba, perdirbimas ir platinimas		ŽŪM	Maisto verslo įmonės, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą			
5. Gamyba	Medicinos priemonių ir in vitro diagnostikos medicinos priemonių gamyba	SAM	Medicinos priemones gaminantys subjektai, ir in vitro diagnostikos medicinos priemones gaminantys subjektai, išskyrus subjektus, gaminančius medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas).			
	Kompiuterinių, elektroninių ir optinių gaminių gamyba	EIM	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 26 skyriuje https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=2&VEIG_KODAS=C#C			
	Elektros įrangos gamyba	ENMIN	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 27 skyriuje https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=2&VEIG_KODAS=C#C			
	Niekur kitur nepriskirtų mašinų ir įrangos gamyba	Ministerijos	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 28 skyriuje https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=2&VEIG_KODAS=C#C			
	Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	SUMIN	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 29 skyriuje https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=2&VEIG_KODAS=C#C			
	Kitos transporto įrangos gamyba	SUMIN	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 30 skyriuje https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=2&VEIG_KODAS=C#C			
6. Skaitmeninių paslaugų teikėjai		EIM	Elektroninių prekyviečių teikėjai	VN, kurioje yra pagrindinė buveinė ES		
		EIM	Paieškos sistemų teikėjai			
		EIM	Socialinių tinklų paslaugų platformos teikėjai			
7. Moksliniai tyrimai		ŠMM	Mokslinių tyrimų organizacijos | Švietimo įstaigos, kai jos vykdo ypatingos svarbos mokslinių tyrimų veiklą	VN, kurioje įsisteigę		

Kas klasifikuojama kaip pažeidimas / incidentas?

BDAR

- **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

NIS2

- **Kibernetinis incidentas** – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.
- **Kibernetinis incidentas laikomas dideliu** bent vienu iš šių atvejų:
- 1) jeigu dėl kibernetinio incidento atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;
- 2) jeigu kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę arba neturtinę žalą.

DORA

- **Incidentai** – apima bet kurį neplanuotą įvykį arba kelis susijusius įvykius, kurie daro neigiamą poveikį finansų sektoriaus subjektų tinklų ir informacinių sistemų saugumui. Tai gali apimti su informacinėmis ir ryšių technologijomis (IRT) susijusius incidentus, kurie kenkia duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui, taip pat gali paveikti teikiamas finansų paslaugas.
- **Su mokėjimu susiję operaciniai arba saugumo incidentai** – apima neplanuotus įvykius, kurie gali būti tiek susiję, tiek nesusiję su IRT, ir kurie taip pat turi neigiamą poveikį su mokėjimais susijusių duomenų aspektams.
- **Dideli incidentai** – apima su IRT susijusius incidentus, kurie daro didelį neigiamą poveikį tinklams ir informacinėms sistemoms, naudojamoms finansų sektoriaus ypatingos svarbos arba svarbioms funkcijoms palaikyti.
- **Dideli su mokėjimu susiję operaciniai arba saugumo incidentai** – yra tie, kurie daro didelį neigiamą poveikį teikiamoms su mokėjimais susijusioms paslaugoms. Abu šie incidentų tipai reikalauja ypatingo dėmesio ir tinkamų valdymo priemonių, kad būtų užtikrintas finansų sektoriaus stabilumas ir saugumas.

Kokie pranešimo apie pažeidimą / incidentą reikalavimai?

BDAR

- Pranešima **priežiūros institucijai per 72 val.** nuo sužinojimo apie pažeidimą momento.
- **Duomenų subjektui** pranešama **nedelsiant** (rekomenduojama pranešti ne vėliau kaip per 72 val., tačiau tikslus terminas nėra numatytas).

NIS2

- Sužinojus apie didelius incidentus esminiai ir svarbūs subjektai laikosi šios incidentų pranešimo tvarkos:
  - ❖**Ankstyvasis perspėjimas** pateikiamas **per 24 val.** nuo didelio incidento aptikimo momento;
  - ❖**Pranešimas apie incidentą** pateikiamas **per 72 val.** nuo didelio incidento aptikimo momento;
  - ❖**Tarpinė ataskaita** pateikiama **kompetentingos institucijos prašymu**.
  - ❖**galutinė ataskaita** pateikiama per **1 mėn.** nuo pranešimo apie kibernetinį incidentą dienos
- Taip pat **reikalaujama informuoti savo paslaugų gavėjus**, kuriuos didelė kibernetinė grėsmė galėjo paveikti.
- Taip pat galimas **savanoriškas pranešimas** dėl:
  - ❖ Esminių ir svarbių subjektų **patirtų incidentų**, **kibernetinių grėsmių** ir **vos neįvykusių incidentų**
  - ❖ **Į direktyvos taikymo sritį nepatenkančių subjektų** pranešimai apie **didelius incidentus**, **kibernetines grėsmes** ir **vos neįvykusius incidentus**

DORA

- Sužinojus apie didelį incidentą laikomasi šios pažeidimų pranešimo tvarkos
  - ❖**Pradinis pranešimas** pateikiamas. **per 4 val.** nuo didelio incidento aptikimo momento, bet ne vėliau kaip **per 24 val.** nuo didelio incidento aptikimo momento.
  - ❖**Tarpinis pranešimas** pateikiamas **per 72 val**. nuo didelio incidento aptikimo momento.
  - ❖**Galutinis pranešimas** pateikiamas per **1 mėn.** nuo paskutinio tarpinio pranešimo dienos.
- Taip pat galimas **savanoriškas pranešimas** apie kibernetines grėsmes

Ellex

Atsakingos institucijos

Pagal BDAR

- Valstybinė duomenų apsaugos inspekcija (VDAI)

Pagal NIS2

- Nacionalinis kibernetinio saugumo centas (NKSC)

Pagal DORA

- Lietuvos bankas (LB)