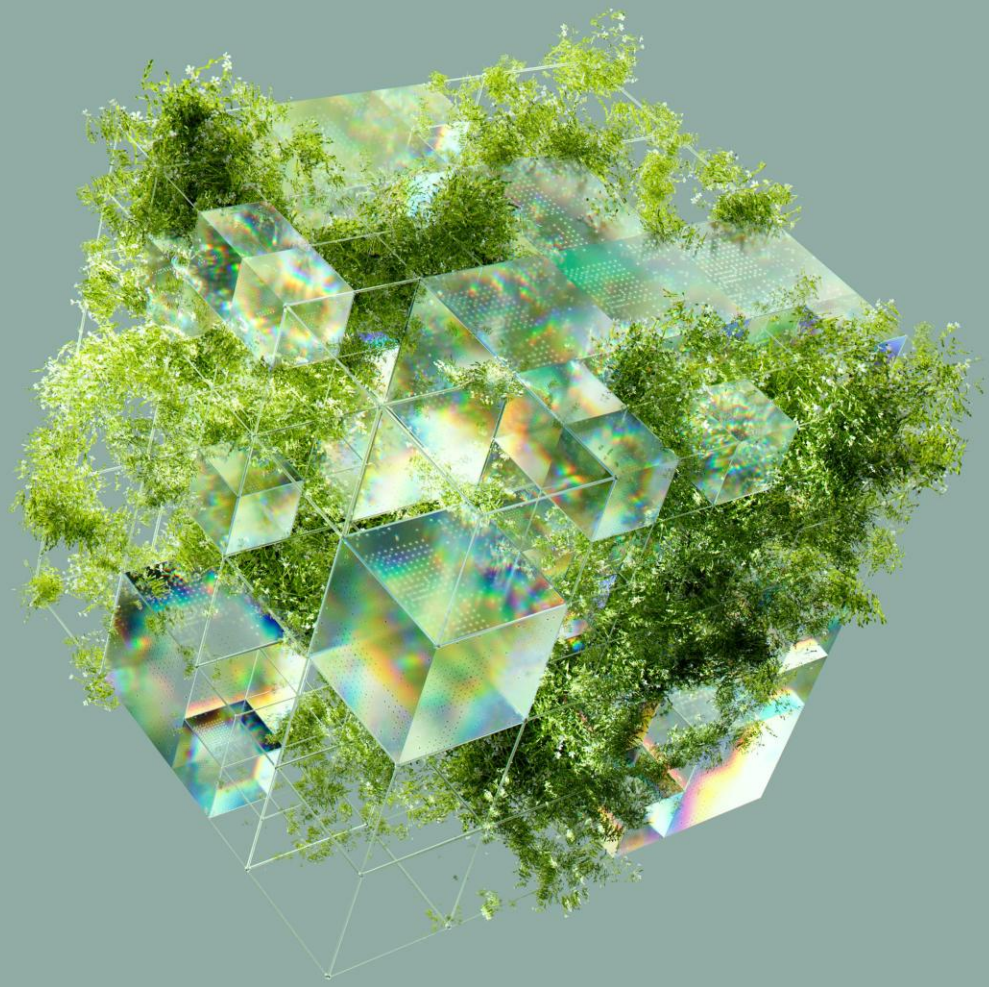
Mākslīgā intelekta un kiberdrošības izaicinājumi mežsaimniecībā un lauksaimniecībā: tiesiskais ietvars un riski



Edvijs Zandars

19.03.2026.

Ellex Klavins

Mākslīgā intelekta regulējums un riski

Ellex Klavins

Mākslīgā intelekta akts

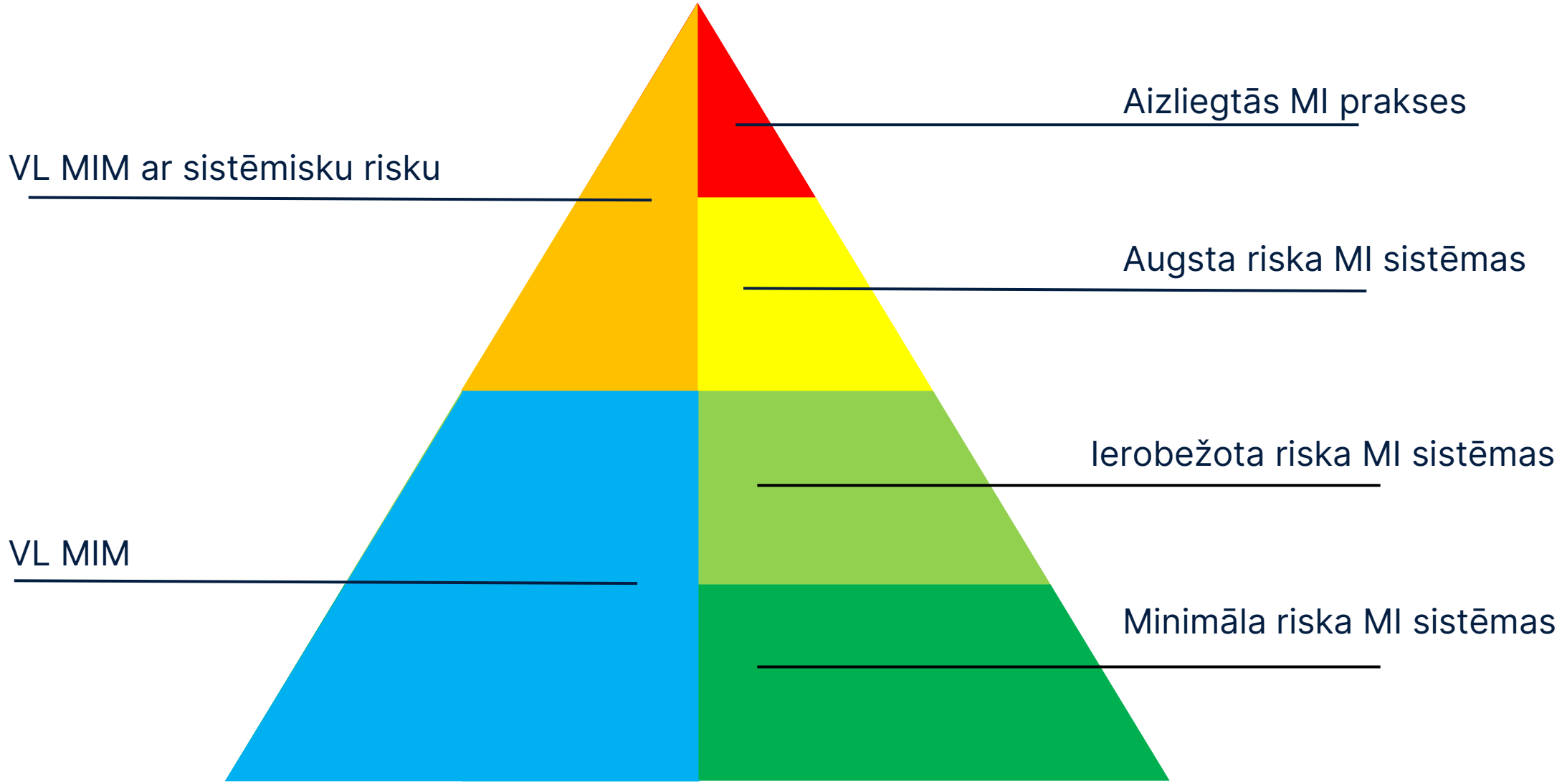
Eiropas Parlamenta un Padomes 2024. gada 13. jūnija Regula Nr. 2024/1689 «**Mākslīgā intelekta akts**»

- MI Akts būs piemērojams no **2. augusta!**
- Aizliegtās prakses – jau piemērojams
- Vispārīga lietojuma MIM – jau piemērojams
- Augsta riska sistēmas kā drošības komponentes vai produkti (MI Akta 6. panta pirmā daļa, I pielikums) – 2027. gada 2. augusts?
- Digitālā omnibusa pakotne: 2027./2028.gads

Akta uzbūve

- MI sistēmu laišana tirgū
- Aizliegtā MI prakse
- MI sistēmu klasifikācija
- Augsta riska MI sistēmas
- Noteiktas MI sistēmas
- Vispārīga lietojuma MI modeļi
- Tirgus uzraudzība un NA izpilde
- Pasākumi inovāciju atbalstam

MI sistēmu un VL MI modeļu klasifikācija



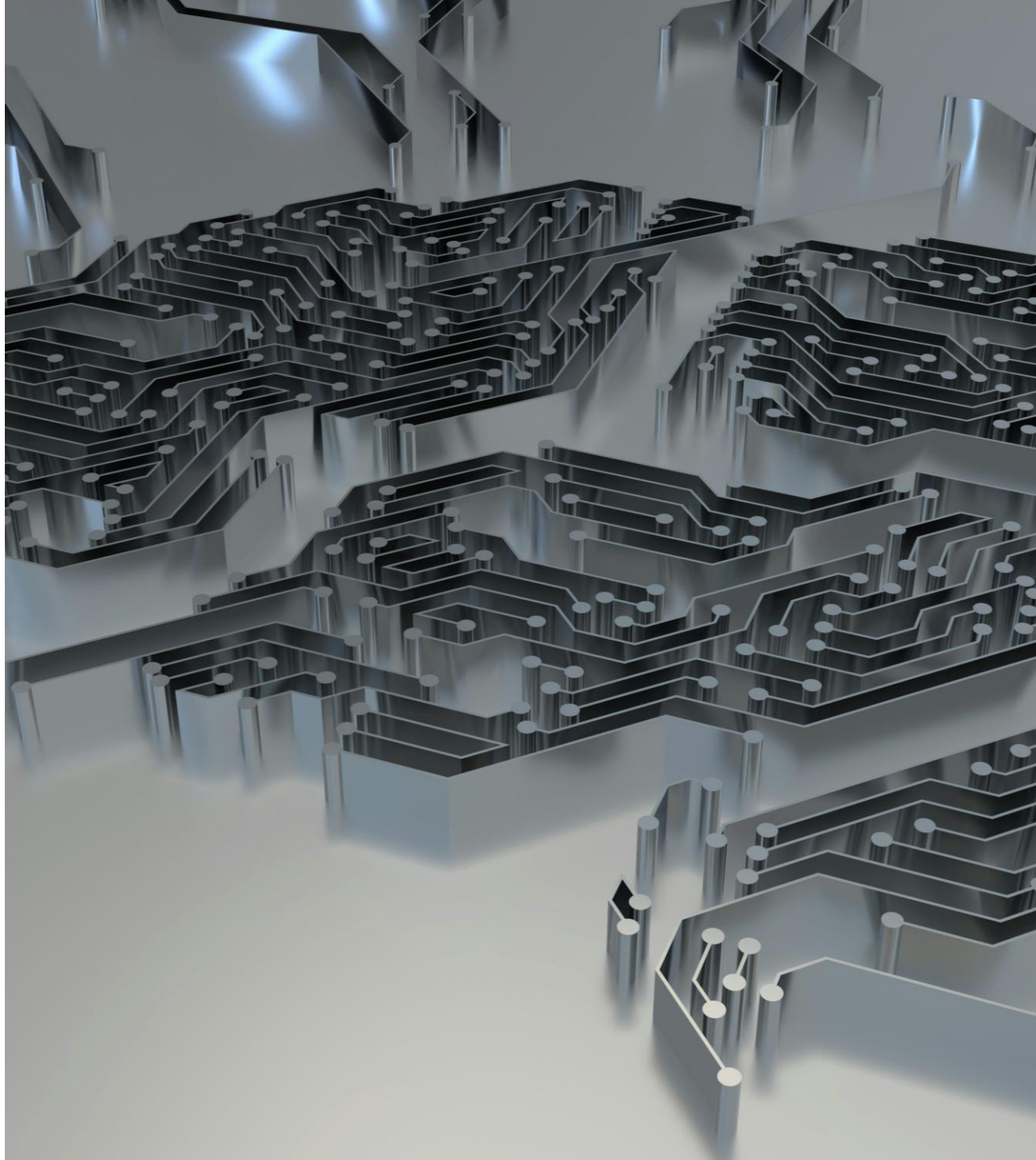
Augsta riska MI sistēmas

MI sistēmas, kas ir drošības komponentes produktos vai noteiktos gadījumos sistēmas, kas pašas ir produkti, piemēram:

- **mašīnās**
- **rūpnieciskās iekārtās**
- **transportlīdzekļos**
- radio iekārtās
- medicīniskās ierīcēs u.c.

vai

III pielikumā uzskaitītās sistēmas



Drošības komponente?

Nosacījumi 6.panta 1.daļā:

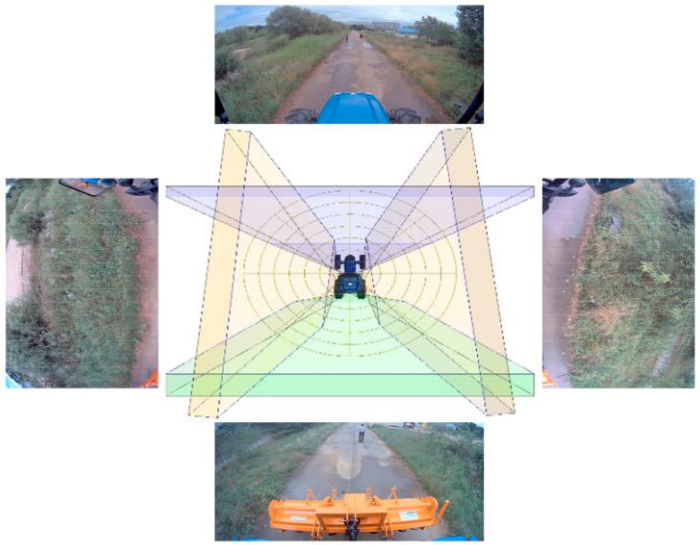
a) MI sistēmu paredzēts izmantot kā produkta drošības sastāvdaļu, vai MI sistēma pati par sevi ir produkts, uz kuru attiecas Savienības saskaņošanas tiesību akti, kas uzskaitīti I pielikumā;

b) produktam, kura drošības sastāvdaļa, ievērojot a) apakšpunktu, ir MI sistēma, vai pašai MI sistēmai kā produktam ir vajadzīgs trešās personas veikts atbilstības novērtējums, lai to varētu laist tirgū vai nodot ekspluatācijā saskaņā ar Savienības saskaņošanas tiesību aktiem, kas uzskaitīti I pielikumā.

I PIELIKUMS
B iedaļa. Citu Savienības saskaņošanas tiesību aktu saraksts

15.Eiropas Parlamenta un Padomes Regula (ES) Nr. 167/2013 (2013. gada 5. februāris) par lauksaimniecības un mežsaimniecības transportlīdzekļu apstiprināšanu un tirgus uzraudzību (OV L 60, 2.3.2013., 1. lpp.).

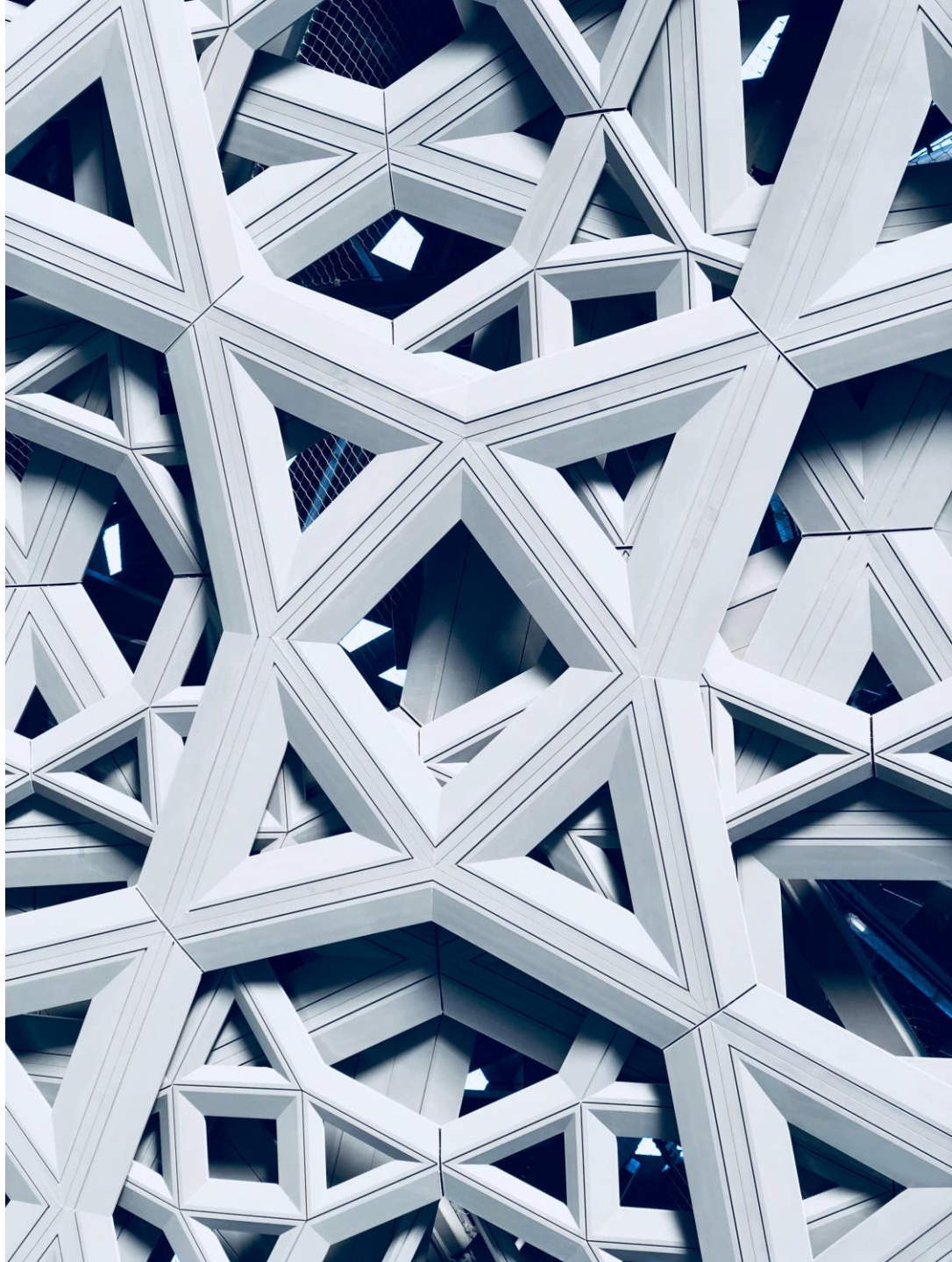
https://www.forsler.com/post/aoro-the-worlds-first-autonomous-forest-machine



https://www.mdpi.com/2411-9660/4/4/54?utm

Augsta riska MI sistēmas (III pielikums)

- **Biometriskās sistēmas**
- Kritiskā infrastruktūra
- Izglītība un profesionālā apmācība
- **Nodarbinātība, darbinieku pārvaldība** un piekļuve pašnodarbinātībai
- Būtiski privātie pakalpojumi un būtiski sabiedriskie pakalpojumi, un labumi (piemēram, veselības aprūpe, kredītspējas vērtējums, veselības apdrošināšana)
- Tiesībaizsardzība
- Migrācija, patvēruma meklētāji un robežkontroles pārvaldība
- Tieslietu un demokrātisko procesu pārvaldība



Augsta riska MI sistēmu uzturētāju pienākumi

Vispārīgi:

- Veikt tehniskos un organizatoriskos pasākumi MI sistēmas atbilstošai izmantošanai
- Virsvadību pār MI sistēmu īsteno kvalificēts un apmācīts personāls
- Ievades dati ir atbilstoši un reprezentatīvi, ņemot vērā MIS mērķi
- Pirms MI sistēmas ieviešanas informēt darbiniekus par MI sistēmas ieviešanu
- Informēt III. pielikuma subjektus par MI sistēmas pielietošanu
- Glabāt MI žurnāldatus, vismaz 6 mēnešus, ja vien cits ES tiesību akts nenoteic citādi
- Sadarboties ar citiem ar konkrēto MI sistēmu saistītajiem operatoriem un publiskajām institūcijām, lai novērstu vai izmeklētu incidentus, risku u.tml.
- Specifiskas prasības publiskām institūcijām un publiski svarīgu pakalpojumu sniedzējiem.

Naudas sodi saistībā ar MI sistēmām

- Aizliegtās prakses regulējuma pārkāpums – līdz **35 000 000 EUR** vai, ja pārkāpējs ir uzņēmums - līdz 7% no tā kopējā gada apgrozījuma pasaulē iepriekšējā finanšu gadā, atkarībā no tā, kura ir lielāka summa.
- Pārējie pārkāpumi (16., 22., 23., 24., 26., 50. pants vai kompetentās iestādes prasības) - līdz **15 000 000 EUR** vai, ja pārkāpējs ir uzņēmums - līdz 3% no tā kopējā gada apgrozījuma pasaulē iepriekšējā finanšu gadā, atkarībā no tā, kura ir lielāka summa:

Nepareizas, nepilnīgas vai maldinošas informācijas sniegšana pilnvarotajai iestādei - līdz **EUR 7 500 000** vai, ja pārkāpējs ir uzņēmums līdz 1% no tā kopējā gada apgrozījuma p asaulē iepriekšējā finanšu gadā, atkarībā no tā, kura ir lielāka summa.

Kiberdrošības regulējums un riski

Ellex Klavins

Nacionālās kiberdrošības likums

Galvenās prasības / jaunumi subjektiem

- Statusa noteikšana un paziņošana
- Ziņošana par incidentiem un ievainojamībām
- Kiberdrošības pārvaldnieka noteikšana
- Pašvērtējuma ziņojums
- Minimālās kiberdrošības prasības
- Subjektu uzraudzība / sodi

Statusa noteikšana un paziņošana

NDKL subjekti

20. pants
Būtisko pakalpojumu sniedzēji

21. pants
Svarīgo pakalpojumu sniedzēji

24. pants
Kritiskā IKT infrastruktūra

MK apstiprinātajā kritiskās infrastruktūras kopumā iekļautā

Liels saimnieciskās darbības veicējs:
- Apgrozījums: >EUR 50 mio
- Darbinieki: vismaz 250

Vidējs saimnieciskās darbības veicējs:
- Apgrozījums: EUR 10-50 mio
- Darbinieki: <250

NKL subjekti

Būtisko pakalpojumu sniedzējs:

- Iestāde vai saimnieciskās darbības veicējs, kura darbības traucējums var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai var radīt būtisku sistēmisku risku, jo īpaši nozarēs, kurās šādam traucējumam var būt pārrobežu ietekme (*NKL 20.panta 11.pkt*).

Svarīgo pakalpojumu sniedzējs:

- komersants, kura pamatdarbība ir pārtikas rūpnieciska ražošana, pārstrāde vai pārtikas izplatīšana vairumtirdzniecībā (*NKL 21.panta 1.d. 2.pkt. e)*

Nacionālās drošības likuma subjekti

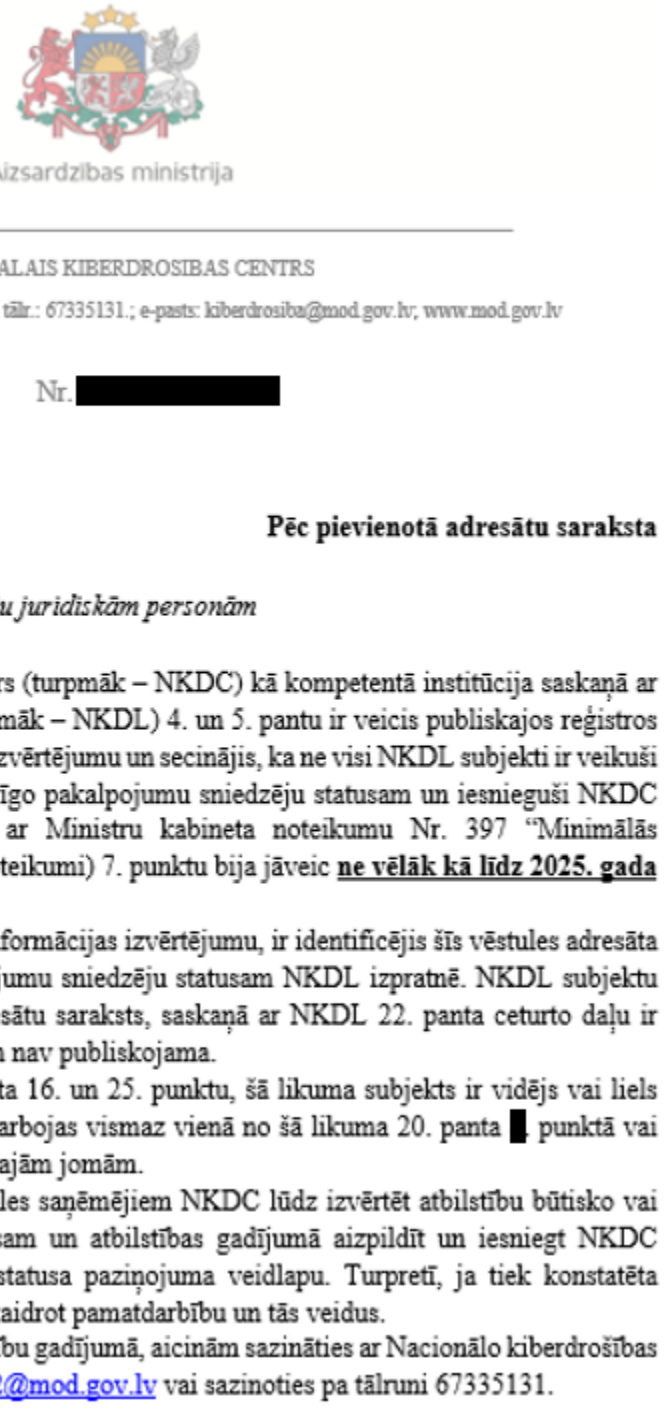
37.pants:

- Latvijas Republikā esošas **meža zemes** vismaz 10 000 hektāru platībā īpašnieks
- Latvijas Republikā esošas **lauksaimniecības zemes** vismaz 4000 hektāru platībā īpašnieks

Kā rīkoties, ja ir saņemts aicinājums no NKC reģistrēties

1. **Saglabāt mieru.** Paziņojums vēl nenozīmē, ka ir jāreģistrējas kā būtiska/svarīga pakalpojuma sniedzējam
2. **Pārskatīt pamatojumu.** Iekšēji izvērtēt, vai uzņēmuma darbība tiešām ietilpst Nacionālā kiberdrošības likuma 20. vai 21. pantā noteikto pakalpojumu tvērumā
3. **Sniegt rakstveida atbildi.** Noteiktajā termiņā sniegt prasīto informāciju **vai** iesniegt argumentētu paskaidrojumu, kāpēc statuss neattiecas.

- **NKC pats nereģistrē** – formāli statusu piešķir Digitālās drošības uzraudzības komiteja
- Paziņojums **nenozīmē automātisku reģistrāciju**, bet gan aicinājumu sniegt informāciju un pamatojumu



Aizsardzības ministrija

NACIONĀLAIS KIBERDROŠĪBAS CENTRS

K. Valdemāra iela 10/12, Rīga, LV-1473; tālr.: 67335131.; e-pasts: kiberdrosiba@mod.gov.lv; www.mod.gov.lv

Rīgā, [redacted] Nr. [redacted]

Pēc pievienotā adresātu saraksta

Par NKDL subjekta statusa reģistrāciju juridiskām personām

Nacionālais kiberdrošības centrs (turpmāk – NKDC) kā kompetentā institūcija saskaņā ar Nacionālās kiberdrošības likuma (turpmāk – NKDL) 4. un 5. pantu ir veicis publiskajos reģistros pieejamās informācijas pirmšķietamu izvērtējumu un secinājis, ka ne visi NKDL subjekti ir veikuši atbilstības noteikšanu būtisko vai svarīgo pakalpojumu sniedzēju statusam un iesnieguši NKDC paziņojuma veidlapas, kas saskaņā ar Ministru kabineta noteikumu Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk – Noteikumi) 7. punktu bija jāveic **ne vēlāk kā līdz 2025. gada 1. aprīlim**.

NKDC, veicot pirmšķietamu informācijas izvērtējumu, ir identificējis šīs vēstules adresāta atbilstību būtisko vai svarīgo pakalpojumu sniedzēju statusam NKDL izpratnē. NKDL subjektu saraksts, attiecīgi arī šīs vēstules adresātu saraksts, saskaņā ar NKDL 22. panta ceturto daļu ir ierobežotas pieejamības informācija un nav publiskojama.

Pamatojoties uz NKDL 1. panta 16. un 25. punktu, šā likuma subjekts ir vidējs vai liels saimnieciskās darbības veicējs, kurš darbojas vismaz vienā no šā likuma 20. panta [redacted] punktā vai 21. panta [redacted] punktā minētajām jomām.

Ņemot vērā norādīto, šīs vēstules saņēmējiem NKDC lūdz izvērtēt atbilstību būtisko vai svarīgo pakalpojumu sniedzēju statusam un atbilstības gadījumā aizpildīt un iesniegt NKDC Noteikumu 1. pielikumā pievienoto statusa paziņojuma veidlapu. Turpretī, ja tiek konstatēta neatbilstība kritērijiem, NKDC lūdz skaidrot pamatdarbību un tās veidus.

Papildu jautājumu vai neskaidrību gadījumā, aicinām sazināties ar Nacionālo kiberdrošības centru, izmantojot e-pasta adresi: NIS2@mod.gov.lv vai sazinoties pa tālruni 67335131.

Subjekta pienākumi kiberdrošības jomā (1)

- Ieviest, uzturēt un periodiski aktualizēt kiberdrošības pārvaldības dokumentāciju
- Iecelt kiberdrošības pārvaldnieku
- Ieviest lietotāju piekļuves pārvaldības sistēmu un nodrošināt, ka visi datu apstrādes procesi ir kontrolējami
- IKT kritiskās infrastruktūras īpašniekam un būtisko pakalpojumu sniedzējam jānodrošina procesu ieviešana tīklu pārvaldībai
- Nodrošināt informācijas sistēmu un tīkla plūsmu logu ģenērēšanu un drošu uzglabāšanu

Subjekta pienākumi kiberdrošības jomā (2)

- Nodrošināt žurnālfailu pārvaldību, informācijas sistēmu rezerves kopiju veidošanu, kiberhigiēnas pasākumus un datu šifrēšanu
- Ziņot par kiberincidentiem
- Uzglabāt rezerves kopijas katrai informācijas sistēmai, kas atrodas subjekta īpašumā vai valdījumā
- Organizēt darbiniekiem kiberdrošības apmācības
- Ievērot ārpakalpojumu prasības par IKT resursa vai pakalpojuma iegādi
- Sagatavot pašvērtējuma ziņojumu par atbilstību kiberdrošības prasībām

Minimālās kiberdrošības prasības (MK noteikumi Nr. 397)

- Minimālās kiberdrošības prasības
- Prasības kiberdrošības pārvaldniekam
- Kiberrisku pārvaldības un darbības nepārtrauktības plāna prasības
- Incidentu nozīmīguma kritēriji

- Prasības drošības auditoriem
- Elektronisko sakaru tīklu drošības prasības
- Incidentu ziņošanas kārtība
- Pašvērtējuma ziņojuma un citas formas
- U.c.

Stājās spēkā 02.07.2025.

Uzsvars uz kiberdrošības pārvaldību, nevis specifiskām prasībām (salāgots ar ISO 27001)

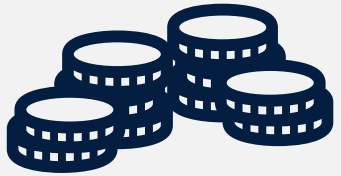
Subjektu uzraudzība / sodi

- **Uzraudzības iestādes:**
  - Nacionālais kiberdrošības centrs
  - Satversmes aizsardzības birojs

- **Iestāžu tiesības:**
  - Uzdot novērst konstatētās neatbilstības
  - Veikt vai uzdot veikt ārēju atbilstības auditu
  - Apturēt IS, resursu vai e-pakalpojumu darbību līdz neatbilstību novēršanai
  - Apturēt produktu tirdzniecību vai pakalpojumu sniegšanu līdz neatbilstību novēršanai
  - Noteikt pagaidu aizliegumu subjektu vadītājam pildīt pienākumus līdz neatbilstību novēršanai

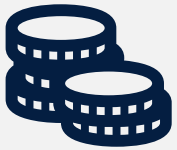
Sodi

Būtisko pakalpojumu sniedzējiem un IKT KI



Līdz 10 miljoniem eiro vai līdz 2% no kopējā gada apgrozījuma pasaulē

Svarīgo pakalpojumu sniedzējiem



Līdz 7 miljoniem eiro vai līdz 1,4% no kopējā gada apgrozījuma pasaulē

*«Kiberapdraudējumu līmenis Latvijā saglabājas augsts ar noturīgu augšupejošu tendenci. Kopš Krievijas pilna mēroga iebrukuma Ukrainā **kiberincidentu skaits Latvijas kibertelpā ir seškāršojies** – 2025. gada 4. ceturksnī fiksēts vēsturiski augstākais CERT.LV **manuāli apstrādātu kiberincidentu skaits (923)**, savukārt **apdraudēto iekārtu skaits** ir pieaudzis astoņkārtīgi, pārskata periodā sasniedzot rekordaugstu līmeni (**731 783**). [..]*

*Pastiprinās sociālā inženierija ar efektīvu **mākslīgā intelekta rīku un automatizācijas pielietojumu**, kas paātrina identitātes zādzības un kontu kompromitēšanu.»**

* CERT.LV 2025. gada 4. ceturkšņa pārskats par situāciju Latvijas kibertelpā

Paldies par uzmanību!
Jautājumi?

Edvijs Zandars
Asociētais partneris
edvijs.zandars@ellex.legal
+371 6781 4848

Ellex

Baltic circle of legal excellence

Ellex Raidla

Ahtri 4
EE-10151 Tallina
Igaunija

+372 640 7170
estonia@ellex.legal

Ellex Klavins

K.Valdemāra 62
LV-1013 Rīga
Latvija

+371 6781 4848
latvia@ellex.legal

Ellex Valiunas

Jogailos g. 9
LT-01116 Viļņa
Lietuva

+370 5268 1888
lithuania@ellex.legal