05.06.2025.

BIEŽĀK UZDOTIE JAUTĀJUMI

Aizsardzības ministrijas Kiberdrošības politikas departaments ir apkopojis biežāk uzdotos jautājumus par Nacionālā kiberdrošības likuma (NKDL) piemērošanu. Dokuments tiks aktualizēts pēc Ministru kabineta noteikumu projekta "Minimālās kiberdrošības prasības" pieņemšanas.

SUBJEKTU PAŠIDENTIFIKĀCIJAS JAUTĀJUMI

1. Kā var pārliecināties par atbilstību NKDL statusam?

Aicinām izmantot izstrādāto interaktīvo rīku - testu, kas palīdzēs noteikt, vai NKDL izpratnē esat uzskatāms par NKDL subjektu un vai uz Jūsu pārstāvēto organizāciju attiecas NKDL normas. Ja pēc testa aizpildīšanas nav iegūta pārliecība par atbilstību vai rodas papildu jautājumi, aicinām sazināties ar NIS2 kontaktpunktu: NIS2@mod.gov.lv

2. Vai iestāde var vienlaikus būt gan būtisko, gan svarīgo pakalpojumu sniedzējs, gan IKT kritiskās infrastruktūras turētājs?

Kaut arī iestāde var atbilst vairākām NKDL subjekta kategorijām, kā atbilstošo nosaka augstāko.
Gadījumā, ja attiecībā uz pakalpojuma sniedzēju vienlaicīgi izpildās būtisko pakalpojumu sniedzēja un svarīgo pakalpojumu sniedzēja pazīmes, šāds pakalpojuma sniedzējs NKDL izpratnē uzskatāms par būtisko pakalpojumu sniedzēju. Piemēram, valsts dibināta augstskola, kas vienlaikus ir atvasināta publiska persona un izglītības informācijas sistēmas uzturētājs, NKDL izpratnē uzskatāma par būtisko pakalpojumu sniedzēju, savukārt šīs augstskolas dibinātās pastarpinātās pārvaldes iestādes (piemēram, zinātniskie institūti), kā arī subjekti, kas uztur augstskolas izglītības informācijas sistēmas (piemēram, privāto tiesību juridiskā persona - izglītības informācijas sistēmas ārpakalpojuma sniedzējs), uzskatāmi par svarīgo pakalpojumu sniedzējiem.

Ja iestāde atbilst vairākām NDKL noteikto subjektu kategorijām, tai reģistrējoties NKDC, tāpat jānorāda visas atbilstošās darbības jomas (gan būtiskās, gan svarīgās).

Augstāk minētājos gadījumos NKDL subjektu uzraudzību veic Aizsardzības ministrija. Savukārt ja uzņēmums ir būtisko pakalpojumu sniedzējs, bet tā valdījumā ir IKT kritiskā infrastruktūra, tam piemēro IKT kritiskajai infrastruktūrai noteiktās prasības un tā uzraudzību veic SAB.

3. Kas uzraudzīs kiberdrošību subjektā, ja tā valdījumā ir sistēma, kas ir IKT KI?

Šādā gadījumā uzraudzību veiks Satversmes aizsardzības birojs.

4. Vai pēc būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapas iesniegšanas tiks saņemts kāds paziņojums, lēmums vai informatīva vēstule par subjekta iekļaušanu šajā sarakstā?

NKDC informēs par subjektu anketas saņemšanu, nepieciešamo papildu informāciju, ja tāda būs, iekļaušanu sarakstā, kā arī atgādinās arī par nākamajiem informācijas iesniegšanas termiņiem.

5. Vai visi vidējas saimnieciskās darbības veicēji, kuri uztur tiešsaistes tirdzniecības vietu, ir tiešsaistes tirdzniecības vietas pakalpojumu sniedzēji saskaņā ar NKDL?

Nē, saskaņā ar NIS2 Direktīvu un Negodīgas komercprakses aizlieguma likumu, tiešsaistes tirdzniecības vieta ir pakalpojuma sniegšanas vieta, izmantojot programmatūru, tostarp tīmekļa vietne, tīmekļa vietnes daļa vai lietotne, ko uztur komercprakses īstenotājs vai kas tiek uzturēta komercprakses īstenotāja vārdā un kas ļauj patērētājiem slēgt distances līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai patērētājiem. Attiecīgi tiešsaistes tirdzniecības vietas pakalpojumu sniedzējs ir tikai tādas platformas uzturētājs, kurā patērētājam ir iespēja slēgt līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai citiem patērētājiem, nevis ar pašu interneta vietnes uztur5ētāju.

6. Vai uzņēmums, kura pamatdarbības joma ietver impregnēšanu ir uzskatāms par NKDL subjektu atbilstoši NKDL 20. un 21. pantā aptvertajam nozaru lokam?

Norādām, ka impregnēšana neietilpst nevienā no NKDL 20. un 21. pantā ietvertajām nozarēm. Vienlaikus norādām, ka Nacionālais kiberdrošības centrs ir analoģiski vērtējis vairākus gadījumus, kuros uzņēmuma pamatdarbība ietver impregnēšanu un secinājis, ka, piemēram, koksnes impregnēšana nevar tikt pielīdzināta ķīmisko vielu ražošanai, jo impregnēšanas procesā koksne tiek tikai apstrādāta ar kāda cita komersanta ražotu ķīmisko vielu, kā rezultātā netiek mainīts koksnes molekulārais sastāvs un pati koksne kā materiāls nekļūst par ķīmisko vielu. Tādējādi neveidojas jauns ķīmiskais elements kā tas notiek ražošanas procesā, līdz ar to impregnēšana neatbilst nevienai no NKDL 20. un 21. pantā ietvertajām nozarēm un nav uzskatāma par būtisko pakalpojumu sniedzēju vai svarīgo pakalpojumu sniedzēju NKDL izpratnē.

7. Vai uzņēmums tiek uzskatīts par NKDL subjektu, ja tas darbojas kādā no likumā minētajām nozarēm, taču šī nav tā galvenā (pamatdarbība)?

Jā, uzņēmums var tikt uzskatīts par NKDL subjektu arī tad, ja tā darbība kādā no likumā minētajām nozarēm nav tā pamatdarbība. Katram uzņēmumam ir individuāli jāizvērtē, vai tā veiktā saimnieciskā darbība ietilpst NKDL noteiktajās jomās. Nacionālais kiberdrošības centrs, vērtējot uzņēmuma atbilstību likuma subjektam, balstās uz publiski pieejamo informāciju par uzņēmumu.

SODI

8. Kā soda valsts iestādes par neatbilstībām? Vai valsts iestāžu vadītājiem neatbilstību gadījumā piespriestu naudas sodu?

Attiecībā uz valsts iestāžu vadītājiem neatbilstību gadījumā netiek piemērots naudas sods. Ja NKDL subjekts, kurš ir tiešās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par šo neatbilstību ziņo attiecīgajam Ministru kabineta loceklim. Šādā gadījumā Ministru kabineta loceklis izvērtē nepieciešamību ierosināt disciplinārlietu un lemj par turpmāko rīcību neatbilstības novēršanai, savukārt atbildīgais Ministru kabineta loceklis par neatbilstības novēršanas gaitu ziņo Ministru kabinetam. Ja NKDL subjekts, kurš ir pašvaldība vai pašvaldības dibināta pastarpinātās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par šo neatbilstību ziņo attiecīgās pašvaldības domes priekšsēdētājam, kuri lemj par pašvaldību institūciju un amatpersonu (darbinieku) atbildību Pašvaldību likumā noteiktajā kārtībā, kā arī viedās administrācijas un reģionālās attīstības ministru. Vienlaikus, ja NKDL subjekts, kurš ir iepriekš neminēta valsts vai pašvaldības institūcija, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par konstatēto neatbilstību ziņo Ministru kabinetam un Ministru kabinets lemj par turpmāko rīcību neatbilstības novēršanai.

9. Kādi ir naudas sodi par likuma prasību neievērošanu?

Attiecībā uz privāto tiesību juridiskajām personām, sankcijas par prasību neizpildi ietver soda naudas piemērošanu un administratīvā akta piespiedu izpildi. Attiecībā uz būtisko pakalpojumu sniedzējiem un IKT kritisko infrastruktūru, soda naudu var piemērot līdz 10 milj. *euro* vai līdz 2% no uzņēmuma kopējā gada apgrozījuma pasaulē. Attiecībā uz svarīgo pakalpojumu sniedzējiem – līdz 7 milj. *euro* vai līdz 1,4% no kopējā gada apgrozījuma pasaulē.

Vienlaikus, Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam atbilstoši NKDL noteiktajam, veicot uz noteiktu darbību vai darbības aizliegumu vērsta lēmuma piespiedu izpildi, ir tiesības uzlikt piespiedu naudas sodu, kas vienā reizē nepārsniedz 10 000 *euro*.

PRASĪBAS KIBERDROŠĪBAS PĀRVALDNIEKAM

10. Vai kiberdrošības pārvaldnieks var būt uzņēmuma IT departamenta pārstāvis?

Jā, vienlaikus pēc labās prakses atbildīgajam par kiberdrošības pārvaldību būtu jābūt tiešā uzņēmuma/iestādes vadītāja pakļautībā, lai novērstu iespējamu interešu konfliktu, kā arī pastāv interešu konflikta risks, jo pēc būtības kiberdrošības pārvaldnieks netieši novērtē/var novērtēt arī organizācijas IT uzturētāju darbu. Vienlaikus norādām, ka subjekta vadītājs atbild par kiberdrošību organizācijā un, ja attiecīgo personu ieceļ organizācijā par pārvaldnieku, tam jāsadarbojas ar uzņēmuma vadītāju nevis IT departamenta direktoru.

11. Vai kiberdrošības pārvaldnieku var nolīgt ārpakalpojumā?

Jā, subjekts var piesaistīt kiberdrošības pārvaldības ārpakalpojumus, nodrošinot kiberdrošības prasībām atbilstošu kontroli. Vienlaikus ir jāņem vērā, ka IKT KI turētājiem ārpakalpojumu saņemšanu jāsaskaņo ar valsts drošības iestādi.

Šobrīd, strādājot pie Ministru kabineta noteikumu projekta "Minimālās kiberdrošības prasības", ir plānots noteikt cik subjektos viena fiziskā persona var vienlaicīgi būt kiberdrošības pārvaldnieks, atkarībā no tā vai subjekts ir būtisko pakalpojumu sniedzējs, svarīgo pakalpojumu sniedzējs vai IKT KI īpašnieks un tiesiskais valdītājs. Minētais MK noteikumu projekts atrodas gala saskaņošanas procesā.Aicinām sekot līdzi MK noteikumu projekta virzībai Tiesību aktu portālā: *šeit*.

12. Kāda izglītība nepieciešama kiberdrošības pārvaldniekam? Kādi starptautiskie kursi vai sertifikāti ir nepieciešami/derīgi?

Atbilstoši Ministru kabineta noteikumu projekta "Minimālās kiberdrošības prasības" 3.1. apakšnodaļai, par kiberdrošības pārvaldnieku var būt fiziska persona, kurai ir augstākā vai vidējā profesionālā izglītība IT, kiberdrošības pārvaldības vai citā saistītā jomā, vai kura ir saņēmusi starptautiski atzītu sertifikātu, kas apliecina personas kvalifikāciju kiberdrošības pārvaldības jomā (piemēram, CISM, CISSP), vai kurai ir vismaz divu gadu darba pieredze kiberdrošības pasākumu plānošanā vai īstenošanā, kas iegūta pēdējo 5 gadu laikā. Līdz ar to ir jāizpildās vismaz vienam no iepriekš uzskaitītajiem kritērijiem, lai persona varētu tikt iecelta par kiberdrošības pārvaldnieku subjektā.

Ir virkne starptautiski atzītu un labu sertifikātu, piemēram, *CompTIA Security+ ,Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), ISO/IEC 27001 Lead Implementer, NIST Cybersecurity Framework*. Vienlaikus norādām, ka attiecībā uz starptautiskajiem sertifikātiem, kas būtu atbilstoši kiberdrošības pārvaldniekiem, primāri uz kiberdrošības pārvaldību attiektos apgabalu *Security and Risk Management* un *Security Assessment And Testing* (*Intermediate* līmeņa un uz augšu) – CISO, CISM, CISSP. No Latvijā biežāk izplatītajiem derētu arī ISACA izdotie CISA sertifikāti vai ITIL.

13. Vai kiberdrošības pārvaldnieks var būt Latvijas nepilsonis?

Saskaņā ar Ministru kabineta noteikumu projekta par minimālajām kiberdrošības prasībām 12. un 13, punktā noteikto par kiberdrošības pārvaldnieku var būt fiziska persona, kurai ir NATO, Eiropas Savienības vai Eiropas Brīvās tirdzniecības asociācijas valsts pilsonība. Ja kiberdrošības pārvaldnieks tiek iecelts IKT kritiskās infrastruktūras objektā, tas drīkst būt tikai Latvijas pilsonis.

14. Vai kiberdrošības pārvaldnieka pienākumus var veikt vairākas personas vai komanda, nevis tikai viena konkrēta persona?

Nē, par kiberdrošības pārvaldnieku ieceļ vienu personu saskaņā ar NKDL 25. panta pirmo daļu. Atsevišķus kiberdrošības pārvaldības pasākumus (piem., rezerves kopiju vai žurnālfailu veidošanu) var veikt vairāki cilvēki, bet kiberdrošības pārvaldnieks ir atbildīgā persona par veikto pasākumu izpildi.

15. Kādi ir ierobežojumi kiberdrošības pārvaldnieka iecelšanai (piemēram, kvalifikācijas vai drošības prasības)?

Kiberdrošības pārvaldniekam jāatbilst vairākiem kritērijiem, kas detalizēti tiks noteikti gala virzības stadijā esošajā Ministru kabineta noteikumu projektā "Minimālās kiberdrošības prasības", kuri aizstās spēku zaudējušos Ministru kabineta 2015. gada 28. jūlija noteikumus Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".

Minētā Ministru kabineta noteikumu projekta 11. punktā ir noteikti kritēriji kiberdrošības pārvaldnieka iecelšanai attiecībā uz IKT KI īpašniekiem un tiesiskajiem valdītājiem. Savukārt Ministru kabineta noteikumu projekta 12. punktā ir noteiktas prasības būtisko pakalpojumu sniedzējiem, kuri nav IKT KI īpašnieki vai tiesiskie valdītāji un noteikumu projekta 13. punktā ietverti kritēriji kiberdrošības pārvaldnieka iecelšanai svarīgo pakalpojumu sniedzējiem, kuri nav IKT KI īpašnieki vai tiesiskie valdītāji.

16. Vai, piemēram, ministrijai un visām tās padotības iestādēm var tikt iecelts viens kiberdrošības pārvaldnieks?

Saskaņā ar Ministru kabineta noteikumu projekta "Minimālās kiberdrošības prasības" 19. punktu kiberdrošības pārvaldnieks drīkst strādāt arī iestādes (piem., ministrijas) padotības iestādēs bez skaita ierobežojuma, kamēr vien kāda no tām nav IKT KI īpašnieks.

APMĀCĪBAS

17. Sākotnējā minimālo kiberdrošības prasību redakcijā noteikts, ka sākotnējās apmācības (instruktāžas) jānodrošina visiem nodarbinātajiem. Attiecīgi sētnieki, apkopējas utt., kas nestrādās ar IS, tad tik un tā būs jāapgūst sākotnējā instruktāža?

Kiberhigiēnas apmācības organizē nodarbinātajiem, kas strādā ar konkrētā uzņēmuma/iestādes informācijas sistēmām vai ir šo IS reģistrētie lietotāji.

18. Vai tiks organizētas apmācības valsts un pašvaldību iestādēm?

CERT.LV divas reizes gadā organizē apmācības kiberdrošības pārvaldniekiem. Vienlaikus vēršam uzmanību uz to, ka Valsts administrācijas skolā ir pieejams bezmaksas kurss: Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem, lai sniegtu praktiskas zināšanas par kiberhigiēnas jautājumiem publiskās pārvaldes darbiniekiem.

TEHNISKĀS PRASĪBAS

19. Vai IS darbības nodrošināšanai drīkst izmantot atvērtā koda vai bezmaksas programmnodrošinājumu, kuru ir radījusi kopiena (fizisku personu grupa), kuru valstiskā piederība precīzi nav zināma?

Var, bet ir jāizvērtē potenciālie riski pret ieguvumiem. Atvērtā koda būtība – liels loks ar izstrādātājiem un entuziastiem – lielā mērā izslēdz iespēju vienam izstrādātājam/programmētājam kodā ietvert ļaunatūru. Vienlaikus, lai pārliecinātos par koda drošumu, vēlams veikt tā revīziju un pārskatīt atvērtā koda programmatūras konfigurāciju pēc lielāku atjauninājumu veikšanas.

Piegādātājs vai pat lietotājs, ja viņam ir nopietns nodoms balstīt savus risinājumus uz konkrēto atvērtā koda sistēmu vai bibliotēku pats var kļūt par vienu no "entuziastiem", kas attīsta konkrēto atvērto kodu vai var veidot savu atzaru "branch", kuru attīsta un neļauj citiem "entuziastiem" tajā kaut ko pievienot.

20. Ja KI turētāja A klases informācijas sistēma, kas izvietota mākoņpakalpojuma resursos: a) vai šajā gadījumā mākoņpakalpojuma sniedzēja resursi ir uzskatāmi par kritisko infrastruktūru un b) vai mākoņpakalpojuma sniedzējam, piemēram, Microsoft, ir jānodrošina pašnovērtējuma u.c. ziņojumu sagatavošana?

Aicinām iepazīties ar Ministru kabineta noteikumu projekta "Minimālās kiberdrošības prasības" iekļauto informācijas sistēmu gradāciju, lai pārliecinātos, ka tiešām pārvaldāt A klases informācijas sistēmu jaunā regulējuma ietvarā. Jāņem vērā arī tas, ka A klases informācijas sistēma neattiecas tikai uz IKT kritisko infrastruktūru.

Vēršam uzmanību, ka saistībā ar šo tiek izstrādāti citi noteikumi "Noteikumi par informācijas sistēmu izvietošanu un datu centru drošības prasībām". Tajos tiks noteikts kādos Datu centros atļauts izvietot A kategorijas IS.

21. Vai informācijas sistēmas ar A drošības klasi var būt tikai būtisko pakalpojumu sniedzējam? Vai svarīgo pakalpojumu sniedzējiem informācijas sistēmu drošības klase pēc noklusējuma nevar būt augstāka par B drošības klasi?

Aicinām iepazīties ar Ministru kabineta noteikumu projektā "Minimālās kiberdrošības prasības" iekļauto informācijas sistēmu gradāciju, lai pārliecinātos, ka tiešām pārvaldāt A klases informācijas sistēmu jaunā regulējuma ietvarā.

INFORMĀCIJAS IESNIEGŠANA NKDC

22. Kad uzņēmumam jāiesūta sākotnējā informācija, konstatējot, ka tas atbilst NKDL subjekta statusam?

Subjekta statusa atbilstības paziņojuma iesniegšanas termiņš ir **01.04.2025**. vai viena mēneša laikā pēc atbilstības iestāšanās.
Savukārt **01.10.2025.** NKDL subjektiem jāiesniedz pirmais pašvērtējuma ziņojums un jāinformē par kiberdrošības pārvaldnieka iecelšanu.

23. Kā noformēt iesniedzamo informāciju? Vai ir pieejami šabloni?

Veidlapas (gan būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapa, gan domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusa paziņojuma veidlapa, gan paziņojuma par kiberdrošības pārvaldnieku veidlapa, gan pašvērtējuma ziņojuma veidlapa u.c.) iesūtīšanai būs pieejamas Ministra kabineta noteikumu projekta "Minimālās kiberdrošības prasības" pielikumā.

24. Kā nosūta informāciju NKDC?

Izmantojot Latvija.lv, nosūta ziņojumu un veidlapas uz Aizsardzības ministrijas Nacionālā kiberdrošības centra oficiālo e-adresi (NKDC@90000022632).

25. Kā informēt Nacionālo kiberdrošības centru un Satversmes aizsardzības biroju par kiberdrošības pārvaldnieka iecelšanu?

Saskaņā ar NKDL 25. panta otrajā daļā un pārejas noteikumu 10. punktā noteikto par kiberdrošības pārvaldnieka noteikšanu ir jāziņo gan Nacionālajam kiberdrošības centram, gan Satversmes aizsardzības birojam ne vēlāk kā līdz 2025. gada 1. oktobrim. Jāņem vērā, ka IKT KI pārvaldniekam kiberdrošības pārvaldnieka iecelšana jāsaskaņo ar Satversmes aizsardzības biroju, un tam ir noteikta atsevišķa veidlapa Ministru kabineta noteikumu projekta ”Minimālās kiberdrošības prasības” pielikumā.

Veidlapa par kiberdrošības pārvaldnieka noteikšanu subjektā nosūtāma uz Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja oficiālajām e-adresēm, atbilstoši NKDL noteiktajam subjektu uzraudzības dalījumam.

CITI JAUTĀJUMI

26. Kāds ir Ministru kabineta noteikumu projekta par minimālajām kiberdrošības prasībām statuss un kā būtu jārīkojas, ja jaunie noteikumi nav vēl pieņemti, bet iepriekšējais regulējums vairs nav spēkā?

Skaidrojam, lai arī šobrīd vēl nav pieņemti Ministru kabineta noteikumi, kas aizstās spēku zaudējušos Ministru kabineta 2015. gada 28. jūlija noteikumus Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (turpmāk – MK noteikumi Nr. 442), NKDL nosaka, ka gan likums, gan Ministru kabineta noteikumu projekts ”Minimālās kiberdrošības prasības” būs attiecināmi uz NKDL subjektiem. Norādām, ka Ministru kabineta noteikumu projekts šobrīd ir gala virzības procesā un jūnija sākumā ievietots Tiesību aktu projektu portālā, lai virzītu noteikumu projektu izskatīšanai Ministru kabineta sēdē. Aicinām sekot līdzi Ministru kabineta noteikumu projekta turpmākai virzībai saitē: šeit.

Vienlaikus norādām, ka pamatojoties uz Administratīvā procesa likuma 15. panta divpadsmito daļu, NKDL noteikto, kā arī apzinoties to, ka spēku ir zaudējuši MK noteikumi Nr. 442 un Ministru kabineta 2011. gada 1. februāra noteikumi Nr. 100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība", rosinām pieturēties pie MK noteikumu Nr. 442 noteiktajām prasībām, pieņemot, ka MK noteikumu projekts par minimālajām kiberdrošības prasībām tuvākajā laikā tiks pieņemts un arī tajā tiks noteiktas līdzvērtīgas prasības, kādas tika ietvertas MK noteikumos Nr. 442 un tās attieksies uz NKDL subjektiem.

27. Kādi kiberdrošības risku pārvaldības pasākumi ir jāievēro digitālās infrastruktūras pakalpojumu sniedzējiem?

Pamatojoties uz NIS2 direktīvu ir izdota Eiropas Komisijas 2024. gada 17. oktobra *īstenošanas regula (ES) 2024/2690, kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu*

nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka NIS2 Direktīvas piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku.

Ar Īstenošanas regulā noteiktajām prasībām aicinām iepazīties: šeit. Norādām, ka Īstenošanas regulas ir tieši piemērojamas un netiek pārņemtas nacionālajos tiesību aktos.

28. Kāds ir NKDL ietverto subjektu uzraudzības sadalījums?

Atbilstoši NKDL 41. pantā noteiktajam, NKDL subjektu uzraudzību veic NKDC attiecībā uz būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, izņemot informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru un Satversmes aizsardzības birojs attiecībā uz informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru,

Visiem subjektiem sākotnējā reģistrācija jāveic Nacionālajā kiberdrošības centrā līdz 2025. gada 1. aprīlim, bet uzraudzību pār daļu subjektu veiks arī Latvijas Banka un Civilās aviācijas aģentūra, piemēram, lidostas, oficiālos kravu aģentus, visus gaisa pārvadātājus, Latvijas Gaisa satiksmi , Latvijas Hidrometeoroloģijas centru, kā arī uzņēmumus, kas piegādā ēdienu/uzkopj lidmašīnas.

29. Kā interpretējams NKDL 20. panta 11. punkts?

NKDL 20. panta 11. punkts ir iekļauts likumā, pamatojoties uz to, ka *Eiropas Parlamenta un Padomes 2022. gada 14. decembra Direktīvas (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva)* (turpmāk – NIS2 direktīva) 2. panta 2. punkta d) apakšpunkts nosaka, ka NIS2 direktīvas I vai II pielikumā minēto vienību veidiem neatkarīgi no to lieluma piemēro arī tad, ja vienības sniegtā pakalpojuma traucējums varētu izraisīt būtisku sistēmisku risku, jo īpaši nozarēm, kurās šādam traucējumam varētu būt pārrobežu ietekme.

Būtisks sistēmisks risks NIS2 direktīvas kontekstā attiecas uz situācijām, kad organizācijas vai pakalpojuma sniedzēja darbības traucējumi var radīt plašas un nopietnas sekas ne tikai attiecīgajā nozarē, bet arī citās nozarēs vai valstīs. Šāds risks var ietekmēt kritiskās infrastruktūras darbību, sabiedrības drošību, ekonomiku un vispārējo stabilitāti. Piemēram, ja traucējumi kādā nozares pakalpojumā, piemēram, enerģētikā, var novest pie plašiem elektrības padeves pārtraukumiem, tas var ietekmēt ne tikai enerģijas patērētājus, bet arī citas nozares, piemēram, transportu, veselības aprūpi un ražošanu. Tādējādi jau NIS2 direktīva uzsver nepieciešamību nodrošināt drošību un noturību pret šādiem traucējumiem, īpaši nozarēs, kurām ir potenciāls radīt pārrobežu ietekmi.

NKDL 20. panta 11. punkts ir tieši saistīts ar NIS2 direktīvas izpratni par būtisku sistēmisku risku. Gan NIS2 direktīvā, gan NKDL tiek uzsvērta nepieciešamība identificēt un aizsargāt būtiskos pakalpojumu sniedzējus, kuru darbības traucējumi var radīt nopietnas sekas sabiedrībai un valstij. NKDL 20. panta 11. punkts skaidri norāda, ka būtisko pakalpojumu sniedzēja darbības traucējumi var ietekmēt sabiedrības drošību, valsts aizsardzību un

sabiedrības veselību, kā arī radīt būtisku sistēmisku risku, īpaši nozarēs ar potenciālu pārrobežu ietekmi. Tādējādi, gan NIS2 direktīva, gan NKDL uzsver nepieciešamību nodrošināt drošību un noturību pret traucējumiem, kas var ietekmēt plašāku sabiedrību un ekonomiku.

30. Ņemot vērā, ka pašvaldība atbilst būtisko pakalpojumu sniedzēja statusam, vai ir nepieciešams vērtēt katru pašvaldības iestādi atsevišķi saskaņā ar 20. panta 10. punktu?

Par katru NKDL atbilstošo juridisko personu nepieciešams iesūtīt savu statusa paziņojuma veidlapu. Pašvaldībai, vērtējot savas iestādes ir jāņem vērā to juridiskais statuss. Visbiežāk tās ir pastarpinātās pārvaldes iestādes (NKDL 20. panta 5. un 10. punkts).

Neatradi atbildi uz interesējošo jautājumu? Raksti uz NIS2@mod.gov.lv