

Stājas spēkā jaunas informācijas sistēmu izvietošanas un datu centru drošības prasības



Nacionālais
kiberdrošības
centrs



AIZSARDZĪBAS
MINISTRIJA



2026. gada 1. oktobrī

stājas spēkā Ministru kabineta noteikumi

“Informācijas sistēmu izvietošanas un datu centru drošības prasības”.

Tie nosaka vienotas prasības Nacionālās kiberdrošības likuma (NKDL) subjektu informācijas sistēmu izvietošanai datu centros, datu centru drošībai un atbilstības novērtēšanai, kā arī telemetrijas datu pieejamībai kompetentajām kiberincidentu novēršanas institūcijām.

Kas mainās NKDL subjektiem?

1.

Ģeogrāfiskais tvērums informācijas sistēmu izvietošanai



Ja noteikumos nav paredzēts citādi, NKDL subjekta informācijas sistēmu vai tās daļu var izvietot datu centrā NATO, Eiropas Savienības, Eiropas Brīvās tirdzniecības asociācijas (EBTA) dalībvalstī vai NATO sadarbības valstī Indijas un Klusā okeāna reģionā (IP4), un arī datu apstrādei jānotiek šo valstu teritorijā.

2.

Stingrākas prasības A klases informācijas sistēmām



Ja A klases informācijas sistēma tiek izvietota datu centrā ārpus subjekta paša IKT infrastruktūras un IKT kritiskās infrastruktūras gadījumā arī iekšējā datu centrā, datu centra atbilstībai jābūt apliecinātai noteikumos paredzētajā kārtībā.

Izņēmuma gadījumos iespējama atkāpe, ja ir dokumentēta nepieciešamība, izvērtēti riski, noteikti risku mazināšanas pasākumi un saņemts Nacionālā kiberdrošības centra saskaņojums.

3.

Datu centra atbilstība būs jāpārbauda



Atbilstību varēs apliecināt ar datu centra auditora atzinumu, noteikumos atzītu sertifikātu vai citu atbilstības dokumentu.

Ja atbilstību apliecina auditora atzinums, tas jāatjauno ne retāk kā reizi divos gados.

4.

Jāpārskata līgumi ar datu centru pakalpojumu sniedzējiem



Slēdzot ārpakalpojuma līgumu par informācijas sistēmas izvietošanu, subjektam līgumā jāparedz datu centra operatora pienākums ievērot jaunās prasības, kā arī jānodrošina atbilstoša datu centra un datu apstrādes atrašanās vieta.

5.

Informācija par izmantotajiem datu centriem pašvērtējumā



Subjekts pašvērtējuma ziņojumā informēs kompetento uzraugošo iestādi par datu centru, kurā izvietota tā informācijas sistēma, un datu centra atbilstību noteikumu prasībām.

6.

Telemetrijas datu pieejamība A klases sistēmām



A klases informācijas sistēmu īpašniekiem un tiesiskajiem valdītājiem jānodrošina kompetentajai kiberincidentu novēršanas institūcijai piekļuve telemetrijas datu pirmavotam un noteiktajos gadījumos datu centra operatora apstrādātiem datiem reāllaikā.

Kas jādara ar jau izvietotām A klases sistēmām?

01.10.2026.

NOTEIKUMI STĀJAS SPĒKĀ



Jaunus A klases informācijas sistēmu izvietojumus drīkst uzsākt tikai atbilstoši jaunajām prasībām, izņemot noteikumos īpaši paredzētos gadījumus.

Līdz 31.12.2026.



- Jāinformē datu centra operators par tajā jau izvietotām A klases informācijas sistēmām.
- IKT kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem jāinformē arī Satversmes aizsardzības birojs.
- Ja izvietojums neatbilst prasībām, jā sagatavo atbilstības nodrošināšanas plāns un jānodrošina risku pārvaldība.

Līdz 31.12.2027.



Esošu prasībām neatbilstošu A klases informācijas sistēmu izvietojumu, ievērojot pārejas nosacījumus un pārvaldot riskus, var turpināt izmantot ne ilgāk kā līdz 2027. gada 31. decembrim. Līdz šim datumam jānodrošina pilnīga atbilstība.

Kas subjektam jāizdara tagad?

Līdz 2026. gada 31. decembrim

1.



Apzināt, kuros datu centros ir izvietotas tā informācijas sistēmas un to daļas.

2.



Identificēt A klases informācijas sistēmas un pārbaudīt to izvietojuma atbilstību jaunajām prasībām.

3.



Pārbaudīt datu centru atbilstības apliecinājumus un noslēgtos ārpakalpojuma līgumus.

4.



Par A klases informācijas sistēmām, kas datu centrā izvietotas jau pirms noteikumu spēkā stāšanās, izpildīt noteikumos paredzētos informēšanas pienākumus.

5.



Ja esošais A klases informācijas sistēmas izvietojums neatbilst prasībām, līdz 2026. gada 31. decembrim sagatavot atbilstības nodrošināšanas plānu.

Svarīgi!



Mākoņdatošanas pakalpojuma izmantošana neatbrīvo NKDL subjektu no pienākuma pārliecināties, ka pakalpojumā izmantotie datu centri atbilst noteikumu prasībām.

Rezultāts



Drošāka informācijas sistēmu izvietošana, augstāka datu centru drošība un labāka sagatavotība kiberincidentu novēršanai.