Izdevējs: Saeima
Veids: likums
Pieņemts: 20.06.2024.
Stājas spēkā: 01.09.2024.

Publicēts:
Latvijas Vēstnesis, 128A, 04.07.2024.
OP numurs: 2024/128A.1

Attēlotā redakcija: 01.10.2026. - ...

Grozījumi:

04.06.2026. likums / LV, 115, 17.06.2026. / Stājas spēkā 18.06.2026.

Saeima ir pieņēmusi un Valsts prezidents izsludina šādu likumu:

Nacionālās kiberdrošības likums

I nodaļa
Vispārīgie noteikumi

1. pants. Likumā lietotie termini

Likumā ir lietoti šādi termini:

1) **augstākā līmeņa domēnu vārdu reģistra uzturētājs** — institūcija, kam deleģēts konkrēts augstākā līmeņa domēns un kas atbild par šā augstākā līmeņa domēna pārvaldību, tai skaitā veic domēnu vārdu reģistrāciju šajā augstākā līmeņa domēnā un nodrošina augstākā līmeņa domēna tehnisko darbību, kā arī tā vārdu serveru darbību, datubāzu uzturēšanu un augstākā līmeņa domēna zonas datņu sadalīšanu starp vārdu serveriem neatkarīgi no tā, vai kādu no minētajām darbībām veic pati institūcija, izņemot situācijas, kad tā augstākā līmeņa domēnu vārdus izmanto tikai savām vajadzībām, vai veic ārpakalpojuma sniedzējs;

2) **datu centrs** — telpa vai telpu komplekss, kas paredzēts informācijas tehnoloģiju un tīkla iekārtu centralizētai izvietošanai, savstarpējai savienošanai un darbībai un kas nodrošina datu uzglabāšanas, apstrādes un pārsūtīšanas (transportēšanas) pakalpojumus, kā arī visas elektroenerģijas sadalei un klimata kontrolei nepieciešamās iekārtas un infrastruktūras;

3) **domēnu vārdu reģistrācijas pakalpojumu sniedzējs** — reģistratūra vai pilnvarotā persona, kas darbojas reģistratūras vārdā, piemēram, privātuma vai pilnvarotās reģistrācijas pakalpojumu sniedzējs vai tālākpārdevējs;

4) **domēnu vārdu sistēma** — hierarhiska, sadalīta vārdu sistēma, kas nodrošina iespēju identificēt interneta pakalpojumus un resursus, ļaujot galalietotāju ierīcēm izmantot interneta maršrutēšanas un savienojumu pakalpojumus, lai piekļūtu šiem pakalpojumiem un resursiem;

5) **gandrīz noticis kiberincidents** — notikums, kurš būtu varējis apdraudēt apstrādātus datus vai tīklu un informācijas sistēmu piedāvāto vai ar tīklu un informācijas sistēmu starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika sekmīgi novērsta vai kurš neīstenojās;

6) **ievainojamība** — informācijas un komunikācijas tehnoloģiju vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam;

7) **informācijas un komunikācijas tehnoloģijas** — tehnoloģijas, kuras tām paredzēto uzdevumu izpildei ar

tehnisko līdzekļu palīdzību veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, izmainīšanu, dzēšanu, glabāšanu, attēlošanu, pārsūtīšanu vai pārraidīšanu (turpmāk — elektroniskā apstrāde), un nodrošina tehnoloģijas izmantotāju savstarpējo komunikāciju;

8) **interneta plūsmu apmaiņas punkts** — tīkla infrastruktūra, kas ļauj nodrošināt vairāk nekā divu neatkarīgu tīklu (autonomu sistēmu) starpsavienojumu galvenokārt nolūkā atvieglot interneta datu plūsmu apmaiņu, nodrošina starpsavienojumu tikai autonomām sistēmām, nepieprasa, lai interneta datu plūsma starp jebkurām divām iesaistītām sistēmām izietu cauri jebkurai trešai autonomai sistēmai, un nedz maina, nedz arī citādi ietekmē šādu datu plūsmu;

9) **kiberapdraudējums** — jebkādi iespējami apstākļi, notikums vai darbība, kas atbilst Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa regulas (ES) 2019/881 par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (turpmāk — regula 2019/881) 2. panta 8. punktā noteiktajai definīcijai;

10) **kiberdrošība** — darbības, kas atbilst regulas 2019/881 2. panta 1. punktā noteiktajai definīcijai;

11) **kiberdrošības incidents** (turpmāk — kiberincidents) — notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību;

12) **kiberhigiēna** — ikdienas prakšu un paradumu kopums, kura mērķis ir mazināt kiberapdraudējumus, nodrošināt datu aizsardzību un saglabāt informācijas un komunikācijas tehnoloģiju resursu pieejamību, integritāti un konfidencialitāti;

13) **kiberincidenta risināšana** — darbību un procedūru kopums, kura mērķis ir novērst, atklāt, analizēt un ierobežot kiberincidentu vai reaģēt uz kiberincidentu un to pārvarēt;

14) **kiberrisks** — kiberincidenta izraisītu zaudējumu vai pakalpojumu traucējumu iespējamība, ko izsaka kā šādu zaudējumu vai traucējumu ietekmes un minētā incidenta varbūtības apvienojumu;

15) **kiberuzbrukums** — aktīva uzbrucēja rīcība, kuras mērķis ir ietekmēt datu un informācijas un komunikācijas tehnoloģiju pakalpojumu konfidencialitāti, integritāti vai pieejamību;

16) **liels saimnieciskās darbības veicējs** — juridiskā vai fiziskā persona vai šādu personu apvienība, kas veic saimniecisko darbību Latvijas Republikā un atbilst vismaz vienai no šādām pazīmēm:

a) saimnieciskās darbības veicējs nodarbina vismaz 250 nodarbinātos,

b) saimnieciskās darbības veicēja pēdējā finanšu gada kopējais neto apgrozījums pārsniedz 50 miljonus *euro* vai gada bilances kopsumma pārsniedz 43 miljonus *euro*;

17) **nacionālā kiberdrošības stratēģija** — stratēģiskās plānošanas dokuments, kas nosaka kiberdrošības politikas veidošanas pamatprincipus, mērķi un stratēģiskās prioritātes;

18) **nozīmīgs kiberapdraudējums** — kiberapdraudējums, kas, ņemot vērā tā tehniskās pamatīpašības, var nopietni ietekmēt kādas juridiskās vai fiziskās personas tīklu un informācijas sistēmas vai šīs personas sniegto pakalpojumu saņēmējus, radot ievērojamu materiālu vai nemateriālu kaitējumu;

19) **nozīmīgs kiberincidents** — pārrobežu kiberincidents vai tāds kiberincidents, kam ir ietekme uz sniegtā pakalpojuma nepārtrauktību vai sabiedrības interesēm un kas atbilst Ministru kabineta noteiktajiem kritērijiem;

20) **pakalpojumatteices kiberuzbrukums** — uzbrukums, kas tiek izdarīts pret pakalpojuma sniedzēja infrastruktūru nolūkā negatīvi ietekmēt pakalpojuma pieejamību;

21) **pārrobežu kiberincidents** — incidents, kas izraisa traucējumus tādā līmenī, kurš pārsniedz dalībvalsts spēju uz to reaģēt, vai kam ir būtiska ietekme uz vismaz divām dalībvalstīm;

22) **tīklu un informācijas sistēma**:

a) elektronisko sakaru tīkls,

b) jebkura ierīce vai tāda savstarpēji savienotu vai saistītu ierīču grupa, no kurām viena vai vairākas ierīces atbilstoši programmai veic digitālu datu automātisku apstrādi,

c) digitāli dati, ko šā punkta "a" un "b" apakšpunktā minētie elementi glabā, apstrādā, iegūst vai sūta to darbības, izmantošanas, aizsardzības un uzturēšanas nolūkā;

23) **tīklu un informācijas sistēmu drošība** — tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties visiem notikumiem, kas var apdraudēt elektroniski apstrādājamo datu konfidencialitāti, integritāti un pieejamību vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos pakalpojumus;

24) **uzticamības pakalpojums** — elektronisks pakalpojums Eiropas Parlamenta un Padomes 2014. gada 23. jūlija regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ direktīvu 1999/93/EK 3. panta 16. punkta izpratnē;

25) **vidējs saimnieciskās darbības veicējs** — juridiskā vai fiziskā persona vai šādu personu apvienība, kas veic saimniecisko darbību Latvijas Republikā un atbilst visām šādām pazīmēm:

a) saimnieciskās darbības veicējs nodarbina līdz 249 nodarbinātajiem;

b) saimnieciskās darbības veicēja pēdējā finanšu gada kopējais neto apgrozījums ir vismaz 10 miljoni *euro*, bet nepārsniedz 50 miljonus *euro* vai gada bilances kopsumma ir vismaz 10 miljoni *euro*, bet nepārsniedz 43 miljonus *euro*;

26) **vienotais valsts interneta plūsmu apmaiņas punkts** — pastāvīgs fiziskās infrastruktūras un pakalpojumu kopums, kas tiek izveidots un uzturēts, lai nodrošinātu vienotu valsts interneta plūsmu apmaiņu.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

2. pants. Likuma mērķis

Likuma mērķis ir:

1) uzlabot informācijas un komunikācijas tehnoloģiju drošību, tai skaitā nosakot prasības būtisko pakalpojumu un svarīgo pakalpojumu sniegšanai un saņemšanai, kā arī informācijas un komunikācijas tehnoloģiju darbībai;

2) noteikt kiberdrošības nodrošināšanas kārtību, paredzot atbildības sadalījumu un Nacionālā kiberdrošības centra kompetenci, sadarbības ietvarus un kiberdrošības veicināšanas uzdevumus;

3) veicināt kiberdrošības pasākumu īstenošanu tā, lai varētu laikus prognozēt un novērst, kā arī pārvarēt kiberapdraudējumu un likvidēt tā sekas, pēc iespējas nodrošinot pakalpojumu konfidencialitātes, integritātes un pieejamības nepārtrauktību.

3. pants. Likuma darbības joma

(1) Likums attiecas uz:

1) būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem (turpmāk visi kopā — subjekti);

2) tiešās un pastarpinātās pārvaldes iestādēm, atvasinātām publiskajām personām un citām valsts institūcijām (turpmāk visas kopā — valsts un pašvaldību institūcijas), izņemot valsts drošības iestādes;

3) privāto tiesību juridiskajām personām;

4) šajā likumā noteiktajos gadījumos — fiziskajām personām, kas piedalās koordinētas ievainojamību atklāšanas procesā.

(2) Likums neattiecas uz elektronisko sakaru tīklos pārraidāmās informācijas saturu, tostarp uz informācijas sabiedrības pakalpojumu saturu un audiovizuālajiem darbiem, ja tie netiek izmantoti kā kiberincidentu sastāvdaļa.

(3) Likums attiecas uz tām finanšu vienībām Eiropas Parlamenta un Padomes 2022. gada 14. decembra regulas

(ES) 2022/2554 par finanšu nozares digitālās darbības noturību un ar ko groza regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) Nr. 2016/1011 (turpmāk — regula 2022/2554) 2. panta 2. punkta izpratnē, kuras atbilstoši šā likuma 20. pantam ir būtisko pakalpojumu sniedzēji, ciktāl regula 2022/2554 vai citi normatīvie akti nenosaka citas prasības jautājumos par finanšu vienību kiberdrošības prasībām, kiberapdraudējumu un risku pārvaldību (tostarp trešo pušu pakalpojumu sniedzēju risku pārvaldību), darbības noturību un nepārtrauktību, atbildīgo par kiberdrošības pārvaldības noteikšanu, testēšanu, rīcību kiberincidenta gadījumā, incidentu ziņošanu un subjektu uzraudzību.

(4) Ja konkrēto nozari regulējošie Eiropas Savienības tiesību akti paredz būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējiem pienākumu veikt kiberdrošības risku pārvaldības pasākumus vai ziņot par kiberincidentiem un ja šādas prasības ietekmes ziņā ir vismaz līdzvērtīgas šajā likumā noteiktajiem pienākumiem, attiecīgos šā likuma nosacījumus, tostarp par subjektu uzraudzību, šiem subjektiem nepiemēro. Ja konkrēto nozari regulējošie Eiropas Savienības tiesību akti neattiecas uz visiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem konkrētajā nozarē, attiecīgās šā likuma prasības turpina piemērot būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, uz kuriem neattiecas minētie Eiropas Savienības tiesību akti.

(5) Šā panta ceturtajā daļā minētās prasības uzskata par ietekmes ziņā līdzvērtīgām šajā likumā noteiktajiem pasākumiem, ja tās atbilst vismaz vienai no šādām pazīmēm:

1) kiberdrošības risku pārvaldības pasākumi ietekmes ziņā ir vismaz līdzvērtīgi šā likuma 26., 27. un 28. pantā noteiktajām prasībām;

2) konkrēto nozari regulējošais Eiropas Savienības tiesību akts paredz šā likuma 9. pantā noteiktajām kiberincidentu novēršanas institūcijām, šā likuma 13. pantā noteiktajām kompetentajām institūcijām un šā likuma 4. panta pirmajā daļā noteiktajai nacionālajai kompetentajai institūcijai tūlītēju un attiecīgā gadījumā automātisku un tiešu piekļuvi paziņojumiem par kiberincidentiem, un prasības ziņot par kiberincidentiem ietekmes ziņā ir vismaz līdzvērtīgas šā likuma 34. pantā noteiktajām prasībām.

(6) Likums neattiecas uz tādiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, kuri atbilst visiem šādiem nosacījumiem:

1) pakalpojumu sniedzējs ir reģistrēts Eiropas Savienības dalībvalstī;

2) pakalpojumu sniedzējs Latvijas Republikā sniedz šā likuma 20. panta 1., 2. punktā un 8. punkta "s", "t", "u" un "v" apakšpunktā minētos būtiskos pakalpojumus vai šā likuma 21. panta pirmās daļas 2. punkta "l", "m" un "n" apakšpunktā minētos svarīgos pakalpojumus;

3) pakalpojumu sniedzējs Latvijas Republikā nesniedz šīs daļas 2. punktā neminētos būtiskos pakalpojumus vai svarīgos pakalpojumus;

4) pakalpojumu sniedzējs nav informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs;

5) pakalpojumu sniedzēja galvenā reģistrācijas vieta Eiropas Savienībā nav Latvijas Republika.

(7) Likums neattiecas uz tādiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, kuri nav reģistrēti Eiropas Savienībā un kuru pārstāvja galvenā reģistrācijas vieta Eiropas Savienībā nav Latvijas Republika.

(8) Šā likuma izpratnē par galveno reģistrācijas vietu uzskata:

1) Eiropas Savienības dalībvalsti, kurā galvenokārt tiek pieņemti lēmumi saistībā ar pakalpojumu sniedzēja kiberdrošības risku pārvaldības pasākumiem;

2) ja šīs daļas 1. punktā minēto valsti nav iespējams noteikt, — Eiropas Savienības dalībvalsti, kurā attiecībā uz pakalpojumu sniedzēju tiek īstenotas kiberdrošības operācijas;

3) ja šīs daļas 2. punktā minēto valsti nav iespējams noteikt, — Eiropas Savienības dalībvalsti, kurā attiecīgajam pakalpojumu sniedzējam ir vislielākais nodarbināto skaits Eiropas Savienībā.

(9) Šā panta astotā daļa neattiecas uz gadījumiem, kad Nacionālais kiberdrošības centrs pēc citas Eiropas Savienības dalībvalsts kompetentās iestādes pieprasījuma īsteno šajā likumā noteiktos uzraudzības un izpildes panākšanas pasākumus attiecībā uz šajā Eiropas Savienības dalībvalstī reģistrēto būtisko pakalpojumu sniedzēju, kurš sniedz pakalpojumus Latvijas Republikā vai kura valdījumā ir tīkls vai informācijas sistēma, kas atrodas Latvijas

Republikā.

(10) Likums neattiecas uz elektronisko sakaru komersantiem, kuri nenodrošina elektronisko sakaru tīklu un nesniedz elektronisko sakaru pakalpojumus Latvijas Republikā.

(11) Likums neattiecas uz tādiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, kuri ir citas Eiropas Savienības dalībvalsts valsts institūcijas.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

II nodaļa
Par kiberdrošību atbildīgās institūcijas

4. pants. Nacionālais kiberdrošības centrs

Nacionālais kiberdrošības centrs ir nacionālā kompetentā institūcija, kas darbojas Aizsardzības ministrijā kā vienotais kontaktpunkts kiberdrošības jautājumos un īsteno nacionālo kiberdrošības pārraudzību, veido nacionālās kiberdrošības rīcībpolitikas iniciatīvas un atbilstoši kompetencei veido un īsteno starptautisko sadarbību.

5. pants. Nacionālā kiberdrošības centra uzdevumi

(1) Nacionālajam kiberdrošības centram ir šādi uzdevumi:

1) koordinēt sadarbību kiberdrošības jautājumos ar citu Eiropas Savienības dalībvalstu kompetentajām iestādēm un vienotajiem kontaktpunktiem, Eiropas Komisiju, Eiropas Savienības Kiberdrošības aģentūru un citām kompetentajām Eiropas Savienības institūcijām;

2) sadarboties ar būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem to informācijas sistēmu drošības līmeņa noteikšanai;

3) īstenot uzraudzības funkcijas, tostarp uzraudzīt, kā būtisko pakalpojumu un svarīgo pakalpojumu sniedzēji izpilda tiem šajā likumā noteiktos pienākumus;

4) izvērtēt būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju kiberrisku pārvaldības pasākumu atbilstību normatīvajos aktos noteiktajām prasībām;

5) uzraudzīt publisko elektronisko sakaru tīklu drošības prasību ievērošanu;

6) uzturēt valsts iestāžu apkopoto un pašidentificēto būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju sarakstu, apstiprināt to, kā arī sniegt kompetentajām Eiropas Savienības institūcijām apkopotu un pēc nepieciešamības anonimizētu informāciju par identificētajiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem;

7) nodrošināt Nacionālās kiberdrošības padomes un Digitālās drošības uzraudzības komitejas sekretariāta funkcijas;

8) izvērtēt valsts informācijas sistēmu un institūciju informācijas sistēmu attīstības projektu atbilstību minimālajām kiberdrošības prasībām, ievērojot Valsts informācijas sistēmu likumu;

9) nodrošināt vienotā valsts interneta plūsmu apmaiņas punkta darbību, kā arī sadarbībā ar valsts drošības iestādēm koordinēt vienotā valsts interneta plūsmu apmaiņas punkta pakalpojumu saņemšanu;

10) sadarbībā ar valsts pārvaldes iestādēm, valsts drošības iestādēm un privātā sektora pārstāvjiem izstrādāt nacionālo kiberdrošības stratēģiju un ne vēlāk kā trīs mēnešus pēc nacionālās kiberdrošības stratēģijas apstiprināšanas informēt par to Eiropas Komisiju;

11) nodrošināt Nacionālā kiberincidentu krīzes vadības plāna izstrādi un integrēt to valsts aizsardzības plānos, līdzdarboties Eiropas Savienības Kiberkrīžu sadarbības organizācijas tīklā;

12) sadarboties ar Eiropas Savienības Kiberdrošības aģentūru un nekavējoties informēt to par pārrobežu kiberincidentiem, kas skar būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējus, kā arī reizi trijos mēnešos sniegt tai ziņojumu par visiem notikušajiem nozīmīgiem kiberincidentiem, kiberincidentiem, gandrīz notikušiem kiberincidentiem un kiberapdraudējumiem, par kuriem subjekti ir paziņojuši;

13) sadarboties ar citu Eiropas Savienības dalībvalstu kompetentajām iestādēm, tostarp pēc kiberincidentu novēršanas institūcijas pieprasījuma nosūtīt tām saņemto informāciju par nozīmīgiem kiberincidentiem, kas skar šīs Eiropas Savienības dalībvalstis;

14) koordinēt pārrobežu kiberincidenta risināšanu sadarbībā ar kiberincidentu novēršanas institūcijām, Eiropas Savienības, ārvalstu un starptautiskām kompetentajām institūcijām;

15) sadarboties ar Eiropas Savienības tīklu un informācijas sistēmu sadarbības grupu (turpmāk — NIS sadarbības grupa) un īstenot ar to saistītos uzdevumus;

16) īstenot Eiropas Parlamenta un Padomes 2021. gada 20. maija regulā (ES) 2021/887, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu Nacionālajam koordinācijas centram noteiktās tiesības un pienākumus;

17) uzturēt vienotu Latvijas kibertelpā notiekošo darbību ataino jumu, izņemot tajā pārraidītās informācijas saturu;

18) informēt sabiedrību par aktuālajiem kiberapdraudējumiem;

19) nodrošināt drošības operāciju centru darbību Ministru kabineta noteiktajām prasībām atbilstošajos datu centros;

20) atbilstoši kompetencei piedalīties koordinētā ievainojamību atklāšanā un novēršanā;

21) ja nepieciešams, informēt Eiropas Savienības Kiberdrošības aģentūru par ziņām, kas iekļaujamas ievainojamību datubāzē;

22) gadījumos, kad ievainojamība skar arī citu Eiropas Savienības dalībvalsti, sadarboties ar šīs dalībvalsts kompetentajām institūcijām;

23) ja nepieciešams, piedalīties Eiropas Savienības dalībvalstu kiberdrošības kapacitātes un rīcībpolitikas izvērtējumos neatkarīgā eksperta statusā.

(2) Šā panta pirmās daļas 2., 3. un 4. punktā minētos uzdevumus Nacionālais kiberdrošības centrs īsteno tikai attiecībā uz tiem būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, kuri nav informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji.

(3) Šā panta pirmās daļas 17., 18., 19., 20., 21., 22. un 23. punktā minēto Nacionālā kiberdrošības centra uzdevumu izpildi Aizsardzības ministrija deleģē Latvijas Universitātes Matemātikas un informātikas institūtam, noslēdzot deleģēšanas līgumu.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

6. pants. Nacionālā kiberdrošības centra tiesības

Nacionālajam kiberdrošības centram ir šādas tiesības:

1) pieprasīt un saņemt no būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem informāciju par to īpašumā un valdījumā esošajām informācijas un komunikācijas tehnoloģijām, par to īstenotajiem un plānotajiem kiberdrošības un kiberrisku pārvaldības pasākumiem, kā arī par kiberincidentiem, gandrīz notikušiem kiberincidentiem, kiberapdraudējumiem un ievainojamībām;

2) pieprasīt un saņemt no valsts un pašvaldību institūcijām to rīcībā esošo informāciju par būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem;

3) sniegt norādījumus, lai nodrošinātu šajā likumā būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem noteikto pienākumu izpildi;

4) pieņemt lēmumu (arī izdot administratīvo aktu), lai nodrošinātu šajā likumā noteikto pienākumu izpildi vai novērstu nacionālās drošības apdraudējumu vai kiberapdraudējumu;

5) piemērot soda naudu un veikt tiesiskā pienākuma piespiedu izpildi;

6) pieprasīt un saņemt no datu centru operatoriem informāciju par tiem noteikto pienākumu izpildi.

7. pants. Satversmes aizsardzības biroja uzdevumi

Satversmes aizsardzības birojam ir šādi uzdevumi:

1) īstenot uzraudzības funkcijas, tostarp uzraudzīt, kā informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieki un tiesiskie valdītāji izpilda tiem šajā likumā noteiktos pienākumus;

2) sadarboties ar informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem to informācijas sistēmu drošības līmeņa noteikšanai;

3) koordinēt pārrobežu kiberincidenta risināšanu sadarbībā ar kiberincidentu novēršanas institūcijām;

4) izvērtēt informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieku un tiesisko valdītāju īstenojamo kiberrisku pārvaldības pasākumu atbilstību normatīvajos aktos noteiktajām prasībām.

8. pants. Satversmes aizsardzības biroja tiesības

Satversmes aizsardzības birojam ir šādas tiesības:

1) pieprasīt un saņemt no informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem informāciju par to īpašumā un valdījumā esošajām informācijas un komunikācijas tehnoloģijām, par to īstenotajiem un plānotajiem kiberdrošības un kiberrisku pārvaldības pasākumiem, kā arī par kiberincidentiem, gandrīz notikušiem kiberincidentiem, kiberapdraudējumiem un ievainojamībām;

2) sniegt norādījumus, lai nodrošinātu šajā likumā informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem noteikto pienākumu izpildi vai novērstu nacionālās drošības apdraudējumu;

3) pieņemt lēmumu (arī izdot administratīvo aktu), lai nodrošinātu šajā likumā noteikto pienākumu izpildi vai novērstu nacionālās drošības apdraudējumu vai kiberapdraudējumu;

4) piemērot soda naudu un veikt tiesiskā pienākuma piespiedu izpildi.

9. pants. Kiberincidentu novēršanas institūcijas

(1) Kiberincidentu novēršanas institūcijas ir institūcijas, kas sniedz valsts un pašvaldību institūcijām atbalstu kiberdrošības jomā, uztur un aktualizē informāciju par kiberapdraudējumiem un sniedz fiziskajām un juridiskajām personām atbalstu kiberincidentu novēršanā.

(2) Kiberincidentu novēršanas institūciju uzdevumus veic:

1) Militārās izlūkošanas un drošības dienests — attiecībā uz Aizsardzības ministriju, tās padotībā esošajām iestādēm un Nacionālajiem bruņotajiem spēkiem;

2) Latvijas Universitātes Matemātikas un informātikas institūts — attiecībā uz valsts un pašvaldību institūcijām (izņemot valsts drošības iestādes un šīs daļas 1. punktā minētās institūcijas), kā arī privāto tiesību juridiskajām personām.

(3) Latvijas Universitātes Matemātikas un informātikas institūts tam noteiktos uzdevumus izpilda un tiesības īsteno saskaņā ar šo likumu aizsardzības ministra funkcionālajā padotībā, ko īsteno pakļautības formā.

(4) Ministru kabinets nosaka prasības kiberincidentu novēršanas institūcijām.

10. pants. Kiberincidentu novēršanas institūciju uzdevumi

Kiberincidentu novēršanas institūcijām ir šādi uzdevumi:

1) veikt valsts līmenī nozīmīgu kiberapdraudējumu, ievainojamību un kiberincidentu analīzi;

2) reaģēt uz kiberincidentiem, pēc subjekta pieprasījuma sniegt atbalstu kiberincidenta risināšanā vai koordinēt kiberincidenta novēršanu;

3) brīdināt un sniegt Nacionālajam kiberdrošības centram, Satversmes aizsardzības birojam, subjektiem un, ja nepieciešams, citām iestādēm informāciju par aktuālajiem nozīmīgiem kiberincidentiem, kiberincidentiem, gandrīz notikušiem kiberincidentiem, kiberapdraudējumiem un ievainojamībām;

4) organizēt izglītojošus pasākumus, veikt analītisko un pētniecisko darbu un rīkot tematisku apmācību kiberdrošības jomā;

5) sniegt valsts institūcijām atbalstu valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas un komunikācijas tehnoloģiju jomā;

6) sadarboties ar Eiropas Savienības, ārvalstu un starptautisko organizāciju kompetentajām iestādēm un kiberincidentu novēršanas institūcijām, līdzdarboties Eiropas Savienības dalībvalstu kiberdrošības incidentu novēršanas institūciju tīklā (turpmāk — CSIRT tīkls);

7) nekavējoties informēt Nacionālo kiberdrošības centru un valsts drošības iestādes par nozīmīgu kiberincidentu, kā arī informēt citas Eiropas Savienības dalībvalsts kompetento iestādi par nozīmīgu kiberincidentu, kas ietekmē būtiska pakalpojuma vai svarīga pakalpojuma darbības nepārtrauktību konkrētajā dalībvalstī;

8) informēt Nacionālo kiberdrošības centru un Satversmes aizsardzības biroju par konstatēto subjekta informācijas un komunikācijas tehnoloģiju neatbilstību normatīvajiem aktiem, kuri nosaka kiberdrošības prasības, kā arī par konstatētajiem gadījumiem, kad subjekts nav ziņojis par kiberincidentu;

9) atbilstoši kompetencei sadarboties ar valsts un privātā sektora institūcijām, lai sekmētu to kiberdrošību un kibernoturību, kā arī sadarboties ar subjektu kopienām un apmainīties ar informāciju par aktuālajiem kiberapdraudējumiem;

10) pēc subjekta pieprasījuma veikt subjekta tīklu un informācijas sistēmu proaktīvu skenēšanu, lai atklātu ievainojamības ar iespējamu būtisku ietekmi;

11) veikt citus tām normatīvajos aktos noteiktos pienākumus.

11. pants. Kiberincidentu novēršanas institūciju tiesības

(1) Kiberincidentu novēršanas institūcijām ir šādas tiesības:

1) pieprasīt un saņemt no subjektiem, valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām:

a) informāciju par ieviestajām informācijas un komunikācijas tehnoloģiju (tostarp tīklu un informācijas sistēmu) drošības prasībām, identificētajām ievainojamībām un kiberapdraudējumiem,

b) tehnisko informāciju par notikušu vai notiekošu kiberincidentu (informācija par kiberincidenta apjomu, kiberincidentu izraisījušu kaitniecisku programmatūru datnes, ievainojamību apraksts, kiberincidenta novēršanai veiktie tehniskie pasākumi, informācija par kaitnieku darbībām vai cita tehniskā informācija, ieskaitot IP adreses);

2) pēc abpusējas vienošanās iegūt no subjektiem, valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām tiešsaistes datu plūsmu kiberapdraudējuma identificēšanai un novēršanai;

3) veikt pārbaudes būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju informācijas un komunikācijas tehnoloģiju infrastruktūrā, izņemot informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru;

4) pēc Satversmes aizsardzības biroja pieprasījuma veikt pārbaudes informācijas un komunikācijas tehnoloģiju kritiskajā infrastruktūrā;

5) lūgt, lai Nacionālais kiberdrošības centrs nosūta citas Eiropas Savienības dalībvalsts kompetentajai institūcijai, NIS sadarbības grupai, CSIRT tīklam vai Eiropas Savienības Kiberdrošības aģentūrai informāciju par kiberincidentu, kuram ir ietekme uz būtisko pakalpojumu vai svarīgo pakalpojumu sniegšanu konkrētajā dalībvalstī;

6) veikt subjektu publiski pieejamo tīklu un informācijas sistēmu proaktīvu mērķsistēmu un tīklu neietekmējošu skenēšanu, lai atklātu ievainojamības vai nedrošas konfigurācijas un par tām informētu attiecīgos subjektus.

(2) Šā panta pirmās daļas 6. punktā minēto skenēšanu kiberincidentu novēršanas institūcija veic tādā veidā, lai tā neietekmētu attiecīgā subjekta pakalpojumu sniegšanas nepārtrauktību. Skenēšanu informācijas un komunikācijas kritiskajā infrastruktūrā veic pēc saskaņošanas ar Satversmes aizsardzības biroju.

12. pants. Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja izdotie lēmumi, pieprasījumi un uzliktie tiesiskie pienākumi

(1) Ja lēmuma, pieprasījuma vai tiesiskā pienākuma adresāts ir privāto tiesību juridiskā persona, tad Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja lēmums, pieprasījums vai uzliktais tiesiskais pienākums ir administratīvais akts.

(2) Ja lēmuma, pieprasījuma vai tiesiskā pienākuma adresāts ir tiešās vai pastarpinātās pārvaldes iestāde, cita valsts institūcija vai atvasināta publiskā persona, tad Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja lēmums, pieprasījums vai uzliktais tiesiskais pienākums nav administratīvais akts.

(3) Ministru kabinets nosaka kārtību ziņošanai par tiešās vai pastarpinātās pārvaldes iestādēm, citām valsts institūcijām un atvasinātām publiskajām personām, kuras nepilda šajā likumā minētos lēmumus, pieprasījumus vai tām uzliktos tiesiskos pienākumus.

(4) Šā panta otrajā daļā minēto lēmumu un pieprasījumu izdod un tiesisko pienākumu uzliek rakstveidā, ietverot tajā šādu informāciju:

1) iestādes nosaukumu un adresi;

2) adresātu;

3) faktu konstatējumu;

4) lēmuma, pieprasījuma vai tiesiskā pienākuma pamatojumu;

5) atsevišķu piemēroto tiesību normu uzskaitījumu (norādot arī normatīvā akta pantu, tā daļu, punktu vai apakšpunktu);

6) adresātam piešķirtās tiesības un noraidītās tiesības;

7) nosacījumus (ja nepieciešams);

8) lēmuma, pieprasījuma vai tiesiskā pienākuma apstrīdēšanas kārtību.

(5) Šā panta pirmajā un otrajā daļā minēto lēmumu, pieprasījumu un tiesisko pienākumu var apstrīdēt:

1) Nacionālā kiberdrošības centra lēmumu, pieprasījumu vai uzlikto tiesisko pienākumu attiecībā uz būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem — iesniedzot attiecīgu iesniegumu aizsardzības ministram. Aizsardzības ministra lēmumu par apstrīdēto šā panta pirmajā daļā minēto lēmumu, pieprasījumu vai tiesisko pienākumu var pārsūdzēt Administratīvā procesa likumā noteiktajā kārtībā. Aizsardzības ministra lēmums par apstrīdēto šā panta otrajā daļā minēto lēmumu, pieprasījumu vai tiesisko pienākumu nav pārsūdzams;

2) Satversmes aizsardzības biroja lēmumu, pieprasījumu vai uzlikto tiesisko pienākumu attiecībā uz informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru — iesniedzot attiecīgu iesniegumu Satversmes aizsardzības biroja direktoram. Satversmes aizsardzības biroja direktora lēmumu par apstrīdēto šā panta pirmajā daļā minēto lēmumu, pieprasījumu vai tiesisko pienākumu var pārsūdzēt Administratīvā procesa likumā noteiktajā kārtībā. Satversmes aizsardzības biroja direktora lēmums par apstrīdēto šā panta otrajā daļā minēto lēmumu, pieprasījumu vai tiesisko pienākumu nav pārsūdzams.

13. pants. Kompetento institūciju sadarbība

(1) Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas pēc nepieciešamības, bet ne retāk kā reizi ceturksnī savstarpēji apmainās ar informāciju par kiberincidentu jomas aktualitātēm.

(2) Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs pēc nepieciešamības, bet ne retāk kā reizi ceturksnī savstarpēji apmainās ar informāciju par subjektu uzraudzības aktualitātēm, tostarp par subjektu identificēšanu, kiberriskiem, kiberapdraudējumiem, kiberincidentiem, gandrīz notikušiem kiberincidentiem, kā arī ar kiberdrošību nesaistītiem drošības riskiem, apdraudējumiem un incidentiem, kas skar subjektus, ja vien šādas informācijas apmaiņa nav pretrunā ar nacionālās drošības interesēm.

(3) Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas regulāri, bet ne retāk kā divas reizes gadā apmainās ar informāciju par aktuālajiem kiberincidentiem un kiberapdraudējumiem, ja vien šādas informācijas apmaiņa nav pretrunā ar nacionālās drošības interesēm, ar šādām institūcijām:

1) Latvijas Banku — jautājumos, kas skar regulas 2022/2554 2. pantā minēto finanšu vienību kiberdrošību, tostarp sniedz Latvijas Bankai savā rīcībā esošo informāciju par konstatētajiem kiberincidentiem šā likuma 20. panta 8. punkta "k" apakšpunktā minēto subjektu informācijas un komunikācijas tehnoloģiju infrastruktūrā, kā arī apmainās ar informāciju par kiberincidentiem, esošiem vai potenciāliem kiberapdraudējumiem, kas var ietekmēt Eiropas Savienības un Latvijas normatīvajos aktos noteikto Latvijas Bankas uzdevumu izpildi;

2) Sabiedrisko pakalpojumu regulēšanas komisiju — jautājumos, kas skar elektronisko sakaru komersantu kiberdrošību, tostarp sniedz Sabiedrisko pakalpojumu regulēšanas komisijai savā rīcībā esošo informāciju, kas tai nepieciešama Elektronisko sakaru likumā noteikto funkciju īstenošanai;

3) Civilās aviācijas aģentūru kā Eiropas Parlamenta un Padomes 2008. gada 11. marta regulā (EK) Nr. 300/2008 par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ regulu (EK) Nr. 2320/2002 un Eiropas Parlamenta un Padomes 2018. gada 4. jūlija regulas (ES) 2018/1139 par kopīgiem noteikumiem civilās aviācijas jomā un ar ko izveido Eiropas Savienības Aviācijas drošības aģentūru, un ar ko groza Eiropas Parlamenta un Padomes regulas (EK) Nr. 2111/2005, (EK) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 un direktīvas 2014/30/ES un 2014/53/ES un atceļ Eiropas Parlamenta un Padomes regulas (EK) Nr. 552/2004 un (EK) Nr. 216/2008 un Padomes regulu (EEK) Nr. 3922/91 9. pantā minēto atbildīgo iestādi civilās aviācijas drošības jomā, kas nodrošina tai noteikto uzraudzības funkciju īstenošanu;

4) valsts sabiedrību ar ierobežotu atbildību "Latvijas Jūras administrācija" — jautājumos, kas skar kuģu, kuģošanas kompāniju, ostu un ostas iekārtu aizsardzības prasību ieviešanu un uzraudzību;

5) Datu valsts inspekciju — jautājumos, kas skar fizisko personu datu aizsardzību, tostarp sniedz Datu valsts inspekcijai savā rīcībā esošo informāciju par fizisko personu datu aizsardzības pārkāpumiem;

6) Digitālās drošības uzraudzības komiteju — jautājumos, kas skar elektroniskās identifikācijas pakalpojumu sniedzējus un to sniegtos pakalpojumus, uzticamus sertifikācijas pakalpojumu sniedzējus un to sniegtos pakalpojumus, parakstu vākšanas tiešsaistes sistēmas, kā arī būtisko pakalpojumu un svarīgo pakalpojumu sniedzējus;

7) policiju, prokuratūru, tiesu un citām kompetentajām iestādēm — jautājumos, kas skar noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu. Ja kiberincidentu novēršanas institūcija konstatē, ka kiberincidentam, gandrīz notikušam kiberincidentam, kiberapdraudējumam vai ievainojamībai pirmšķietami piemīt noziedzīga nodarījuma pazīmes, kiberincidentu novēršanas institūcija par to nekavējoties informē kompetento iestādi, sniedzot tai savā rīcībā esošo informāciju, kas nepieciešama procesuālo darbību veikšanai;

8) valsts drošības iestādēm — jautājumos, kas saistīti ar nacionālo drošību, tostarp sniedz kompetentajām valsts drošības iestādēm savā rīcībā esošo informāciju par kiberincidentiem, gandrīz notikušiem kiberincidentiem, kiberapdraudējumiem un ievainojamībām, kas apdraud vai var apdraudēt nacionālo drošību.

(4) Latvijas Universitātes Matemātikas un informātikas institūts sniedz Militārās izlūkošanas un drošības dienestam savā rīcībā esošo informāciju par kiberincidentiem Aizsardzības ministrijā, tās padotībā esošajās iestādēs un Nacionālajos bruņotajos spēkos.

(5) Militārās izlūkošanas un drošības dienests sniedz Latvijas Universitātes Matemātikas un informātikas institūtam informāciju, kas tam nepieciešama šā likuma 10. panta 5. punktā noteikto uzdevumu izpildei, kā arī citu tā rīcībā esošo informāciju par Latvijas Universitātes Matemātikas un informātikas institūta kompetencē esošajiem kiberincidentiem.

(6) Ja šā panta trešās daļas 1. punktā minētie jautājumi skar *Eurosistēmas* uzturētas informācijas un komunikācijas tehnoloģiju infrastruktūras, kompetentās institūcijas sniegto informāciju Latvijas Banka nosūta Eiropas Centrālajai bankai.

14. pants. Kompetento institūciju sadarbība ar citu Eiropas Savienības dalībvalstu kompetentajām institūcijām

(1) Ja būtisko pakalpojumu sniedzējs vai svarīgo pakalpojumu sniedzējs sniedz pakalpojumus vairāk nekā vienā Eiropas Savienības dalībvalstī vai arī sniedz pakalpojumus vienā vai vairākās Eiropas Savienības dalībvalstīs un tā tīklu un informācijas sistēmas atrodas vienā vai vairākās citās Eiropas Savienības dalībvalstīs, Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas, ja nepieciešams, sadarbojas ar citu Eiropas Savienības dalībvalstu kompetentajām institūcijām:

1) ar Nacionālā kiberdrošības centra starpniecību informē citu attiecīgo Eiropas Savienības dalībvalstu kompetentās institūcijas un savstarpēji apmainās ar informāciju par veiktajiem uzraudzības un izpildes panākšanas pasākumiem;

2) ja nepieciešams, nosūta informācijas pieprasījumu vai lūdz, lai citas Eiropas Savienības dalībvalsts kompetentā institūcija veic uzraudzības vai izpildes panākšanas pasākumus;

3) saņemot pamatotu savstarpējās palīdzības lūgumu no citas Eiropas Savienības dalībvalsts kompetentās institūcijas, sniedz tai palīdzību, lai uzraudzības vai izpildes panākšanas pasākumi tiktu īstenoti efektīvi un konsekventi.

(2) Šā panta pirmās daļas 3. punktā minētā savstarpējā palīdzība var ietvert informācijas pieprasījumus un uzraudzības pasākumus, tostarp pieprasījumus veikt klātienes pārbaudes, attālinātu pārraudzību vai mērķtiecīgas drošības revīzijas.

(3) Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas nodrošina savstarpējās palīdzības lūguma īstenošanu, ja vien netiek konstatēts, ka tās nav kompetentas sniegt pieprasīto palīdzību, pieprasītās palīdzības lūgums nav samērīgs ar kompetento institūciju uzraudzības uzdevumiem vai saņemtais savstarpējās palīdzības lūgums ir pretrunā ar būtiskām nacionālās drošības interesēm.

(4) Pirms saņemtā savstarpējās palīdzības lūguma noraidīšanas Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas savstarpēji apspriežas. Ja kāda no Eiropas Savienības dalībvalstīm to pieprasa, minētās kompetentās institūcijas pirms savstarpējās palīdzības lūguma noraidīšanas apspriežas ar Eiropas Komisiju un Eiropas Savienības Kiberdrošības aģentūru.

(5) Nacionālais kiberdrošības centrs, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas pēc kopīgas vienošanās ar citas Eiropas Savienības dalībvalsts kompetento institūciju var veikt kopīgu subjektu uzraudzību.

15. pants. Sadarbība ar institūcijām, kuras ir atbildīgas par kiberdrošību

Subjektiem, valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām ir pienākums sadarboties ar Nacionālo kiberdrošības centru, Satversmes aizsardzības biroju un kiberincidentu novēršanas institūcijām, sniedzot tām nepieciešamo informāciju un pildot to likumīgās prasības.

16. pants. Nacionālā kiberdrošības padome

(1) Nacionālā kiberdrošības padome ir koleģiāla institūcija, kas koordinē ar kiberdrošību saistītās politikas izstrādi,

kā arī attiecīgu uzdevumu un pasākumu plānošanu un īstenošanu.

(2) Nacionālās kiberdrošības padomes sastāvu nosaka Ministru prezidents.

17. pants. Digitālās drošības uzraudzības komiteja

(1) Digitālās drošības uzraudzības komiteja ir koleģiāla uzraudzības institūcija aizsardzības ministra pakļautībā.

(2) Digitālās drošības uzraudzības komitejas nolikumu apstiprina Ministru kabinets.

(3) Kiberincidentu novēršanas institūcijas atbilstoši savai kompetencei sadarbojas ar Digitālās drošības uzraudzības komiteju un sniedz šai komitejai tās funkciju īstenošanai nepieciešamo informāciju, tostarp informē to par konstatētajiem nozīmīgiem kiberincidentiem un kiberapdraudējumiem, kas skar kvalificētus uzticamības pakalpojumu sniedzējus vai to sniegtos kvalificētus uzticamības pakalpojumus.

18. pants. Nacionālā kiberdrošības stratēģija

(1) Nacionālo kiberdrošības stratēģiju reizi četros gados izstrādā Nacionālais kiberdrošības centrs sadarbībā ar valsts pārvaldes iestādēm, valsts drošības iestādēm un privātā sektora pārstāvjiem un apstiprina Ministru kabinets.

(2) Nacionālā kiberdrošības stratēģija nosaka:

1) kiberdrošības pārvaldības stratēģiskos mērķus un modeli, kiberdrošības pārvaldībai nepieciešamos resursus;

2) kiberdrošības pārvaldībā iesaistīto valsts pārvaldes iestāžu lomu sadalījumu, kā arī nacionālos un starptautiskos sadarbības mehānismus;

3) valstiski aizsargājamo informācijas un komunikācijas tehnoloģiju un resursu noteikšanas un kiberrisku izvērtēšanas kārtību;

4) gatavības kiberincidentiem, reaģēšanas uz tiem, to novēršanas un pārvarēšanas plānu izstrādes kārtību un prasības, informācijas apmaiņas veidus, kā arī publiskā sektora un privātā sektora sadarbības kārtību;

5) pasākumu kopumu sabiedrības digitālo un kiberdrošības prasmju uzlabošanai.

(3) Nacionālā kiberdrošības stratēģija attiecas uz subjektiem, ja vien tajā nav noteikts citādi.

(4) Nacionālais kiberdrošības centrs sešu mēnešu laikā pēc nacionālās kiberdrošības stratēģijas apstiprināšanas izstrādā un Ministru kabinets apstiprina pasākumu plānu stratēģijā izvirzīto mērķu sasniegšanai, identificējot darba uzdevumus, atbildīgās institūcijas, uzdevumu izpildes termiņus un sasniedzamos rezultātus. Plānā iekļauj vismaz šādus pasākumus:

1) pasākumus subjektu informācijas un komunikācijas tehnoloģiju produktu un pakalpojumu piegādes ķēžu drošības uzlabošanai;

2) kiberdrošības pasākumus valsts tiešās un pastarpinātās pārvaldes iestāžu, atvasinātu publisko personu un citu valsts institūciju informācijas un komunikācijas tehnoloģiju produktu un pakalpojumu iepirkumos, tostarp attiecībā uz informācijas un komunikācijas tehnoloģijas sertifikāciju, šifrēšanu un atvērtā pirmkoda risinājumu izmantošanu;

3) pasākumus ievainojamību pārvaldībai, tostarp koordinētas ievainojamību atklāšanas un novēršanas nodrošināšanai;

4) pasākumus atklātā interneta publiskā kodola konfidencialitātes, integritātes un pieejamības nodrošināšanai, tostarp attiecībā uz zemūdens sakaru kabeļu kiberdrošību;

5) pasākumus kiberrisku pārvaldības īstenošanai;

6) pasākumus subjektu un citu valsts un privātā sektora institūciju, tostarp mazo un vidējo saimnieciskās

darbības veicēju, un visas sabiedrības kibernoturības veicināšanai, kiberdrošības prasmju un izpratnes veidošanai, kiberdrošības izglītības un apmācības programmu attīstīšanai, kā arī kiberhigiēnas pamatlīmeņa nodrošināšanai;

7) pasākumus kiberdrošības pētniecības un attīstības iniciatīvu atbalstam, tostarp kiberdrošības rīku izstrādei un drošas informācijas un komunikācijas tehnoloģiju infrastruktūras attīstīšanai, uzlabošanai un ieviešanai;

8) pasākumus brīvprātīgas kiberdrošības informācijas apmaiņas veicināšanai starp subjektiem;

9) aktīvas kiberaizsardzības pasākumus.

(5) Nacionālais kiberdrošības centrs divas reizes gadā informē Nacionālo kiberdrošības padomi par nacionālās kiberdrošības stratēģijas ieviešanas gaitu.

(6) Nacionālais kiberdrošības centrs triju mēnešu laikā pēc nacionālās kiberdrošības stratēģijas pieņemšanas paziņo to Eiropas Komisijai, izņemot nacionālajai drošībai nozīmīgu informāciju.

19. pants. Personas datu apstrāde

(1) Kiberincidentu novēršanas institūcija, pildot tai šajā likumā noteiktos uzdevumus un īstenojot savas tiesības, saņem un apstrādā personu identificējošu informāciju, lai pamatotu vai izslēgtu aizdomas par kiberapdraudējumu vai lai to novērstu, kā arī nodrošinātu saziņu ar iesaistītajām personām.

(2) Kiberincidentu novēršanas institūcija pēc ievainojamības un kiberincidenta atrisināšanas ir tiesīga uzglabāt un analizēt datus, kas iegūti, lai pamatotu vai izslēgtu aizdomas par ievainojamību un kiberincidentu, un satur personas datus, ja minētā informācija ir noderīga saistītu ievainojamību un kiberincidentu atklāšanai vai novēršanai.

(3) Personas datus kiberincidentu novēršanas institūcija drīkst nodot šā likuma 9. panta otrajā daļā minētajām institūcijām, lai atpazītu un novērstu tādu kiberapdraudējumu, ievainojamību vai kiberincidentu, kas rada vai var radīt draudus nacionālajai drošībai.

(4) Personas datus nepieciešamajā apjomā un veidā kiberincidentu novēršanas institūcija drīkst nodot Latvijas Republikas Zemessardzei, lai atpazītu un novērstu tādu kiberapdraudējumu, ievainojamību vai kiberincidentu, kas rada vai var radīt draudus nacionālajai drošībai, ja Latvijas Republikas Zemessardze atbilstoši Latvijas Republikas Zemessardzes likumam tiek iesaistīta atbalsta sniegšanā kompetentajai kiberincidentu novēršanas institūcijai.

(5) Satversmes aizsardzības birojs, pildot tam šajā likumā noteiktos uzdevumus un īstenojot savas tiesības, saņem, apstrādā, uzglabā un analizē datus, kas iegūti, lai pamatotu vai izslēgtu aizdomas par kiberapdraudējumu, ievainojamību vai kiberincidentu, kas rada vai var radīt draudus nacionālajai drošībai.

(6) Personas datus nepieciešamajā apjomā un veidā kiberincidentu novēršanas institūcija drīkst nodot Satversmes aizsardzības birojam, lai atpazītu un novērstu tādu kiberapdraudējumu, ievainojamību vai kiberincidentu, kas rada vai var radīt draudus nacionālajai drošībai.

III nodaļa
Subjektu identifikācija un uzskaite

20. pants. Būtisko pakalpojumu sniedzējs

Būtisko pakalpojumu sniedzējs šā likuma izpratnē ir:

1) augstākā līmeņa domēnu vārdu reģistra uzturētājs, piemēram, augstākā līmeņa domēna ".lv" reģistra uzturētājs;

2) domēnu vārdu sistēmas pakalpojumu sniedzējs, kas sniedz publiski pieejamus rekursīvus domēnu vārdu atrises pakalpojumus interneta galalietotājiem vai autoritatīvus domēnu vārdu atrises pakalpojumus trešo personu lietošanai, izņemot saknes vārdu serverus;

3) elektronisko sakaru komersants;

4) kvalificēts uzticamības pakalpojumu sniedzējs;

5) tiešās pārvaldes iestāde un cita valsts institūcija, izņemot valsts drošības iestādes;

6) atvasināta publiskā persona;

7) sabiedriskie elektroniskie plašsaziņas līdzekļi;

8) liels saimnieciskās darbības veicējs, kurš ir:

a) energoapgādes komersants,

b) naftas apgādes komersants,

c) ūdeņraža apgādes komersants,

d) aeronavigācijas pakalpojumu sniedzējs, gaisa kuģa ekspluatants vai lidlauka vai citu civilās aviācijas objektu un iekārtu ekspluatants,

e) dzelzceļa pārvadātājs vai dzelzceļa infrastruktūras pārvaldītājs,

f) kuģošanas kompānija, neietverot šīs kompānijas pārvaldītos individuālus kuģus,

g) ostas pārvalde,

h) komersants, kurš veic komercdarbību ostas teritorijā,

i) komersants, kurš pārvalda valsts autoceļus vai veic valsts autoceļu infrastruktūras uzturēšanas darbus,

j) intelektisko transporta sistēmu operators,

k) kredītiestāde, centrālais darījumu partneris vai tirdzniecības vieta Finanšu instrumentu tirgus likuma izpratnē,

l) ārstniecības iestāde vai Eiropas Savienības references laboratorija,

m) komersants, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, ražo zāles un aktīvās vielas,

n) kritiski svarīgu medicīnisko ierīču ražotājs (atbilstoši Eiropas Parlamenta un Padomes 2022. gada 25. janvāra regulas (ES) 2022/123 par pastiprinātu Eiropas Zāļu aģentūras lomu attiecībā uz zālēm un medicīniskajām ierīcēm krīžgatavības un krīžu pārvarēšanas kontekstā 22. pantam),

o) dzeramā ūdens piegādātājs vai izplatītājs, izņemot gadījumu, kad komersanta pamatdarbība nav saistīta ar dzeramā ūdens izplatīšanu,

p) ūdenssaimniecības pakalpojumu sniedzējs,

r) interneta plūsmu apmaiņas punkta pakalpojumu sniedzējs,

s) mākoņdatošanas pakalpojumu sniedzējs,

t) datu centru pakalpojumu sniedzējs,

u) satura piegādes tīkla pakalpojumu sniedzējs,

v) informācijas un komunikācijas tehnoloģiju pārvaldības vai kiberdrošības pakalpojumu sniedzējs,

z) kosmosā izvietotu pakalpojumu sniedzējs vai šo pakalpojumu sniegšanai izmantojamās infrastruktūras operators;

9) saimnieciskās darbības veicējs, kurš veic saimniecisko darbību vismaz vienā no šā panta 8. punktā minētajām jomām un ir vienīgais šāda veida pakalpojuma sniedzējs Latvijas Republikā;

10) pastarpinātās pārvaldes iestāde, kura sniedz pakalpojumus vai darbojas privāto tiesību jomā vismaz vienā no šā panta 8. punktā minētajām jomām;

11) 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, tai skaitā nacionālajai drošībai nozīmīga komercsabiedrība, nodibinājums un biedrība, izņemot Latvijas Republikā esošas meža zemes vismaz 10 000 hektāru platībā īpašnieku vai Latvijas Republikā esošas lauksaimniecības zemes vismaz 4000 hektāru platībā īpašnieku.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026. Grozījumi 11. punktā par nacionālajai drošībai nozīmīgām komercsabiedrībām, nodibinājumiem un biedrībām stājas spēkā 01.10.2026. Sk. pārejas noteikumu 15. punktu)

21. pants. Svarīgo pakalpojumu sniedzējs

(1) Svarīgo pakalpojumu sniedzējs šā likuma izpratnē ir persona, kas nav būtisko pakalpojumu sniedzējs un ir:

1) vidējs saimnieciskās darbības veicējs, kurš veic saimniecisko darbību vismaz vienā no šā likuma 20. panta 8. punktā minētajām jomām;

2) vidējs vai liels saimnieciskās darbības veicējs, kurš ir:

a) pasta komersants,

b) atkritumu apsaimniekotājs,

c) ķīmisko vielu vai to maisījumu ražotājs vai izplatītājs vairumtirdzniecībā, ja ķīmisko vielu vai to maisījumu izplatīšana ir komersanta pamatdarbība,

d) komersants, kurš ražo izstrādājumus no ķīmiskajām vielām vai to maisījumiem,

e) komersants, kura pamatdarbība ir pārtikas rūpnieciska ražošana, pārstrāde vai pārtikas izplatīšana vairumtirdzniecībā,

f) medicīnisko ierīču ražotājs,

g) datoru, elektronisko un optisko iekārtu ražotājs,

h) elektrisko iekārtu ražotājs,

i) citur neklasificētu iekārtu, mehānismu un darba mašīnu ražotājs,

j) automobiļu, piekabju un puspiekabju ražotājs,

k) citu transportlīdzekļu ražotājs,

l) tiešsaistes tirdzniecības vietas pakalpojumu sniedzējs,

m) tiešsaistes meklētājprogrammas pakalpojumu sniedzējs,

n) sociālo mediju platformas pakalpojumu sniedzējs,

o) zinātniskā institūcija,

p) apsardzes pakalpojumu sniedzējs;

3) saimnieciskās darbības veicējs, kurš veic saimniecisko darbību vismaz vienā no šā panta pirmās daļas

2. punktā minētajām jomām un ir vienīgais šāda veida pakalpojuma sniedzējs Latvijas Republikā;

4) pastarpinātās pārvaldes iestāde, kura sniedz pakalpojumus vai darbojas privāto tiesību jomā vismaz vienā no šā panta pirmās daļas 2. punktā minētajām jomām;

5) izglītības informācijas sistēmas uzturētājs;

6) uzticamības pakalpojumu sniedzējs, kurš nav kvalificēts uzticamības pakalpojumu sniedzējs.

(2) Izglītības informācijas sistēma šā likuma izpratnē ir tāda informācijas sistēma, kurā tiek veikta Latvijas Republikā akreditētas izglītības iestādes izglītojamo personas datu elektroniskā apstrāde.

22. pants. Būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju uzskaite

(1) Persona veic pašvērtējumu, nosakot savu atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam. Atbilstības gadījumā persona ne vēlāk kā mēneša laikā par to paziņo Nacionālajam kiberdrošības centram. Paziņojumā norāda:

1) personas nosaukumu (fiziskā persona — vārdu, uzvārdu un personas kodu), juridisko statusu un saimnieciskās darbības formu, reģistrācijas numuru, juridisko adresi un citu kontaktinformāciju (piemēram, oficiālo elektronisko adresi, elektroniskā pasta adresi, tālruņa numuru, tīmekļvietnes adresi);

2) informāciju par personas darbības jomu atbilstoši šā likuma 20. un 21. pantam;

3) personas sniegto būtisko pakalpojumu un svarīgo pakalpojumu uzskaitījumu un detalizētu aprakstu;

4) personas pastāvīgi izmantoto interneta protokola (IP) adrešu diapazonus;

5) valstis, kurās persona sniedz pakalpojumus;

6) personas kontaktpersonas datus (vārdu, uzvārdu, amatu, tālruņa numuru, elektroniskā pasta adresi).

(2) Būtisko pakalpojumu un svarīgo pakalpojumu sniedzējs nekavējoties, bet ne vēlāk kā divu nedēļu laikā paziņo Nacionālajam kiberdrošības centram par jebkādām šā panta pirmajā daļā minētajā paziņojumā norādīto ziņu izmaiņām.

(3) Nacionālais kiberdrošības centrs šā panta pirmajā un otrajā daļā minētos paziņojumus, izņemot šā panta pirmās daļas 4. punktā minēto informāciju un citu informāciju, kuras izpaušana ir pretrunā ar nacionālās drošības interesēm, nekavējoties pārsūta Eiropas Savienības Kiberdrošības aģentūrai.

(4) Nacionālais kiberdrošības centrs apkopo un apstiprina būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju sarakstu. Būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju saraksts ir ierobežotas pieejamības informācija.

(4^1) Nacionālais kiberdrošības centrs var pieņemt lēmumu izslēgt no būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju saraksta tiešās pārvaldes iestādi, pastarpinātās pārvaldes iestādi, atvasinātu publisku personu un citu valsts institūciju, kuras darbības traucējums nevar būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai nevar radīt būtisku sistēmisku risku, kā arī privāto tiesību juridisko personu, ja tā vairs neatbilst būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam.

(5) Ja persona par savu atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam nav paziņojusi Nacionālajam kiberdrošības centram šajā likumā noteiktajā termiņā, bet Nacionālā kiberdrošības centra rīcībā esošā informācija ir pietiekama, lai noteiktu minētās personas atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam, Nacionālais kiberdrošības centrs pieņem lēmumu par personas atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam un iekļauj minēto personu būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju sarakstā, par to rakstveidā paziņojot minētajam būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējam. Šādā gadījumā būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējam ir pienākums nekavējoties, bet ne vēlāk kā mēneša laikā pēc paziņojuma saņemšanas sniegt Nacionālajam kiberdrošības centram šā panta pirmajā daļā minēto informāciju.

(5^1) Šā panta piektajā daļā minēto lēmumu Nacionālais kiberdrošības centrs pieņem arī tad, ja tas konstatē, ka persona savu atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam ir noteikusi

neatbilstoši.

(6) Šā panta ceturtajā daļā minēto sarakstu pārskata vismaz reizi divos gados. Nacionālais kiberdrošības centrs nodrošina, ka Eiropas Komisijai, NIS sadarbības grupai, kā arī pēc pieprasījuma citām Eiropas Savienības kompetentajām institūcijām tiek iesniegta apkopota informācija par būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju skaitu, darbības jomām un sniegtajiem pakalpojumiem.

(7) Nacionālais kiberdrošības centrs pēc Eiropas Komisijas vai citas Eiropas Savienības kompetentās institūcijas pieprasījuma var tai sniegt informāciju par būtisko pakalpojumu vai svarīgo pakalpojumu sniedzēja identitāti (piemēram, būtisko pakalpojumu vai svarīgo pakalpojumu sniedzēja nosaukumu, juridisko statusu, saimnieciskās darbības formu, kontaktinformāciju), ja vien šādas informācijas izpaušana nav pretrunā ar nacionālās drošības interesēm.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

23. pants. Domēnu vārdu reģistrācijas pakalpojumu sniedzēju uzskaite un domēnu vārdu reģistrācijas datubāzes prasības

(1) Domēnu vārdu reģistrācijas pakalpojumu sniedzējs, kurš atbilst domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam un kura lēmumi saistībā ar kiberdrošību tiek pieņemti Latvijas Republikā vai kuram Latvijas Republikā ir vislielākais darbinieku skaits, ne vēlāk kā mēneša laikā par to paziņo Nacionālajam kiberdrošības centram. Paziņojumā norāda:

1) personas nosaukumu (fiziskā persona — vārdu, uzvārdu un personas kodu), juridisko statusu un saimnieciskās darbības formu, reģistrācijas numuru, juridisko adresi un citu kontaktinformāciju (piemēram, oficiālo elektronisko adresi, elektroniskā pasta adresi, tālruņa numuru, tīmekļvietnes adresi);

2) informāciju par personas darbības jomu atbilstoši šā likuma 20. un 21. pantam, ja attiecināms;

3) personas pastāvīgi izmantoto interneta protokola (IP) adrešu diapazonus;

4) valstis, kurās persona sniedz pakalpojumus;

5) personas kontaktpersonas datus (vārdu, uzvārdu, amatu, tālruņa numuru, elektroniskā pasta adresi).

(2) Domēnu vārdu reģistrācijas pakalpojumu sniedzējs nekavējoties, bet ne vēlāk kā divu nedēļu laikā paziņo Nacionālajam kiberdrošības centram par jebkādām šā panta pirmajā daļā minētajā paziņojumā norādīto ziņu izmaiņām.

(3) Nacionālais kiberdrošības centrs šā panta pirmajā un otrajā daļā minētos paziņojumus, izņemot šā panta pirmās daļas 3. punktā minēto informāciju un citu informāciju, kuras izpaušana ir pretrunā ar nacionālās drošības interesēm, nekavējoties pārsūta Eiropas Savienības Kiberdrošības aģentūrai.

(4) Nacionālais kiberdrošības centrs apkopo un apstiprina domēnu vārdu reģistrācijas pakalpojumu sniedzēju sarakstu.

(5) Ja persona par savu atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam nav paziņojusi Nacionālajam kiberdrošības centram šajā likumā noteiktajā termiņā, bet Nacionālā kiberdrošības centra rīcībā esošā informācija ir pietiekama, lai noteiktu minētās personas atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam, Nacionālais kiberdrošības centrs pieņem lēmumu par personas atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam un iekļauj minēto personu domēnu vārdu reģistrācijas sniedzēju sarakstā, par to rakstveidā paziņojot minētajam domēnu vārdu reģistrācijas pakalpojumu sniedzējam. Šādā gadījumā domēnu vārdu reģistrācijas pakalpojumu sniedzējam ir pienākums nekavējoties, bet ne vēlāk kā mēneša laikā pēc paziņojuma saņemšanas sniegt Nacionālajam kiberdrošības centram šā panta pirmajā daļā minēto informāciju.

(5^1) Šā panta piektajā daļā minēto lēmumu Nacionālais kiberdrošības centrs pieņem arī tad, ja tas konstatē, ka persona savu atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam ir noteikusi neatbilstoši.

(6) Prasības domēnu vārdu reģistrācijas datubāzei, kas piemērojamas augstākā līmeņa domēna ".lv" reģistra uzturētājam un domēnu vārdu reģistrācijas pakalpojumu sniedzējiem, nosaka Ministru kabinets.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

24. pants. Informācijas un komunikācijas tehnoloģiju kritiskā infrastruktūra

(1) Par informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru šā likuma izpratnē uzskatāma Ministru kabineta apstiprinātajā kritiskās infrastruktūras kopumā iekļautā informācijas un komunikācijas tehnoloģiju kritiskā infrastruktūra.

(2) Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras drošības prasības, izmantoto informācijas un komunikācijas tehnoloģiju resursu, pakalpojumu un piegādes ķēžu drošības risku pārvaldības prasības, kā arī pasākumus un to plānošanas un īstenošanas kārtību nosaka Ministru kabinets.

(3) Šā panta otrajā daļā minētās prasības informācijas un komunikācijas tehnoloģiju kritiskajai infrastruktūrai nedrīkst būt zemākas par prasībām, kas šajā likumā noteiktas būtisko pakalpojumu sniedzējiem.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

IV nodaļa
Subjektu kiberdrošības pārvaldība

25. pants. Subjekta vadītāja un kiberdrošības pārvaldnieka kompetence

(1) Subjekta kiberdrošības pārvaldību nodrošina un par to atbild subjekta vadītājs. Katra subjekta vadītājs nosaka atbildīgo personu, kura īsteno un pārrauga kiberdrošības pasākumu īstenošanu attiecīgajā subjektā (turpmāk — kiberdrošības pārvaldnieks). Ministru kabinets nosaka kiberdrošības pārvaldniekam izvirzāmās prasības.

(2) Subjekta vadītājs kiberdrošības pārvaldnieku nosaka ne vēlāk kā triju mēnešu laikā no šā likuma 22. panta pirmajā daļā minētā paziņojuma sniegšanas vai piektajā daļā minētā lēmuma pieņemšanas brīža. Subjekts nekavējoties, bet ne vēlāk kā piecu darbdienu laikā paziņo Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam par kiberdrošības pārvaldnieka noteikšanu. Paziņojumā norāda kiberdrošības pārvaldnieka vārdu, uzvārdu, personas kodu, amatu, elektroniskā pasta adresi un tālruņa numuru.

(3) Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kiberdrošības pārvaldnieku nosaka pēc saskaņošanas ar Satversmes aizsardzības biroju, kas pārbauda kiberdrošības pārvaldnieka atbilstību izvirzītajām prasībām. Par kiberdrošības pārvaldnieka pretendentu Satversmes aizsardzības birojam paziņo ne vēlāk kā triju mēnešu laikā no brīža, kad subjekts iekļauts Ministru kabineta apstiprinātajā kritiskās infrastruktūras kopumā.

(4) Subjekts nekavējoties, bet ne vēlāk kā piecu darbdienu laikā paziņo Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam par jebkādām šā panta otrajā daļā minētajā paziņojumā norādīto ziņu izmaiņām.

(5) Kiberdrošības pārvaldniekam ir šādi pienākumi:

1) organizēt institūcijas informācijas un komunikācijas tehnoloģiju infrastruktūras drošības pasākumus;

2) ne retāk kā reizi gadā veikt informācijas un komunikācijas tehnoloģiju drošības pārbaudi un atbilstoši tās rezultātiem organizēt konstatēto trūkumu novēršanu;

3) vismaz reizi gadā apmeklēt kiberincidentu novēršanas institūcijas organizētu apmācību kiberdrošības jautājumos;

4) ne retāk kā reizi gadā nodrošināt, ka tiek veikta institūcijā nodarbināto instruktāža par subjektam aktuālajiem kiberriskiem un kiberdrošību.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

26. pants. Minimālās kiberdrošības prasības

Ministru kabinets nosaka minimālās kiberdrošības prasības subjektiem, kārtību, kādā subjekti nodrošina savu tīklu un informācijas sistēmu atbilstību minimālajām kiberdrošības prasībām, prasības un veicamos pasākumus subjektu tīklu un informācijas sistēmu konfidencialitātes, integritātes un pieejamības nodrošināšanai un datu atjaunošanai, kā arī veidu, kādā Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam sniedz šā likuma 22. panta pirmajā, otrajā un piektajā daļā, 23. panta pirmajā, otrajā un piektajā daļā un 25. panta otrajā un ceturtajā daļā minēto

informāciju (piemēram, izmantojot Nacionālā kiberdrošības centra uzturēto valsts informācijas sistēmu vai citu tehnoloģisko risinājumu).

26.[1] pants. Personāla drošības prasības

(1) Par subjekta darbinieku informācijas un komunikācijas tehnoloģiju jomā, kuram ir privileģētas tiesības piekļūt sistēmām vai informācijas un komunikācijas tehnoloģiju resursiem, kam ir tieša ietekme uz subjekta pamatdarbību, nevar būt persona, kura sodīta, izņemot personas, kuras reabilitētas vai kurām sodāmība noņemta vai dzēsta, par:

1) tāda tīša nozieguma izdarīšanu, kas saistīts ar terorismu;

2) tīša nozieguma izdarīšanu pret valsti, pārvaldības kārtību vai tīša nozieguma izdarīšanu valsts institūciju dienestā;

3) tīša nozieguma izdarīšanu pret īpašumu vai tīša nozieguma izdarīšanu tautsaimniecībā.

(2) Subjektam ir pienākums, izvērtējot attiecīgās personas radīto drošības risku, izdarītā nozieguma raksturu, laiku, kas pagājis kopš soda izciešanas, un personas piemērotību amatam, pieņemt individuālu lēmumu par personas nodarbināšanu, ja tā ir sodīta par kādu no šā panta pirmajā daļā minētajiem noziegumiem un nav reabilitēta vai tai nav noņemta vai dzēsta sodāmība.

(3) Subjektam ir tiesības pieprasīt un saņemt ziņas no Sodu reģistra, lai pirms fiziskās personas pieņemšanas darbā vai dienestā pārbaudītu tās atbilstību šā panta pirmajā daļā noteiktajiem ierobežojumiem.

(04.06.2026. likuma redakcijā, kas stājas spēkā 18.06.2026.)

27. pants. Subjekta pienākumi kiberapdraudējuma pārvaldības jomā

Subjekts veic piemērotus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu kiberriskus subjekta izmantoto elektronisko sakaru tīklu un informācijas sistēmu drošībai un novērstu vai līdz minimumam samazinātu kiberincidentu ietekmi uz subjekta pakalpojumu saņēmējiem un uz citiem pakalpojumiem.

28. pants. Kiberrisku pārvaldības un informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plāns

(1) Subjektam ir pienākums izstrādāt kiberrisku pārvaldības un informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plānu un nodrošināt darbiniekiem regulāru apmācību efektīvai plānā iekļauto pasākumu īstenošanai.

(2) Subjekta kiberrisku pārvaldības un informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plānā iekļaujamās informācijas veidu un apjomu, kā arī plāna izpildes uzraudzības un kontroles kārtību nosaka Ministru kabinets.

29. pants. Agrās brīdināšanas sensori

(Izslēgts ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

30. pants. Datu centru kiberdrošība

(1) Subjekts savā īpašumā vai valdījumā esošās informācijas sistēmas uztur savā informācijas un komunikācijas tehnoloģiju infrastruktūrā, kas atbilst minimālajām kiberdrošības prasībām, vai Ministru kabineta noteiktajām prasībām atbilstošos datu centros (turpmāk — datu centri).

(2) Ministru kabinets nosaka:

1) datu centru drošības prasības, datu centru atbilstības novērtēšanas un uzraudzības kārtību, kā arī datu centra operatora pienākumus;

2) noteikumus par informācijas sistēmu izvietošanu datu centros;

3) noteikumus par drošības operāciju centru izveidi un darbību datu centros.

(3) Kompetentajai kiberincidentu novēršanas institūcijai ir tiesības izveidot drošības operāciju centru valsts nozīmes datu centrā, tiešās un pastarpinātās pārvaldes iestādēs, atvasinātās publiskajās personās un citās valsts institūcijās un nodrošināt tā darbību. Drošības operāciju centra ietvaros kiberincidentu novēršanas institūcijai ir tiesības vākt, glabāt un elektroniski apstrādāt kiberapdraudējuma identificēšanai nepieciešamos datus, tai skaitā žurnālfailus, datu plūsmas, serveru veiktspējas datus. Datu centra operators, ja tā rīcībā ir nepieciešamie dati, nodod kompetentajai kiberincidentu novēršanas institūcijai ar saviem rīkiem iegūtos datus.

(4) Izvērtējot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras esošo un plānoto drošības operāciju centru kapacitāti, kompetentā kiberincidentu novēršanas institūcija ir tiesīga izveidot drošības operāciju centru informācijas un komunikācijas tehnoloģiju kritiskajā infrastruktūrā.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

31. pants. Centralizēta aizsardzība pret pakalpojumatteices kiberuzbrukumiem

Ministru kabinets nosaka:

1) prasības centralizētai informācijas un komunikācijas tehnoloģiju infrastruktūras un interneta aizsardzībai pret pakalpojumatteices kiberuzbrukumiem;

2) kritērijus, atbilstoši kuriem informācijas un komunikācijas tehnoloģiju infrastruktūras un interneta resursi tiek iekļauti pret pakalpojumatteices kiberuzbrukumiem centralizēti aizsargājamo resursu sarakstā;

3) kārtību, kādā tiek izvērtēta informācijas un komunikācijas tehnoloģiju infrastruktūras un interneta resursu atbilstība šā panta 2. punktā minētajiem kritērijiem;

4) pret pakalpojumatteices kiberuzbrukumiem centralizēti aizsargājamo resursu saraksta apstiprināšanas kārtību.

32. pants. Vienotā valsts interneta plūsmu apmaiņas punkta darbība

(1) Vienoto valsts interneta plūsmu apmaiņas punktu izveido un uztur, lai:

1) pastāvīgi nodrošinātu kritiskās datu plūsmas atrašanos tikai Latvijas Republikas teritorijā;

2) nodrošinātu svarīgu sabiedrības funkciju īstenošanai, kā arī cilvēku veselības, aizsardzības, drošības, ekonomiskās un sociālās labklājības nodrošināšanai nepieciešamo informācijas sistēmu sasniedzamību gadījumā, kad Latvijas Republikā nav pieejams globālais internets;

3) nodrošinātu interneta darbību un datu plūsmu apmaiņu Latvijas Republikas teritorijā, ja veikta atslēgšanās no globālā interneta.

(2) Vienotā valsts interneta plūsmu apmaiņas punkta pakalpojumus ir tiesīga saņemt valsts vai pašvaldības institūcija vai subjekts, kura iekļaušanu vienotā valsts interneta plūsmu apmaiņas punkta pakalpojumu saņēmēju sarakstā ir atbalstījusi starpinstitūciju komisija. Minētās komisijas sastāvu, izveides un darbības kārtību nosaka Ministru kabinets.

(3) Ministru kabinets nosaka:

1) vienotā valsts interneta plūsmu apmaiņas punkta darbības un pakalpojumu sniegšanas un saņemšanas kārtību;

2) kritērijus valsts un pašvaldību institūciju un subjektu iekļaušanai vienotā valsts interneta plūsmu apmaiņas punkta pakalpojumu saņēmēju sarakstā;

3) valsts un pašvaldību institūcijas un subjektus, kuriem ir noteikta prasība datu plūsmu nepastarpināti virzīt caur vienoto valsts interneta plūsmu apmaiņas punktu.

33. pants. Kiberhigiēnas prasības

Ministru kabinets nosaka subjektiem kiberhigiēnas pasākumu pamatelementus un prasības attiecībā uz kiberhigiēnas pasākumu īstenošanu.

V nodaļa
Rīcība kiberincidenta gadījumā

34. pants. Subjekta rīcība kiberincidenta gadījumā

(1) Konstatējot kiberincidentu, subjekts nekavējoties veic visas kiberincidenta novēršanai nepieciešamās darbības, kā arī nekavējoties par kiberincidentu informē kompetento kiberincidentu novēršanas institūciju un izpilda tās sniegtos norādījumus par rīcību kiberincidenta gadījumā. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kiberincidenta gadījumā nekavējoties par to informē arī kompetento valsts drošības iestādi. Ministru kabinets nosaka kārtību informēšanai par kiberincidentu un to kiberincidentu kritērijus, informācija par kuriem ir sniedzama kompetentajai kiberincidentu novēršanas institūcijai.

(2) Nozīmīga kiberincidenta gadījumā subjekts nekavējoties, bet ne vēlāk kā 24 stundu laikā elektroniski iesniedz kompetentajai kiberincidentu novēršanas institūcijai agrīno brīdinājumu par nozīmīgo kiberincidentu.

(3) Nozīmīga kiberincidenta gadījumā subjekts nekavējoties, bet ne vēlāk kā 72 stundu laikā (uzticamības pakalpojumu sniedzējs — 24 stundu laikā) elektroniski iesniedz kompetentajai kiberincidentu novēršanas institūcijai sākotnējo ziņojumu par nozīmīgo kiberincidentu.

(4) Nozīmīga kiberincidenta vai nozīmīga kiberapdraudējuma gadījumā subjekts nekavējoties informē savu pakalpojumu saņēmējus, tostarp elektronisko sakaru tīkla vai informācijas sistēmas lietotājus, kurus šāds nozīmīgs kiberincidents vai nozīmīgs kiberapdraudējums varētu skart, par iespējamiem kiberdrošības pasākumiem vai līdzekļiem, ko pakalpojumu saņēmēji var izmantot, lai novērstu kiberincidentu vai mazinātu kiberapdraudējumu. Attiecīgajā gadījumā subjekts pēc saskaņošanas ar kompetento kiberincidentu novēršanas institūciju (informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs — arī ar kompetento valsts drošības iestādi) nekavējoties informē savu pakalpojumu saņēmējus arī par nozīmīgu kiberincidentu vai nozīmīgu kiberapdraudējumu, ja vien šādas informācijas izpaušana nerada jauna nozīmīga kiberincidenta risku vai nav citādi pretrunā ar nacionālās drošības interesēm.

(5) Subjekts mēneša laikā pēc šā panta trešajā daļā minētā ziņojuma iesniegšanas iesniedz kompetentajai kiberincidentu novēršanas institūcijai galaziņojumu par nozīmīgā kiberincidenta atrisināšanu. Pēc kompetentās kiberincidentu novēršanas institūcijas pieprasījuma subjekts iesniedz tai arī starpposma ziņojumu par nozīmīgā kiberincidenta risināšanu.

(6) Ja šā panta piektajā daļā noteiktajā termiņā nozīmīgo kiberincidentu nav iespējams atrisināt, subjekts iesniedz kompetentajai kiberincidentu novēršanas institūcijai progresa ziņojumu par nozīmīgā kiberincidenta risināšanu, savukārt šā panta piektajā daļā minēto galaziņojumu iesniedz pēc nozīmīgā kiberincidenta atrisināšanas.

(7) Ministru kabinets nosaka šā panta otrajā daļā minētā brīdinājuma, kā arī šā panta trešajā, piektajā un sestajā daļā minēto ziņojumu saturu un iesniegšanas kārtību.

(8) Personas, uz kurām neattiecas šā panta pirmajā daļā noteiktie pienākumi, kiberincidenta gadījumā var veikt visas tā novēršanai nepieciešamās darbības un var pēc savas iniciatīvas brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai par konstatēto kiberincidentu. Kiberincidentu novēršanas institūcija vienojas ar personu, kura ziņojusi par kiberincidentu, par atbalsta sniegšanu kiberincidenta risināšanā. Brīvprātīga ziņošana par kiberincidentu neuzliek minētajai personai papildu pienākumus.

(9) Subjekti un citas personas var pēc savas iniciatīvas brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai par gandrīz notikušu kiberincidentu vai kiberapdraudējumu. Brīvprātīga ziņošana par gandrīz notikušu kiberincidentu vai kiberapdraudējumu neuzliek personai papildu pienākumus.

(10) Subjekts pēc Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja pieprasījuma ne ilgāk kā uz piecām dienām slēdz lietotājam piekļuvi elektronisko sakaru tīklam, ja lietotājs būtiski apdraud citu lietotāju tiesības vai elektronisko sakaru tīkla, informācijas sistēmas vai pakalpojuma drošību. Pieprasījumā norāda kiberapdraudējumu, piekļuves ierobežojuma ilgumu un, ja nepieciešams, citas subjektam veicamās darbības (piemēram, datu plūsmas pārvirzīšana uz kompetentās kiberincidentu novēršanas institūcijas infrastruktūru).

Pieprasījuma apstrīdēšana vai pārsūdzēšana neaptur tā darbību. Nosacījumus un kārtību, kādā lietotājam tiek slēgta piekļuve elektronisko sakaru tīklam, nosaka Ministru kabinets.

35. pants. Kiberincidentu novēršanas institūcijas rīcība kiberincidenta gadījumā

(1) Kiberincidentu novēršanas institūcija nekavējoties informē Nacionālo kiberdrošības centru par šā likuma 34. panta otrajā daļā minētā agrīnā brīdinājuma vai trešajā, piektajā vai sestajā daļā minētā ziņojuma saņemšanu. Kiberincidentu novēršanas institūcija informē Nacionālo kiberdrošības centru arī par šā likuma 34. panta astotajā un devītajā daļā minētā paziņojuma saņemšanu.

(2) Kiberincidentu novēršanas institūcija 24 stundu laikā pēc tam, kad saņēmusi sākotnējo informāciju par nozīmīgu kiberincidentu, vienojas ar personu, kura ziņojusi par nozīmīgu kiberincidentu, par atbalsta sniegšanu nozīmīgā kiberincidenta novēršanā, kā arī sniedz kiberincidenta sākotnējo vērtējumu un priekšlikumus kiberincidenta novēršanai.

(3) Ja konstatētais kiberincidents apdraud nacionālo drošību, kiberincidentu novēršanas institūcija par to informē Nacionālo kiberdrošības centru un valsts drošības iestādes. Nacionālais kiberdrošības centrs par to informē aizsardzības ministru un par nozari atbildīgo ministru.

(4) Ja konstatētajam kiberincidentam ir nozīmīga ietekme uz elektronisko sakaru tīklu vai elektronisko sakaru pakalpojuma nepārtrauktību, kiberincidentu novēršanas institūcija par to informē Nacionālo kiberdrošības centru un Satversmes aizsardzības biroju. Nacionālais kiberdrošības centrs par to informē Sabiedrisko pakalpojumu regulēšanas komisiju, kā arī var informēt Eiropas Savienības Kiberdrošības aģentūru un CSIRT tīklu.

(5) Pārrobežu kiberincidenta gadījumā kompetentā kiberincidentu novēršanas institūcija nekavējoties informē kiberincidenta skarto Eiropas Savienības dalībvalstu kompetentās iestādes un Eiropas Savienības Kiberdrošības aģentūru.

(6) Ja sabiedrības informēšana par nozīmīgu kiberincidentu vai kiberapdraudējumu var palīdzēt novērst vai risināt nozīmīgu kiberincidentu, mazināt kiberapdraudējumu vai citādā ziņā ir sabiedrības interesēs, Nacionālais kiberdrošības centrs vai kompetentā kiberincidentu novēršanas institūcija pēc iepriekšējas apspriešanās ar subjektu var informēt sabiedrību vai uzdot subjektam informēt sabiedrību, ja vien minētās informācijas izpaušana nav pretrunā ar nacionālās drošības interesēm.

36. pants. Nozīmīgu kiberincidentu un krīžu vadība

(1) Kiberincidentu nozīmīguma kritērijus apstiprina Ministru kabinets.

(2) Nozīmīgu kiberincidentu un krīžu vadību nodrošina Nacionālais kiberdrošības centrs sadarbībā ar kiberincidentu novēršanas institūcijām un valsts drošības iestādēm.

(3) Nozīmīgu kiberincidentu un krīžu vadības mērķus, spējas, resursus un kārtību nosaka Nacionālajā kiberincidentu krīzes vadības plānā, kura izstrādi un pārskatīšanu ne retāk kā reizi četros gados nodrošina Nacionālais kiberdrošības centrs sadarbībā ar valsts drošības iestādēm. Nacionālo kiberincidentu krīzes vadības plānu apstiprina Ministru kabinets.

(4) Nacionālajā kiberincidentu krīzes vadības plānā iekļauj:

1) Nacionālā kiberdrošības centra, kiberincidentu novēršanas institūciju un valsts drošības iestāžu uzdevumus, pienākumus un savstarpējās sadarbības mehānismu;

2) ar Nacionālā kiberincidentu krīzes vadības plāna īstenošanu saistītās mācības;

3) ietvaru sadarbībai ar ārvalstu un starptautiskajiem partneriem;

4) ietvaru sadarbībai ar valsts un pašvaldību iestādēm, kā arī privātā sektora pārstāvjiem, uz ko var attiekties nozīmīga kiberincidenta ietekme;

5) kompetento iestāžu sadarbības ietvaru un kārtību nozīmīgu kiberincidentu un krīžu efektīvai pārvaldībai Eiropas Savienībā.

(5) Nacionālajā kiberincidentu krīzes vadības plānā noteiktās procedūras regulāri iekļauj Nacionālā kiberdrošības centra un citu kompetento institūciju rīkotajās mācībās un apmācības aktivitātēs.

(6) Nacionālais kiberdrošības centrs iesniedz Eiropas Komisijai un Eiropas Savienības Kiberkrīžu sadarbības organizācijas tīklā informāciju par Nacionālo kiberincidentu krīzes vadības plānu, izņemot informāciju, kas skar nacionālās drošības intereses.

37. pants. Ierobežojošās darbības kiberapdraudējuma vai kiberincidenta gadījumā

(1) Ja kiberapdraudējums vai kiberincidents rada vai var radīt nozīmīgus draudus informācijas sistēmu un elektronisko sakaru tīklu drošībai vai nacionālajai drošībai un kiberincidentu vai kiberapdraudējumu nav iespējams novērst citā veidā, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs, ierobežojot piekļuvi interneta resursiem, ir tiesīgs pieņemt lēmumu:

1) atslēgt vai ierobežot piekļuvi kiberincidentā vai kiberapdraudējumā iesaistītajam domēna vārdam;

2) ierobežot piekļuvi kiberincidentā vai kiberapdraudējumā iesaistītajai interneta protokola (IP) adresei;

3) ierobežot piekļuvi kiberincidentā vai kiberapdraudējumā iesaistītajai mobilo platformu lietotnei.

(2) Šā panta pirmajā daļā minētajā Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja lēmumā norāda piekļuves ierobežojumu un tā ilgumu, kas nepārsniedz vienu gadu.

(3) Šā panta pirmajā daļā minētā Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja lēmuma apstrīdēšana vai pārsūdzēšana neaptur tā darbību un izpildi.

(4) Elektronisko sakaru pakalpojumu sniedzēji šā panta pirmās daļas 2. un 3. punktā minēto Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja lēmumu izpilda ne vēlāk kā vienas darbdienas laikā pēc tā paziņošanas, ja tiem ir pieejami šā lēmuma izpildīšanai nepieciešamie tehnoloģiskie līdzekļi.

(5) Elektronisko sakaru pakalpojumu sniedzēji un augstākā līmeņa domēnu vārdu reģistra uzturētājs šā panta pirmās daļas 1. punktā minēto Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja lēmumu izpilda nekavējoties pēc tā paziņošanas, izmantojot kompetentās kiberincidentu novēršanas institūcijas uzturēto ierobežojamo interneta resursu sarakstu, un ierobežo galalietotājiem piekļuvi sarakstā iekļautajiem interneta resursiem, nekavējoties nodrošinot arī to, ka kompetentajai kiberdrošības incidentu novēršanas institūcijai tiek pārsūtīta informācija par galalietotāju mēģinājumiem piekļūt ierobežotajiem resursiem.

(6) Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam pirms šā panta pirmās daļas 1. un 2. punktā minēto tiesību īstenošanas attiecībā uz piekļuves atslēgšanu vai ierobežošanu Latvijas Bankas vārdā reģistrētam domēna vārdam vai piekļuves ierobežošanu Latvijas Bankas interneta protokola (IP) adresei konsultējas ar Latvijas Banku.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

38. pants. Kiberuzbrukumu attiecināšana

Ministru kabinets nosaka kritērijus un kārtību, kādā Latvija veic kiberuzbrukumu attiecināšanu.

VI nodaļa
Koordinēta ievainojamību atklāšana un novēršana

39. pants. Koordinēta ievainojamību atklāšana

(1) Ja persona subjekta informācijas sistēmā vai elektronisko sakaru tīklā konstatē ievainojamību, tā nekavējoties, bet ne vēlāk kā piecu darbdienu laikā iesniedz ievainojamības atklāšanas ziņojumu kompetentajai kiberincidentu novēršanas institūcijai.

(2) Ievainojamības atklāšanas ziņojumā iekļauj šādu informāciju:

1) ievainojamības konstatēšanas datumu un laiku (ja iespējams);

2) ziņas par informācijas sistēmu vai elektronisko sakaru tīklu, kurā konstatēta ievainojamība;

3) ievainojamības aprakstu;

4) ievainojamības konstatēšanai izmantotās metodoloģijas vai veikto darbību secības aprakstu;

5) ievainojamības atklāšanas ziņojuma iesniedzēja kontaktinformāciju;

6) citas ziņas, ko ievainojamības atklāšanas ziņojuma iesniedzējs uzskata par nepieciešamām konstatētās ievainojamības identificēšanai un novēršanai.

(3) Kompetentā kiberincidentu novēršanas institūcija apstiprina ievainojamības atklāšanas ziņojuma saņemšanu, pārbauda ziņojumā ietverto informāciju un informē ziņojuma iesniedzēju par ziņojumā ietvertās informācijas pamatotību un ievainojamības novēršanas rezultātu.

(4) Ja ievainojamības atklāšanas ziņojumā sniegto informāciju par ievainojamību kiberincidentu novēršanas institūcija novērtējusi kā pamatotu, kiberincidentu novēršanas institūcija par to nekavējoties informē attiecīgo subjektu u n Satversmes aizsardzības biroju, ja tas ir attiecināms uz informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru.

(5) Ievainojamības atklāšana nedrīkst tikt izmantota ļaunprātīgi. Informācija par atklāto ievainojamību ir ierobežotas pieejamības informācija, ja vien normatīvie akti neparedz augstāku klasifikācijas pakāpi. Ievainojamības atklāšanas ziņojuma iesniedzējs un attiecīgais subjekts ir atbildīgi par minētās informācijas neizpaušanu. Kompetentā kiberincidentu novēršanas institūcija nosaka nosacījumus, kārtību un apjomu, kādā var tikt izpausta informācija par konkrētu atklāto ievainojamību.

(6) Ievainojamības atklāšanas ziņojuma iesniedzējs ir tiesīgs iesniegt ievainojamības atklāšanas ziņojumu anonīmi vai lūgt kompetento kiberincidentu novēršanas institūciju neatklāt ziņojuma iesniedzēja identitāti. Šādā gadījumā kompetentās kiberincidentu novēršanas institūcijas pienākums ir nodrošināt ziņojuma iesniedzēja identitātes konfidencialitāti, ja vien ziņojuma iesniedzējs ievēro šajā likumā noteiktās prasības un pirmšķietami nav konstatējamas noziedzīga nodarījuma pazīmes. Minētais konfidencialitātes nodrošināšanas pienākums neattiecas uz šā likuma 13. panta trešās daļas 7. un 8. punktā minētajām institūcijām. Ievainojamības atklāšanas ziņojuma anonīma iesniegšana neatbrīvo ievainojamības atklāšanas ziņojuma iesniedzēju no pienākuma neizpaust informāciju par ievainojamību.

40. pants. Koordinēta ievainojamību novēršana

(1) Subjekts kompetentās kiberincidentu novēršanas institūcijas noteiktajā termiņā, bet ne vēlāk kā 90 dienu laikā pēc informācijas saņemšanas veic ievainojamības novēršanai nepieciešamās darbības un par ievainojamības novēršanas gaitu informē kompetento kiberincidentu novēršanas institūciju.

(2) Ja objektīvu iemeslu dēļ ievainojamību nav iespējams novērst šā panta pirmajā daļā norādītajā termiņā, pēc subjekta pieprasījuma kiberincidentu novēršanas institūcija var pagarināt ievainojamības novēršanas termiņu, bet ne vairāk kā līdz 180 dienām no ievainojamības atklāšanas ziņojuma iesniegšanas brīža, par to informējot ievainojamības atklāšanas ziņojuma iesniedzēju.

(3) Personas, uz kurām neattiecas šā panta pirmajā daļā noteiktie pienākumi, pēc savas iniciatīvas var vienoties ar ievainojamības atklāšanas ziņojuma iesniedzēju par ievainojamības novēršanas termiņu un par ievainojamības novēršanas gaitu informēt kompetento kiberincidentu novēršanas institūciju.

(4) Kompetentā kiberincidentu novēršanas institūcija sniedz atbalstu ievainojamības atklāšanas ziņojuma iesniedzēja un attiecīgā subjekta saziņā, ja kāda no pusēm izsaka šādu vēlmi. Kompetentā kiberincidentu novēršanas institūcija veic atklātās ievainojamības novēršanas pēckontroli, kā arī nodrošina ievainojamības atklāšanas ziņojuma iesniedzēja konfidencialitāti atbilstoši šā likuma 39. panta sestajai daļai.

(5) Ja atklātā ievainojamība ietekmē vairākus subjektus, kompetentā kiberincidentu novēršanas institūcija koordinē šīs ievainojamības novēršanu sadarbībā ar visiem minētajiem subjektiem.

(6) Ja atklātā ievainojamība var būtiski ietekmēt būtisko pakalpojumu vai svarīgo pakalpojumu sniegšanu vai saņemšanu citā Eiropas Savienības dalībvalstī, kompetentā kiberincidentu novēršanas institūcija sadarbojas ar šīs

valsts kiberincidentu novēršanas institūcijām minētās ievainojamības novēršanā. Ja atklātā ievainojamība skar vairāk nekā divas Eiropas Savienības dalībvalstis, kompetentā kiberincidentu novēršanas institūcija sadarbojas ar šo valstu kiberincidentu novēršanas institūcijām, izmantojot CSIRT tīklu.

VII nodaļa
Subjektu uzraudzība un izpildes panākšanas pasākumi

41. pants. Uzraugošās iestādes

Subjektu uzraudzību veic:

1) Nacionālais kiberdrošības centrs — attiecībā uz būtisko pakalpojumu un svarīgo pakalpojumu sniedzējiem, izņemot informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru;

2) Satversmes aizsardzības birojs — attiecībā uz informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru.

42. pants. Subjektu uzraudzība

(1) Subjektu uzraudzība ietver kiberdrošības prasību ievērošanas kontroli, informācijas un komunikācijas tehnoloģiju klātienes pārbaudes un attālinātu pārraudzību, datu un dokumentu pārbaudes, tostarp attiecībā uz risku vadību un auditos vai atbilstības novērtējumos konstatēto nepilnību novēršanu, kā arī subjekta elektronisko sakaru tīklu un informācijas sistēmu drošības skenēšanu.

(2) Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam ir tiesīgi prioritizēt šā panta pirmajā daļā minēto uzraudzības pasākumu īstenošanu, izvērtējot aktuālos kiberriskus.

(3) Ministru kabinets nosaka kritērijus un kārtību šā panta pirmajā daļā minētās drošības skenēšanas veikšanai.

43. pants. Subjektu atbilstības pašvērtējuma ziņojums

(1) Subjekts atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam iesniedz Nacionālajam kiberdrošības centram vai Satversmes aizsardzības birojam subjekta atbilstības pašvērtējuma ziņojumu (turpmāk — pašvērtējuma ziņojums).

(2) Pašvērtējuma ziņojuma veidlapu un tajā iekļaujamās informācijas saturu un apjomu, kā arī pašvērtējuma ziņojuma iesniegšanas termiņu un regularitāti nosaka Ministru kabinets.
(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

44. pants. Subjektu atbilstības audits

(1) Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam ir tiesīgi veikt subjekta atbilstības auditu vai uzdot subjektam veikt ārēju auditu par subjekta atbilstību šajā likumā un Ministru kabineta noteikumos noteiktajām kiberdrošības prasībām, ja ir aizdomas par kiberdrošības pārkāpumiem vai tie ir konstatēti.

(2) Ārējo auditu veic neatkarīgs kiberdrošības auditors, kuram ar subjektu nav interešu konflikta un kurš atbilst kiberdrošības auditoram izvirzāmajām prasībām. Kiberdrošības auditoram izvirzāmās prasības nosaka Ministru kabinets.

(3) Informācijas un komunikācijas tehnoloģiju kritiskajā infrastruktūrā ārējo auditu veic šā panta otrajā daļā noteiktajiem kritērijiem atbilstošs ar Satversmes aizsardzības biroju saskaņots kiberdrošības auditors.

(4) Ārējā audita izmaksas sedz un auditā konstatētos pārkāpumus novērš attiecīgais subjekts.

(5) Pēc ārējā audita beigām subjekts nekavējoties iesniedz Nacionālajam kiberdrošības centram (informācijas un

komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs — Satversmes aizsardzības birojam) ārējā audita ziņojuma kopiju. Pēc Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja pieprasījuma subjekts uzrāda arī pierādījumus, kas bija par pamatu ārējā audita ziņojumā iekļautajiem secinājumiem.

(Ar grozījumiem, kas izdarīti ar 04.06.2026. likumu, kas stājas spēkā 18.06.2026.)

45. pants. Subjektu neatbilstības novēršana

(1) Ja konstatētas neatbilstības, Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam ir tiesīgi izteikt subjektam brīdinājumu vai uzdot subjektam:

1) veikt noteiktas darbības neatbilstības novēršanai, nosakot samērīgu termiņu neatbilstības novēršanai un kārtību ziņošanai par neatbilstības novēršanas gaitu;

2) nekavējoties pārtraukt un turpmāk nepieļaut rīcību, kas pārkāpj šajā likumā noteiktās prasības;

3) informēt pakalpojumu saņēmējus vai publicēt informāciju par kiberapdraudējumu, tā veidu un apmēru, kā arī tā novēršanai vai mazināšanai nepieciešamajām darbībām;

4) informēt pakalpojumu saņēmējus vai publicēt informāciju par konstatētajiem subjekta pārkāpumiem.

(2) Ja konstatētā neatbilstība rada nozīmīga kiberincidenta risku, Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs par konstatēto risku informē Ministru kabinetu, bet, ja neatbilstība apdraud nacionālo drošību, — Nacionālās drošības padomi.

(3) Subjekts nekavējoties veic visus nepieciešamos, piemērotos un samērīgos pasākumus neatbilstību novēršanai, tostarp izpilda Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja norādījumus.

(4) Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs ir tiesīgi veikt klātienes pārbaudes, tostarp norīkot amatpersonas pārraudzīt, kā subjekts noteiktā laikposmā pilda tam šajā likumā noteiktos pienākumus.

(5) Ja subjekts nepilda saskaņā ar šā panta pirmo daļu uzliktos tiesiskos pienākumus, Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam ir tiesīgi:

1) uzdot subjektam apturēt tā informācijas sistēmas, resursa vai elektroniskā pakalpojuma darbību līdz konstatētās neatbilstības novēršanai;

2) uzdot subjektam apturēt informācijas un komunikācijas tehnoloģiju produkta tirdzniecību vai pakalpojuma sniegšanu līdz konstatētās neatbilstības novēršanai;

3) uz laiku aizliegt jebkurai fiziskajai personai, kas subjektā ir atbildīga par vadības un pārstāvības pienākumu veikšanu izpildinstitūcijas līmenī vai tam līdzvērtīgā līmenī, veikt vadības un pārstāvības funkcijas.

(6) Lemjot par jebkuru no šā panta pirmajā vai piektajā daļā minētajiem izpildes panākšanas pasākumiem, Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs ņem vērā šādus apsvērumus:

1) neatbilstību smagumu un pārkāpto prasību nozīmīgumu, ņemot vērā to, ka par nozīmīgu neatbilstību šā likuma izpratnē ir uzskatāmi šādi gadījumi:

a) atkārtotu neatbilstību konstatēšana,

b) nozīmīgu incidentu nepaziņošana vai neatrisināšana,

c) konstatētās neatbilstības nenovēršana pretēji Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja sniegtajiem norādījumiem,

d) šķēršļu likšana auditiem vai uzraudzības darbībām, ko uzdevis Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs pēc neatbilstības konstatēšanas,

e) nepatiesas vai neprecīzas informācijas sniegšana saistībā ar kiberdrošības risku pārvaldības

pasākumiem vai ziņošanas pasākumiem;

2) neatbilstības ilgumu;

3) jebkādas iepriekš konstatētas attiecīgā subjekta neatbilstības;

4) jebkādu izraisīto materiālo vai nemateriālo kaitējumu, tai skaitā jebkādu finansiālo vai ekonomisko zaudējumu, ietekmi uz citiem pakalpojumiem un skarto lietotāju skaitu;

5) neatbilstības izraisītāja nodomu vai nolaidību;

6) jebkādus pasākumus, ko subjekts veicis, lai novērstu vai mazinātu materiālo vai nemateriālo kaitējumu;

7) vai subjekts ievēro iekšējos noteikumus, kas izdoti, lai izpildītu minimālās kiberdrošības prasības, kiberrisku pārvaldības un darbības nepārtrauktības plānu, kā arī subjektam saistošos starptautiskos un nacionālos standartus un sertifikācijas shēmas (ja attiecināms);

8) cik lielā mērā fiziskā persona, kura subjektā ir atbildīga par vadības un pārstāvības pienākumu veikšanu izpildinstitūcijas līmenī vai tam līdzvērtīgā līmenī sadarbojas ar Nacionālo kiberdrošības centru un Satversmes aizsardzības biroju.

(7) Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs šā panta piektās daļas 3. punktā minēto lēmumu nosūta subjektam.

(8) Šā panta piektās daļas 3. punktā minēto aizliegumu nepiemēro svarīgo pakalpojumu sniedzējam, kurš nav informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

(9) Šā panta piektās daļas 3. punktā minēto aizliegumu piemēro līdz brīdim, kad attiecīgais subjekts izpildījis tam saskaņā ar šā panta pirmo daļu uzliktos tiesiskos pienākumus.

(10) Kad subjekts ir izpildījis tam saskaņā ar šā panta pirmo daļu uzliktos tiesiskos pienākumus, Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam atceļ šā panta piektās daļas 3. punktā minēto aizliegumu.

(11) Šā panta piektās daļas 3. punktā minēto aizliegumu nepiemēro tiešās vai pastarpinātās pārvaldes iestādēm, citām valsts institūcijām un atvasinātām publiskajām personām.

(12) Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs atbilstoši šā likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam pirms šā panta piektās daļas 1. punktā minēto tiesību īstenošanas attiecībā uz Latvijas Bankas uzturētām informācijas sistēmām, resursiem vai elektroniskajiem pakalpojumiem konsultējas ar Latvijas Banku.

46. pants. Soda naudas piemērošana un piespiedu izpildes noteikumi

(1) Nacionālais kiberdrošības centrs ir tiesīgs par būtisku neatbilstību šajā likumā noteiktajām prasībām piemērot būtisko pakalpojumu sniedzējam soda naudu līdz 10 miljoniem *euro*, bet, ja būtisko pakalpojumu sniedzēja pēdējā finanšu gada kopējā neto apgrozījuma summa pārsniedz 500 miljonus *euro*, — līdz diviem procentiem no būtisko pakalpojumu sniedzēja pēdējā finanšu gada kopējā neto apgrozījuma.

(2) Nacionālais kiberdrošības centrs ir tiesīgs par būtisku neatbilstību šajā likumā noteiktajām prasībām piemērot svarīgo pakalpojumu sniedzējam soda naudu līdz septiņiem miljoniem *euro*, bet, ja svarīgo pakalpojumu sniedzēja pēdējā finanšu gada kopējā neto apgrozījuma summa pārsniedz 500 miljonus *euro*, — līdz 1,4 procentiem no svarīgo pakalpojumu sniedzēja pēdējā finanšu gada kopējā neto apgrozījuma.

(3) Satversmes aizsardzības birojs ir tiesīgs par būtisku neatbilstību šajā likumā noteiktajām prasībām piemērot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam soda naudu līdz 10 miljoniem *euro*, bet, ja informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja pēdējā finanšu gada kopējā neto apgrozījuma summa pārsniedz 500 miljonus *euro*, — līdz diviem procentiem no informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja pēdējā finanšu gada kopējā neto apgrozījuma.

(4) Ministru kabinets nosaka kārtību, kādā nosakāms finanšu gada neto apgrozījums, no kura aprēķina soda

naudu, un soda naudas apmēra noteikšanas kritērijus.

(5) Būtiska neatbilstība šā likuma izpratnē ir tas, ka:

1) subjekts neveic piemērotus un samērīgus tehniskos un organizatoriskos pasākumus kiberapdraudējuma vai kiberincidenta ietekmes mazināšanai;

2) subjekts vairākkārt atsakās pildīt Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja amatpersonu likumīgās prasības, kas saistītas ar šajā likumā subjektam noteikto pienākumu sniegt informāciju kiberdrošības uzraudzības ietvaros;

3) subjekts šajā likumā noteiktajā termiņā nepaziņo kompetentajai kiberincidentu novēršanas institūcijai par nozīmīgu kiberincidentu vai apzināti sniedz tai nepatiesu informāciju.

(6) Soda naudas apmērs ir nosakāms samērīgs ar izdarīto pārkāpumu. Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs, pieņemot lēmumu par soda naudas piemērošanu un tās apmēru, izvērtē un ņem vērā šā likuma 45. panta sestajā daļā minētos apsvērumus, kā arī personas mantisko stāvokli.

(7) Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja lēmumu par piemēroto soda naudu var pārsūdzēt tiesā Administratīvā procesa likumā noteiktajā kārtībā.

(8) Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja piemēroto soda naudu subjekts samaksā mēneša laikā no dienas, kad stājas spēkā lēmums par tās piemērošanu. Ja lēmums par soda naudas piemērošanu nav izpildīts labprātīgi, tā piespiedu izpildi veic tiesu izpildītājs. Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs ir atbrīvots no valsts nodevas par lēmuma iesniegšanu izpildei.

(9) Ja lēmumi, kas pieņemti saskaņā ar šā likuma 34. panta desmito daļu, 37. panta pirmo daļu un 45. panta pirmo daļu, nav izpildīti labprātīgi, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs tos izpilda piespiedu kārtā saskaņā ar Administratīvā procesa likumu. Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs, veicot uz noteiktu darbību vai darbības aizliegumu vērsta lēmuma piespiedu izpildi, var uzlikt piespiedu naudu — vienā reizē ne vairāk kā 10 000 *euro*.

(10) Uzliktās piespiedu naudas apmērs ir nosakāms samērīgs ar izdarīto pārkāpumu. Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs, nosakot šā panta piektajā daļā minētās piespiedu naudas apmēru, ņem vērā šā likuma 34. panta desmitajā daļā, 37. panta pirmajā daļā un 45. panta pirmajā daļā minēto lēmumu nepildīšanas ietekmi uz tīklu un informācijas sistēmu drošību, pārkāpuma ilgumu, kā arī citus apstākļus, kuriem ir nozīme lietā.

(11) Pirms izpildrīkojuma izdošanas Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs rakstveidā paziņo adresātam, ka ir iegūta informācija, kas nepieciešama izpildrīkojuma izdošanai. Adresāts septiņu dienu laikā pēc minētā paziņojuma saņemšanas var iepazīties ar lietu, izteikt savu viedokli un iesniegt papildu informāciju.

(12) Šo pantu nepiemēro tiešās vai pastarpinātās pārvaldes iestādēm, citām valsts institūcijām un atvasinātām publiskām personām.

(13) Samaksāto soda naudu vai piespiedu naudu ieskaita valsts pamatbudžetā.

Pārejas noteikumi

1. Ar šā likuma spēkā stāšanos spēku zaudē Informācijas tehnoloģiju drošības likums (Latvijas Vēstnesis, 2010, 178. nr.; 2012, 179. nr.; 2013, 228. nr.; 2015, 34. nr.; 2017, 132. nr.; 2018, 210. nr.).

2. Ministru kabinets līdz 2024. gada 17. oktobrim izdod šā likuma 9. panta ceturtajā daļā, 12. panta trešajā daļā, 17. panta otrajā daļā, 23. panta sestajā daļā, 24. panta otrajā daļā, 25. panta pirmajā daļā, 26. pantā, 28. panta otrajā daļā, 29. pantā, 31. pantā, 32. panta otrajā un trešajā daļā, 33. pantā, 34. panta pirmajā, septītajā un desmitajā daļā, 36. panta pirmajā daļā, 42. panta trešajā daļā, 43. panta otrajā daļā un 44. panta otrajā daļā minētos noteikumus.

3. Ministru kabinets līdz 2025. gada 1. aprīlim nosaka kritērijus un kārtību, kādā Latvija veic kiberuzbrukumu

attiecināšanu.

4. Ministru kabinets līdz 2025. gada 1. aprīlim izdod šā likuma 30. panta otrajā daļā minētos noteikumus.

5. Līdz šā likuma 17. panta otrajā daļā minēto noteikumu spēkā stāšanās dienai, bet ne ilgāk kā līdz 2025. gada 1. janvārim ir piemērojami Ministru kabineta 2016. gada 1. novembra noteikumi Nr. 695 "Digitālās drošības uzraudzības komitejas nolikums", ciktāl tie nav pretrunā ar šo likumu.

6. Līdz šā likuma 12. panta trešajā daļā, 24. panta otrajā daļā, 25. panta pirmajā daļā, 26. pantā, 28. panta otrajā daļā, 29. pantā, 30. panta otrajā daļā, 34. panta pirmajā, septītajā un desmitajā daļā, 36. panta pirmajā daļā, 42. panta trešajā daļā, 43. panta otrajā daļā un 44. panta otrajā daļā minēto noteikumu spēkā stāšanās dienai, bet ne ilgāk kā līdz 2024. gada 17. oktobrim ir piemērojami Ministru kabineta 2015. gada 28. jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" un 2011. gada 1. februāra noteikumi Nr. 100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība", ciktāl tie nav pretrunā ar šo likumu.

7. Veicot sākotnējo pašvērtējumu saskaņā ar šā likuma 22. panta pirmo daļu, persona par savu atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam paziņo Nacionālajam kiberdrošības centram ne vēlāk kā līdz 2025. gada 1. aprīlim. Ja atbilstība būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam ir iestājusies pēc minētā termiņa, persona par to paziņo Nacionālajam kiberdrošības centram šā likuma 22. panta pirmajā daļā noteiktajā termiņā.

8. Šā likuma 22. panta ceturtajā daļā minēto būtisko pakalpojumu un svarīgo pakalpojumu sniedzēju sarakstu apstiprina līdz 2025. gada 17. aprīlim.

9. Šā likuma 23. panta pirmajā daļā minēto informāciju par personas atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam paziņo Nacionālajam kiberdrošības centram ne vēlāk kā līdz 2025. gada 1. aprīlim. Ja atbilstība domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam ir iestājusies pēc minētā termiņa, persona par to paziņo Nacionālajam kiberdrošības centram šā likuma 23. panta pirmajā daļā noteiktajā termiņā.

10. Šā likuma 25. panta otrajā daļā minēto informāciju par subjekta kiberdrošības pārvaldnieka noteikšanu pirmreizēji paziņo Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam ne vēlāk kā līdz 2025. gada 1. oktobrim. Ja subjekta kiberdrošības pārvaldnieks tiek noteikts pēc minētā termiņa, subjekts par to paziņo Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam šā likuma 25. panta otrajā daļā noteiktajā termiņā.

11. Šā likuma 34. panta otro, trešo, ceturto un piekto daļu piemēro no 2025. gada 1. jūlija.

12. Šā likuma 43. panta pirmajā daļā minēto pašvērtējuma ziņojumu pirmreizēji iesniedz Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam ne vēlāk kā līdz 2025. gada 1. oktobrim.

13. Būtisko pakalpojumu sniedzēji, kas ir finanšu vienības regulas 2022/2554 2. panta 2. punkta izpratnē, līdz 2025. gada 17. janvārim attiecībā uz risku pārvaldību — trešo personu saistīto risku pārvaldību, darbības noturību, testēšanu un incidentu ziņošanu — piemēro attiecīgo jomu regulējošos normatīvajos aktos noteiktās prasības.

14. Līdz šā likuma 44. panta otrajā daļā minēto Ministru kabineta noteikumu spēkā stāšanās dienai, bet ne ilgāk kā līdz 2026. gada 1. decembrim kiberdrošības auditoram piemēro tās prasības, kas Ministru kabineta 2025. gada 25. jūnija noteikumos Nr. 397 "Minimālās kiberdrošības prasības" bija noteiktas, lai auditors varētu tikt reģistrēts kiberdrošības auditoru sarakstā.

(04.06.2026. likuma redakcijā, kas stājas spēkā 18.06.2026.)

15. Grozījumi šā likuma 20. panta 11. punktā par nacionālajai drošībai nozīmīgām komercsabiedrībām, nodibinājumiem un biedrībām stājas spēkā 2026. gada 1. oktobrī.

(04.06.2026. likuma redakcijā, kas stājas spēkā 18.06.2026.)

Informatīva atsauce uz Eiropas Savienības direktīvām

Likumā iekļautas tiesību normas, kas izriet no:

1) 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);

2) Eiropas Parlamenta un Padomes 2018. gada 11. decembra direktīvas (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija).

Likums stājas spēkā 2024. gada 1. septembrī.

Likums Saeimā pieņemts 2024. gada 20. jūnijā.

Valsts prezidenta vietā
Saeimas priekšsēdētāja *D. Mieriņa*

Rīgā 2024. gada 4. jūlijā

© Oficiālais izdevējs "Latvijas Vēstnesis"