Likumprojekts

**Grozījumi Informācijas tehnoloģiju drošības likumā**

Izdarīt [Informācijas tehnoloģiju drošības likumā](http://likumi.lv/doc.php?id=220962" \t "_blank) (Latvijas Vēstnesis, 2010, 178. nr.; 2012, 179. nr.; 2013, 228. nr.; 2015, 34. nr.; 2017, 132. nr.) šādus grozījumus:

1. Papildināt likumu ar 3.1 pantu šādā redakcijā:

“**3.1 pants. Pamatpakalpojuma sniedzējs, digitālā pakalpojuma sniedzējs un digitālā pakalpojuma sniedzēja pārstāvis**

1. Pamatpakalpojuma sniedzējs:

1) ir valsts vai pašvaldības institūcija vai privāto tiesību juridiska persona, kas veic saimniecisko darbību Latvijas Republikā;

2) sniedz pakalpojumu enerģētikas, transporta, banku, finanšu tirgus infrastruktūras, veselības, dzeramā ūdens piegādes vai izplatīšanas, elektronisko sakaru un digitālās infrastruktūras nozarē kādā no Eiropas Savienības dalībvalstīm;

3) sniedz pakalpojumu, kas ir svarīgs sabiedrisku vai ekonomisku darbību nodrošināšanai;

4) sniedz pakalpojumu, kura sniegšana ir atkarīga no informācijas tehnoloģijām, tostarp tīklu un informācijas sistēmām un

5) sniedz pakalpojumu un informācijas tehnoloģiju drošības incidents var radīt būtiski traucējošu ietekmi uz tā sniegšanu.

(2) Digitālā pakalpojuma sniedzējs ir:

1) privāto tiesību juridiska persona, kas veic saimniecisko darbību Latvijas Republikā un sniedz pakalpojumu par atlīdzību no attāluma, izmantojot elektroniskos līdzekļus, un pēc pakalpojuma saņēmēja individuāla pieprasījuma un sniedz tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai mākoņdatošanas pakalpojumu (turpmāk – digitālais pakalpojums) kādā no Eiropas Savienības dalībvalstīm;

2) privāto tiesību juridiska persona, kas veic saimniecisko darbību ārpus Eiropas Savienības un digitālo pakalpojumu sniedz Latvijas Republikā ar pilnvarota pārstāvja starpniecību.

(3) Par digitālā pakalpojuma sniedzēja pārstāvi var būt fiziska persona vai privāto tiesību juridiska persona, kas veic saimniecisko darbību Latvijas Republikā. Uz digitālā pakalpojuma sniedzēja pārstāvi attiecas šajā likumā noteiktie digitālā pakalpojuma sniedzēja pienākumi un tiesības.

 (4) Šā panta pirmā, otrā un trešā daļa neattiecas uz elektronisko sakaru komersantu un uzticamu sertifikācijas pakalpojumu sniedzēju. Šā panta otrā un trešā daļa neattiecas uz privāto tiesību juridisko personu, kas nodarbina mazāk par 250 personām un tā gada apgrozījums nepārsniedz 50 miljonus *euro* vai gada bilances kopsumma nepārsniedz 43 miljonus *euro*.

 (5) Ministru kabinets nosaka šā panta pirmās daļas 5. punktā minētā informācijas tehnoloģiju drošības incidenta būtiski traucējošās ietekmes identificējošos faktorus šā panta pirmās daļas 2. punktā minētajās nozarēs un kārtību kādā enerģētikas, transporta, banku, finanšu tirgus infrastruktūras, veselības, dzeramā ūdens piegādes vai izplatīšanas, elektronisko sakaru un digitālās infrastruktūras uzraugošā ministrija (turpmāk – nozari uzraugošā ministrija) identificē pamatpakalpojuma sniedzējus un pamatpakalpojumus un iesniedz informāciju par identificētajiem pamatpakalpojuma sniedzējiem un pamatpakalpojumiem Digitālās drošības uzraudzības komitejā.”.

1. 5. pantā:

papildināt pirmās daļas 6. punktu aiz vārdiem “pašvaldību institūcijas” ar vārdiem “pamatpakalpojuma sniedzēji, digitālā pakalpojuma sniedzēji”;

papildināt pirmo daļu ar 7.1, 7.2, 7.3, 7.4 un 7.5 punktu šādā redakcijā:

“71) informē Aizsardzības ministriju par šā likuma 6. panta otrajā prim daļā minēto drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību, un citas Eiropas Savienības dalībvalsts kompetento iestādi par drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību konkrētajā dalībvalstī. Ar Eiropas Savienības dalībvalsts kompetento iestādi šā likuma izpratnē saprot Eiropas Savienības dalībvalsts izraudzītu iestādi, kura atbild par pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošību konkrētajā dalībvalstī un uzrauga to darbību;

72) informē Aizsardzības ministriju par šā likuma 6. panta otrajā prim daļā minēto drošības incidentu, kuram ir būtiska ietekme uz digitālā pakalpojuma sniegšanu, un citas Eiropas Savienības dalībvalstu kompetentās iestādes, ja drošības incidentam ir būtiska ietekme uz digitālā pakalpojuma sniegšanu vismaz divās Eiropas Savienības dalībvalstīs;

73) informē Digitālās drošības uzraudzības komiteju par konstatēto pamatpakalpojuma sniedzēja vai digitālā pakalpojuma sniedzēja informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošības prasību neatbilstību normatīvajiem aktiem, kas nosaka informācijas tehnoloģiju drošības prasības un atklātajiem gadījumiem, kad pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs nav ziņojis par drošības incidentu saskaņā ar šā likuma 6. panta septīto daļu;

74) var prasīt, lai Aizsardzības ministrija nosūta citu Eiropas Savienības dalībvalstu kontaktpunktiem informāciju par šā likuma 6. panta otrajā prim daļā minēto drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu konkrētajā dalībvalstī. Ar Eiropas Savienības dalībvalsts kontaktpunktu šā likuma izpratnē saprot Eiropas Savienības dalībvalsts izraudzītu iestādi, kura atbild par pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošību konkrētajā dalībvalstī un koordinē sadarbību, nodrošinot pārrobežu sadarbību ar citām dalībvalstīm, Tīklu un informācijas sistēmu drošības direktīvas sadarbības grupu (turpmāk – NIS Sadarbības grupa) un datordrošības incidentu reaģēšanas vienību tīklu (turpmāk – NIS CSIRT tīkls).

NIS Sadarbības grupa sastāv no dalībvalstu, Eiropas Komisijas un Eiropas Savienības Tīklu un informācijas drošības aģentūras (turpmāk – ENISA) pārstāvjiem. NIS Sadarbības grupa izveidota, lai atbalstītu un atvieglotu stratēģisko sadarbību un apmaiņu ar informāciju starp dalībvalstīm, lai attīstītu uzticēšanos un paļāvību, kā arī nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību Eiropas Savienībā.

NIS CSIRT tīkls sastāv no dalībvalstu datordrošības incidentu reaģēšanas vienību (turpmāk – dalībvalstu CERT) un Eiropas institūciju datordrošības incidentu reaģēšanas vienības pārstāvjiem. Eiropas Komisija NIS CSIRT tīklā piedalās novērotāja statusā un ENISA nodrošina sekretariātu un aktīvi atbalsta sadarbību starp dalībvalstu CERT. NIS CSIRT tīkls izveidots, lai palīdzētu attīstīt paļāvību un uzticēšanos starp dalībvalstīm un veicinātu ātru un efektīvu operatīvo sadarbību;

75)sadarbojas ar NIS CSIRT tīklu;”;

aizstāt pirmajā prim daļā ciparus un vārdu “ 2., 4., 5., 6., 7. un 8.” ar cipariem un vārdu “2., 4., 5., 6., 7., 7.1., 7.2., 7.3.,7.4., 7.5 un8.”;

papildināt otrās daļas 1. punktu pēc vārdiem “juridiskajām personām” ar vārdiem “informāciju par informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošības prasībām un”.

1. Papildināt likumu ar 5.1 un5.2 pantu šādā redakcijā:

“**5.1 pants.** **Digitālās drošības uzraudzības komitejas uzdevumi un tiesības**

1. Digitālās drošības uzraudzības komiteja:

1) sadarbojas ar nozari uzraugošajām ministrijām pamatpakalpojuma sniedzēju un pamatpakalpojumu identificēšanas procesā, tajā skaitā apkopo nozaru uzraugošo ministriju iesniegto informāciju par identificētajiem pamatpakalpojuma sniedzējiem un pamatpakalpojumiem un reizi divos gados sagatavo pamatpakalpojumu sniedzēju un pamatpakalpojumu sarakstu, un rakstiski informē identificētos pakalpojuma sniedzējus;

2) reizi divos gados Eiropas Komisijai iesniedz informāciju par kārtību, kādā identificē pamatpakalpojuma sniedzējus, pamatpakalpojumu sarakstu, identificēto pamatpakalpojuma sniedzēju skaitu katrā no šā likuma 3.1 panta pirmajās daļas 2. punktā minētajām nozarēm un šā likuma 3.1 panta piektajā daļā minētos informācijas tehnoloģiju drošības incidenta būtiski traucējošās ietekmes identificējošos faktorus.

3) pieprasa, lai pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs novērš konstatētās informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošības prasību neatbilstības;

4) pieprasa, lai pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs izpilda šā likuma 6. panta otrajā prim daļā noteikto pienākumu.

(2) Digitālās drošības uzraudzības komiteja kontrolē šā panta pirmās daļas 3. un 4. punktā minēto uzdevumu izpildi. Ja pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs nepilda uzdevumu, Digitālās drošības uzraudzības komiteja veic lēmuma piespiedu izpildi Administratīvā procesa likumā noteiktajā kārtībā.

 **5.2 pants.** **Aizsardzības ministrijas uzdevumi**

Aizsardzības ministrija:

1) sadarbojas ar citu Eiropas Savienības dalībvalstu kontaktpunktiem, tostarp pēc kompetentās Drošības incidentu novēršanas institūcijas pieprasījuma nosūta tiem informāciju par šā likuma 6. panta otrajā prim daļā minētajiem drošības incidentiem, kuriem ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu konkrētajā dalībvalstī;

2) sadarbojas un vienu reizi gadā iesniedz NIS Sadarbības grupai ziņojumu par saņemto informāciju par šā likuma 6. panta otrajā prim daļā minētajiem drošības incidentiem, tostarp ziņojumu skaitu, informāciju par drošības incidentu raksturu, kā arī sniegtajiem ziņojumiem citu Eiropas Savienības dalībvalstu kompetentajām iestādēm;

3) informē Eiropas Komisiju par nacionālās kiberdrošības stratēģijas apstiprināšanu ne vēlāk kā trīs mēnešus pēc tās apstiprināšanas.”.

1. 6. pantā:

papildināt pantu ar otro prim daļu šādā redakcijā:

“(21) Pamatpakalpojuma sniedzējs un digitālā pakalpojuma sniedzējs, kas nav valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, drošības incidenta gadījumā nekavējoties veic visas tā novēršanai nepieciešamās darbības (it īpaši izpilda kompetentās Drošības incidentu novēršanas institūcijas rekomendācijas par vēlamo sākotnējo rīcību drošības incidenta gadījumā), kā arī šā panta septītajā daļā minētajos gadījumos un kārtībā tūlīt informē kompetento Drošības incidentu novēršanas institūciju par drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu. Kompetentā Drošības incidentu novēršanas institūcija vienojas ar pamatpakalpojuma sniedzēju vai digitālā pakalpojuma sniedzēju par atbalsta sniegšanu drošības incidenta novēršanā. Kompetentā Drošības incidentu novēršanas institūcija pēc apspriešanās ar pamatpakalpojuma sniedzēju vai digitālā pakalpojuma sniedzēju var informēt sabiedrību vai arī prasīt, lai to dara attiecīgais pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs, ja drošības incidenta publiskošana var atrisināt vai novērst to, vai kādā citā ziņā ir sabiedrības interesēs.”;

papildināt trešo daļu pēc vārda “otrajā” ar vārdiem “un otrajā prim”;

papildināt pantu ar septīto daļu šādā redakcijā:

“(7) Ministru kabinets nosaka šā panta otrajā prim daļā minētā drošības incidenta būtiskuma kritērijus, informēšanas kārtību un ziņojuma saturu.”.

1. 8. pantā:

papildināt panta nosaukumu pēc vārdiem “pašvaldību institūciju” ar vārdiem “informācijas tehnoloģiju kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju, pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju”;

papildināt pirmo daļu pēc vārdiem “pašvaldību institūciju” ar vārdiem “informācijas tehnoloģiju kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju, pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju”;

papildināt otro daļu pēc vārdiem “pašvaldības institūcijas” ar vārdiem “pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja”;

papildināt ceturto daļu pēc vārdiem “pašvaldības institūcija” ar vārdiem “pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs”;

papildināt piekto daļu pēc vārdiem “pašvaldību institūcijas” ar vārdiem “informācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji”.

papildināt pantu ar sesto daļu šādā redakcijā:

“(6) Ministru kabinets nosaka informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošības prasības pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem, uz kuriem neattiecas šā panta piektajā daļā minētās prasības.”.

6. Papildināt likumu ar 11. pantu šādā redakcijā:

“**11. Nacionālā kiberdrošības stratēģija**

(1) Nacionālā kiberdrošības stratēģija nosaka kiberdrošības politikas veidošanas pamatprincipus, mērķi un stratēģiskās prioritātes, tostarp, elektronisko sakaru tīklu un informācijas sistēmu drošības mērķus, politikas un regulatīvus pasākumus, lai panāktu un saglabātu augsta līmeņa elektronisko sakaru tīklu un informācijas sistēmu drošību, kas attiecas uz pamatpakalpojuma sniedzējiem, pamatpakalpojumiem, digitālā pakalpojuma sniedzējiem un digitālajiem pakalpojumiem;

(2) Nacionālo kiberdrošības stratēģijas izstrādi reizi četros gados nodrošina Aizsardzības ministrija un to apstiprina Ministru kabinets.”.

7. Papildināt likuma Pārejas noteikumus ar 6., 7., 8. un 9. punktu šādā redakcijā:

“6. Ministru kabinets līdz 2018. gada 1. augustam izdod šā likuma 3.1panta piektajā daļā paredzētos noteikumus.

7. Digitālās drošības uzraudzības komiteja šā likuma 5.1 panta pirmā daļas otrajā punktā minēto informāciju pirmo reizi Eiropas Komisijai iesniedz līdz 2018. gada 9. novembrim.

8. Aizsardzības ministrija šā likuma 5.2panta 2. punktā minēto ziņojumu pirmo reizi NIS Sadarbības grupai iesniedz līdz 2018. gada 9. augustam.

9. Ministru kabinets šā likuma 11. panta otrajā daļā minēto nacionālo kiberdrošības stratēģiju apstiprina līdz 2019. gada 1. janvārim.”.

8. Izteikt likuma “Informatīvā atsauce uz Eiropas Savienības direktīvu” šādā redakcijā:

“**Informatīvā atsauce uz Eiropas Savienības direktīvām**

Likumā iekļautas tiesību normas, kas izriet no:

1) Eiropas Parlamenta un Padomes 2009. gada 25. novembra direktīvas [2009/140/EK](http://eur-lex.europa.eu/eli/dir/2009/140/oj/?locale=LV" \t "_blank), ar ko izdara grozījumus direktīvā [2002/21/EK](http://eur-lex.europa.eu/eli/dir/2002/21/oj/?locale=LV" \t "_blank) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem, direktīvā [2002/19/EK](http://eur-lex.europa.eu/eli/dir/2002/19/oj/?locale=LV" \t "_blank) par piekļuvi elektronisko komunikāciju tīkliem un ar tiem saistītām iekārtām un to savstarpēju savienojumu un direktīvā [2002/20/EK](http://eur-lex.europa.eu/eli/dir/2002/20/oj/?locale=LV" \t "_blank) par elektronisko komunikāciju tīklu un pakalpojumu atļaušanu;

2) Eiropas Parlamenta un Padomes 2016. gada 6. jūlija direktīvas (ES) 2016/1148/EK par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.”.

|  |
| --- |
|  |

Aizsardzības ministrs                                                         Raimonds Bergmanis