Izdevējs: Saeima
Veids: likums
Pieņemts: 28.10.2010.
Stājas spēkā: 01.02.2011.

Publicēts:
"Latvijas Vēstnesis", 178 (4370), 10.11.2010.

Attēlotā redakcija: 25.10.2018. - ...

Grozījumi:

01.11.2012. likums / LV, 179 (4782), 13.11.2012. / Stājas spēkā 01.01.2013.
06.11.2013. likums / LV, 228 (5034), 22.11.2013. / Stājas spēkā 01.01.2014.
05.02.2015. likums / LV, 34 (5352), 18.02.2015. / Stājas spēkā 04.03.2015.
15.06.2017. likums / LV, 132 (5959), 05.07.2017. / Stājas spēkā 19.07.2017.
11.10.2018. likums / LV, 210 (6296), 24.10.2018. / Stājas spēkā 25.10.2018.

Saeima ir pieņēmusi un Valsts prezidents izsludina šādu likumu:

Informācijas tehnoloģiju drošības likums

1.pants. Likuma mērķis

(1) Likuma mērķis ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas šīs tehnoloģijas.

(2) Informācijas tehnoloģiju drošība ir sargājama tā, lai varētu savlaicīgi prognozēt un novērst, kā arī pārvarēt šīs drošības apdraudējumu un likvidēt tā sekas.

(3) Informācijas tehnoloģijas šā likuma izpratnē ir tehnoloģijas, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, dzēšanu, glabāšanu, attēlošanu vai pārsūtīšanu.

2.pants. Likuma darbība

(1) Likums attiecas uz valsts un pašvaldību institūcijām, kā arī uz komersantiem un citām privāto tiesību juridiskajām personām (turpmāk — privāto tiesību juridiskās personas).

(2) Likums neattiecas uz elektronisko sakaru tīklos pārraidāmās informācijas saturu (piemēram, uz informācijas sabiedrības pakalpojumu saturu un audiovizuālajiem darbiem).

3.pants. Informācijas tehnoloģiju kritiskā infrastruktūra

(1) Informācijas tehnoloģiju kritiskā infrastruktūra ir infrastruktūra, kuru atbilstoši Nacionālās drošības likumam apstiprina Ministru kabinets.

(2) Informācijas tehnoloģiju kritisko infrastruktūru aizsargā, lai nodrošinātu valstij un sabiedrībai būtisku pamatfunkciju veikšanu. Turklāt tiek nodrošināta informācijas tehnoloģiju kritiskās infrastruktūras integritāte, pieejamība un konfidencialitāte.

(3) Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtību nosaka Ministru kabinets.

3.[1] pants. Pamatpakalpojuma sniedzējs, digitālā pakalpojuma sniedzējs un digitālā pakalpojuma sniedzēja pārstāvis

(1) Pamatpakalpojuma sniedzējs ir valsts vai pašvaldības institūcija vai privāto tiesību juridiskā persona, kas veic saimniecisko darbību Latvijas Republikā un sniedz:

1) finanšu pakalpojumus Kredītiestāžu likuma izpratnē un finanšu tirgus infrastruktūras pakalpojumus, dzeramā ūdens piegādes vai izplatīšanas pakalpojumus, interneta plūsmas apmaiņas punkta pakalpojumus, domēnu nosaukumu sistēmas pakalpojumus, augstākā līmeņa domēna nosaukumu reģistra pakalpojumus vai pakalpojumus enerģētikas, transporta vai veselības nozarē kādā no Eiropas Savienības dalībvalstīm;

2) pakalpojumus, kuru sniegšana ir atkarīga no informācijas tehnoloģijām;

3) pakalpojumus, uz kuru sniegšanu būtiski traucējošu ietekmi var radīt informācijas tehnoloģiju drošības incidents.

(2) Digitālā pakalpojuma sniedzējs ir privāto tiesību juridiskā persona, kas atbilst vienai no šādām pazīmēm:

1) veic saimniecisko darbību Latvijas Republikā un sniedz tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai mākoņdatošanas pakalpojumu (turpmāk — digitālais pakalpojums) kādā no Eiropas Savienības dalībvalstīm;

2) veic saimniecisko darbību ārpus Eiropas Savienības un digitālo pakalpojumu Latvijas Republikā sniedz ar pilnvarota pārstāvja starpniecību.

(3) Par digitālā pakalpojuma sniedzēja pārstāvi var būt fiziskā persona vai privāto tiesību juridiskā 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, kuras darbinieku skaits nepārsniedz 50 personas un kuras gada apgrozījums vai bilances kopsumma nepārsniedz 10 miljonus *euro*.

(5) Lēmumu par pamatpakalpojuma sniedzēja un pamatpakalpojuma statusa piešķiršanu, pārskatīšanu un izbeigšanu pieņem par dzeramā ūdens piegādes vai izplatīšanas pakalpojumu jomu, interneta plūsmas apmaiņas punkta pakalpojumu jomu, domēnu nosaukumu sistēmas pakalpojumu jomu, augstākā līmeņa domēna nosaukumu reģistra pakalpojumu jomu un par enerģētikas, transporta un veselības nozari atbildīgā ministrija (turpmāk — par jomu un nozari atbildīgā ministrija). Lēmuma apstrīdēšana un pārsūdzēšana neaptur tā darbību.

(6) Nosacījumus informācijas tehnoloģiju drošības incidenta būtiski traucējošās ietekmes noteikšanai, kārtību, kādā pieprasa informāciju no privāto tiesību juridiskajām personām, kā arī pamatpakalpojuma sniedzēja un pamatpakalpojuma statusa piešķiršanas, pārskatīšanas un izbeigšanas nosacījumus un kārtību, kādā Digitālās drošības uzraudzības komiteju informē par pamatpakalpojumiem un to sniedzējiem, nosaka Ministru kabinets.
(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

4. pants. Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas

(1) Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (turpmāk — Drošības incidentu novēršanas institūcijas) veicina informācijas tehnoloģiju drošību Latvijas Republikā. Drošības incidentu 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 šīs daļas 1. punktā noteikto), kā arī privāto tiesību juridiskajām personām.

(2) Latvijas Universitātes Matemātikas un informātikas institūts tam noteiktos uzdevumus izpilda un tiesības īsteno Aizsardzības ministrijas pakļautībā atbilstoši normatīvajiem aktiem, deleģēšanas līguma noteikumiem un piešķirtajiem valsts budžeta līdzekļiem. Pieņemot pārvaldes lēmumus, Latvijas Universitātes Matemātikas un informātikas institūts ievēro Valsts pārvaldes iekārtas likuma prasības.

(3) Drošības incidentu novēršanas institūcijās personas tiek nodarbinātas dienesta vai darba tiesisko attiecību ietvaros, ja tās ir tiesīgas saņemt speciālo atļauju pieejai valsts noslēpumam un atbilst citām tiesību aktos izvirzītajām prasībām.

(4) Drošības incidentu novēršanas institūcijas šajā likumā noteiktos uzdevumus izpilda atbilstoši tām piešķirtajiem valsts budžeta līdzekļiem, un šīm institūcijām nav tiesību pieprasīt samaksu par veiktajām darbībām.

(5) Valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām ir pienākums sadarboties ar Drošības incidentu novēršanas institūcijām, sniedzot tām nepieciešamo informāciju un pildot to likumīgās prasības.

(6) Valsts apdraudējuma gadījumā Ministru kabinets var pieņemt lēmumu par Latvijas Universitātes Matemātikas un informātikas institūtam noteikto uzdevumu, tiesību un resursu nodošanu Nacionālajiem bruņotajiem spēkiem.

(7) Šajā likumā noteikto tiesību īstenošanai izdoto tiešu valsts drošības vai informācijas tehnoloģiju drošības apdraudējumu novēršanai paredzēto administratīvo aktu apstrīdēšana vai pārsūdzēšana neaptur šo aktu darbību. Tas neattiecas uz administratīvajiem aktiem par administratīvo sodu uzlikšanu.

(15.06.2017. likuma redakcijā, kas stājas spēkā 19.07.2017.)

4.[1] pants. Drošības incidentu novēršanas institūciju sadarbība

(1) Militārās izlūkošanas un drošības dienests sniedz informāciju Latvijas Universitātes Matemātikas un informātikas institūtam, lai tas nodrošinātu šā likuma 5. panta pirmās daļas 1. un 3. punktā noteikto uzdevumu īstenošanu, kā arī citu tā rīcībā esošo informāciju par Latvijas Universitātes Matemātikas un informātikas institūta kompetencē esošajiem informācijas tehnoloģiju drošības incidentiem.

(2) Latvijas Universitātes Matemātikas un informātikas institūts informē Militārās izlūkošanas un drošības dienestu par savā rīcībā esošo informāciju par informācijas tehnoloģiju drošības incidentiem Aizsardzības ministrijā, tās padotībā esošajās iestādēs un Nacionālajos bruņotajos spēkos.

(3) Drošības incidentu novēršanas institūcijas regulāri savstarpēji apmainās ar informāciju par aktualitātēm informācijas tehnoloģiju drošības incidentu jomā.

(15.06.2017. likuma redakcijā, kas stājas spēkā 19.07.2017.)

5.pants. Drošības incidentu novēršanas institūciju uzdevumi un tiesības

(1) Latvijas Universitātes Matemātikas un informātikas institūts:

1) uztur vienotu elektroniskās informācijas telpā notiekošo darbību ataino jumu;

2) sniedz atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinē to novēršanu;

3) uztur sabiedrībai pieejamā veidā atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu;

4) veic pētniecisko darbu, organizē izglītojošus pasākumus, apmācību un mācības informācijas tehnoloģiju drošības jomā;

5) sniedz atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas tehnoloģiju jomā, ievērojot normatīvajos aktos noteiktos datu apstrādes ierobežojumus;

6) uzrauga, kā valsts un pašvaldību institūcijas, pamatpakalpojuma sniedzēji, digitālā pakalpojuma sniedzēji un elektronisko sakaru komersanti izpilda šajā likumā noteiktos pienākumus;

7) sadarbojas ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām);

7[1]) informē Aizsardzības ministriju par šā likuma 6. panta 2.[1] daļā minēto drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību, un informē 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 drošību konkrētajā dalībvalstī un uzrauga to darbību;

7^{2}) informē Aizsardzības ministriju par šā likuma 6. panta $2.^{1}$ daļā minēto drošības incidentu, kuram ir būtiska ietekme uz digitālā pakalpojuma sniegšanu, un informē citas Eiropas Savienības dalībvalstu kompetentās iestādes, ja drošības incidentam ir būtiska ietekme uz digitālā pakalpojuma sniegšanu vismaz divās Eiropas Savienības dalībvalstīs;

7^{3}) informē Digitālās drošības uzraudzības komiteju par konstatēto pamatpakalpojuma sniedzēja vai digitālā pakalpojuma sniedzēja informācijas tehnoloģiju drošības prasību neatbilstību normatīvajiem aktiem, kuri nosaka informācijas tehnoloģiju drošības prasības, un par atklātajiem gadījumiem, kad pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs nav ziņojis par drošības incidentu saskaņā ar šā likuma 6. panta septīto daļu;

7^{4}) var lūgt, lai Aizsardzības ministrija nosūta citu Eiropas Savienības dalībvalstu kontaktpunktiem informāciju par šā likuma 6. panta $2.^{1}$ daļā minēto drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu konkrētajā dalībvalstī. Eiropas Savienības dalībvalsts kontaktpunkts šā likuma izpratnē ir Eiropas Savienības dalībvalsts izraudzīta iestāde, kura atbild par pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju informācijas tehnoloģiju 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);

7^{5}) sadarbojas ar NIS CSIRT tīklu;

8) veic citus normatīvajos aktos noteiktos pienākumus.

(1^{1}) Militārās izlūkošanas un drošības dienests veic šā panta pirmās daļas 2., 4., 5., 6., 7., $7.^{1}$, $7.^{2}$, $7.^{3}$, $7.^{4}$, $7.^{5}$ un 8. punktā noteiktos uzdevumus.

(2) Drošības incidentu novēršanas institūcijas ir tiesīgas:

1) pieprasīt un saņemt no valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām informāciju par informācijas tehnoloģiju (tostarp tīklu un informācijas sistēmu) drošības prasībām un tehnisko informāciju par notikušu vai notiekošu informācijas tehnoloģiju drošības incidentu (informācija par incidenta apjomu, incidentu izraisījušu kaitniecisku programmatūru datnes, ievainojamību apraksts, incidenta novēršanai veiktie tehniskie pasākumi, informācija par kaitnieku darbībām vai cita tehniskā informācija, ieskaitot IP adreses);

2) iegūt no valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām pēc abpusējas vienošanās tiešsaistes datu plūsmu;

3) veikt informācijas tehnoloģiju kritiskās infrastruktūras pārbaudes;

4) pieņemt lēmumus (arī izdot administratīvos aktus), lai nodrošinātu šajā likumā valsts un pašvaldību institūcijām, kā arī privāto tiesību juridiskajām personām noteikto pienākumu izpildi.

(Ar grozījumiem, kas izdarīti ar 05.02.2015., 15.06.2017. un 11.10.2018. likumu, kas stājas spēkā 25.10.2018.)

5.^{1} 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 $2.^{1}$ daļā minētajiem drošības incidentiem, kuriem ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu konkrētajā dalībvalstī;

2) sadarbojas ar NIS sadarbības grupu un reizi gadā sniedz tai ziņojumu par informāciju, kas saņemta par šā likuma 6. panta $2.^{1}$ daļā minētajiem drošības incidentiem (tostarp norāda ziņojumu skaitu un drošības incidentu raksturu), kā arī par citu Eiropas Savienības dalībvalstu kompetentajām iestādēm sniegtajiem ziņojumiem;

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

(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

6.pants. Rīcība informācijas tehnoloģiju drošības incidenta gadījumā

(1) Informācijas tehnoloģiju drošības incidents (turpmāk — drošības incidents) ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

(2) 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 Drošības incidentu novēršanas institūcijas rekomendācijas par vēlamo sākotnējo rīcību drošības incidenta gadījumā), kā arī tūlīt informē par notikušo kompetento Drošības incidentu novēršanas institūciju. Drošības incidentu novēršanas institūcija vienojas ar drošības incidenta pieteicēju par atbalsta sniegšanu drošības incidenta novēršanā.

(2^1) Ja noticis drošības incidents, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu, pamatpakalpojuma sniedzējs un digitālā pakalpojuma sniedzējs 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 nodrošināšanu 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 šo incidentu atrisināt vai novērst vai arī citādā ziņā ir sabiedrības interesēs.

(2^2) Šā panta $2.^1$ daļu nepiemēro kredītiestāde Kredītiestāžu likuma 1. panta otrās daļas 1. punkta izpratnē, tirdzniecības vieta Finanšu instrumentu tirgus likuma 1. panta pirmās daļas 77. punkta izpratnē un centrālo darījumu partneris Eiropas Parlamenta un Padomes 2012. gada 4. jūlija regulas (ES) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (Dokuments attiecas uz EEZ) 2. panta 1. punkta izpratnē.

(3) Privāto tiesību juridiskās personas, uz kurām neattiecas šā panta otrajā un $2.^1$ daļā noteiktie pienākumi, drošības incidenta gadījumā veic visas tā novēršanai nepieciešamās darbības un var pēc savas iniciatīvas informēt par notikušo Kompetentā Drošības incidentu novēršanas institūciju. Drošības incidentu novēršanas institūcija vienojas ar drošības incidenta pieteicēju par atbalsta sniegšanu drošības incidenta novēršanā.

(4) Drošības incidentu novēršanas institūcija, konstatējusi drošības incidentu, kas apdraud nacionālo drošību, par to informē satiksmes ministru, aizsardzības ministru, par nozari atbildīgo ministru un kompetento valsts drošības iestādi, kā arī iesniedz priekšlikumus par nepieciešamo rīcību, bet, konstatējusi tādu drošības incidentu, kuram ir būtiska ietekme uz elektronisko sakaru tīklu vai elektronisko sakaru pakalpojuma nepārtrauktību, par notikušo informē Sabiedrisko pakalpojumu regulēšanas komisiju un var informēt par notikušo Eiropas Savienības dalībvalstu valsts pārvaldes iestādes un Eiropas Tīklu un informācijas drošības aģentūru. Drošības incidentu novēršanas institūcija var informēt sabiedrību vai arī prasīt, lai to dara attiecīgie elektronisko sakaru komersanti, ja tā uzskata, ka pārkāpuma publiskošana ir sabiedrības interesēs.

(5) Kompetentajai Drošības incidentu novēršanas institūcijai ir tiesības pieprasīt, lai augstākā līmeņa domēna ".lv" reģistra un elektroniskās numurēšanas sistēmas uzturētājs atslēdz ".lv" domēna vārdu, ja šis domēna vārds ir iesaistīts drošības incidentā, kas būtiski apdraud informācijas sistēmu vai elektronisko sakaru tīklu drošību, un drošības incidentu nav iespējams novērst citā veidā.

(6) Pieprasījumā atslēgt ".lv" domēna vārdu kompetentā Drošības incidentu novēršanas institūcija norāda pieprasījuma iemeslu un domēna vārda atslēgšanas ilgumu, kas nav garāks par piecām dienām, un, ja nepieciešams, citas papildu darbības, kas veicamas augstākā līmeņa domēna ".lv" reģistra un elektroniskās numurēšanas sistēmas uzturētājam (piemēram, datu plūsmas pārvirzīšana uz kompetentās Drošības incidentu novēršanas institūcijas infrastruktūru).

(7) Ministru kabinets nosaka drošības incidenta būtiskuma kritērijus, informēšanas kārtību un ziņojuma saturu.

(Ar grozījumiem, kas izdarīti ar 01.11.2012., 05.02.2015., 15.06.2017. un 11.10.2018. likumu, kas stājas spēkā 25.10.2018.)

6.[1] pants. Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā

(1) Informācijas tehnoloģiju drošības nepilnība (turpmāk — drošības nepilnība) ir būtiska informācijas sistēmas vai elektronisko sakaru tīkla izveides, uzturēšanas vai pārveidošanas gaitā tīši vai nejauši radīta sistēmiska vājība, kuras rezultātā var tikt apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

(2) Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, konstatējis drošības nepilnību, 90 dienu laikā veic visas tās novēršanai nepieciešamās darbības, kā arī par konstatēto tūlīt informē kompetento Drošības incidentu novēršanas institūciju.

(3) Kompetentā Drošības incidentu novēršanas institūcija, konstatējusi drošības nepilnību, par šo faktu tūlīt informē informācijas sistēmas vai elektronisko sakaru tīkla īpašnieku vai tiesisko valdītāju. Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kompetentās Drošības incidentu novēršanas institūcijas noteiktajā termiņā, bet ne vēlāk kā 90 dienu laikā kopš informēšanas brīža veic visas drošības nepilnības novēršanai nepieciešamās darbības.

(05.02.2015. likuma redakcijā ar grozījumiem, kas izdarīti ar 15.06.2017. likumu, kas stājas spēkā 19.07.2017.)

7.pants. Personas datu apstrāde

(1) Drošības incidentu novēršanas institūcija ir tiesīga saņemt un apstrādāt personas datus, lai pamatotu vai izslēgtu aizdomas par drošības incidentu vai to novērstu, ja personas datus nav iespējams anonimizēt un pastāv vismaz viens no šādiem nosacījumiem:

1) kaitnieciska programmatūra varētu saturēt personas datus;

2) personas dati tiek pārraidīti, izmantojot kaitniecisku programmatūru;

3) personas dati var sniegt būtisku informāciju par kaitniecisku programmatūru.

(2) Ja tiek konstatēts drošības incidents, personas datu apstrāde ir atļauta, lai nodrošinātu aizsardzību pret kaitniecisku programmatūru vai tās radītajām sekām, kā arī atklātu citu kaitniecisku programmatūru un nodrošinātu aizsardzību pret to.

(3) Apstrādātos personas datus Drošības incidentu novēršanas institūcija drīkst nodot šā likuma 5.panta pirmās daļas 5. un 7.punktā minētajām institūcijām (vienībām), lai atpazītu un novērstu tādas kaitnieciskas programmatūras darbību, kas var radīt vai rada draudus nacionālajai vai sabiedrības drošībai.

(3[1]) Apstrādātos un neapstrādātos personas datus Drošības incidentu novēršanas institūcijas drīkst nodot Zemessardzei tādā apjomā un veidā, lai atpazītu un novērstu tādas kaitnieciskas programmatūras darbību, kas var radīt vai rada draudus nacionālajai vai sabiedrības drošībai, ja Zemessardze atbilstoši Zemessardzes likumā noteiktajam tiek iesaistīta atbalsta sniegšanā kompetentajai Drošības incidentu novēršanas institūcijai.

(4) Personas datu apstrādi, kas nav saistīta ar tāda incidenta novēršanu, sakarā ar kuru šie dati iegūti, Drošības incidentu novēršanas institūcijai ir atļauts veikt vienīgi tad, ja tā sagatavo un nosūta Datu valsts inspekcijai plānotās personas datu apstrādes un aizsardzības aprakstu. Drošības incidentu novēršanas institūcija līdz nākamā gada 20.janvārim sagatavo un iesniedz Datu valsts inspekcijai ziņojumu par iepriekšējā gadā veikto personas datu apstrādi.

(Ar grozījumiem, kas izdarīti ar 15.06.2017. likumu, kas stājas spēkā 19.07.2017.)

8. pants. Informācijas tehnoloģiju drošības pārvaldība

(1) Valsts un pašvaldību institūciju, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju, pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju informācijas tehnoloģiju drošības pārvaldību nodrošina katras attiecīgās institūcijas vadītājs.

(2) Valsts vai pašvaldības institūcijas, pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā (turpmāk šajā pantā — atbildīgā persona). Par atbildīgās personas noteikšanu ne vēlāk kā piecu darbdienu laikā informējama kompetentā Drošības incidentu novēršanas institūcija.

(2[1]) Informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, kā arī privāto tiesību juridiskā

persona, kas ir pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs, nodrošina informācijas tehnoloģiju drošības pārvaldību un nosaka atbildīgo personu, kas īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā uzņēmumā, un par atbildīgās personas noteikšanu ne vēlāk kā piecu darbdienu laikā informē kompetento Drošības incidentu novēršanas institūciju.

(3) Atbildīgajai personai papildus citos tiesību aktos noteiktajam ir šādi pienākumi:

1) organizēt institūcijas informācijas tehnoloģiju drošības pārvaldību;

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

3) vismaz reizi gadā apmeklēt Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos;

4) ne retāk kā reizi gadā veikt institūcijas darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos.

(4) *(Izslēgta ar 11.10.2018. likumu)*

(5) Ministru kabinets nosaka informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā valsts un pašvaldību institūcijas, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām.

(6) Ministru kabinets nosaka informācijas tehnoloģiju drošības prasības privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji.

(7) Šā panta prasības, kas noteiktas pamatpakalpojuma sniedzējam, neattiecas uz kredītiestādi Kredītiestāžu likuma 1. panta otrās daļas 1. punkta izpratnē, tirdzniecības vietu Finanšu instrumentu tirgus likuma 1. panta pirmās daļas 77. punkta izpratnē un centrālo darījumu partneri Eiropas Parlamenta un Padomes 2012. gada 4. jūlija regulas (ES) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (Dokuments attiecas uz EEZ) 2. panta 1. punkta izpratnē.

(Ar grozījumiem, kas izdarīti ar 05.02.2015., 15.06.2017. un 11.10.2018. likumu, kas stājas spēkā 25.10.2018.)

8.[1] pants. Pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja uzraudzības institūcija

(1) Pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja uzraudzības institūciju (turpmāk — uzraudzības institūcija) un tās darba organizācijas kārtību nosaka Ministru kabinets.

(2) Uzraudzības institūcija:

1) apkopo nozari uzraugošo ministriju iesniegto informāciju par identificētajiem pamatpakalpojuma sniedzējiem un pamatpakalpojumiem un sastāda to sarakstu;

2) reizi divos gados iesniedz Eiropas Komisijai informāciju par kārtību, kādā identificē pamatpakalpojuma sniedzējus, identificēto pamatpakalpojuma sniedzēju skaitu un pamatpakalpojumu sarakstu;

3) saņem informāciju no Drošības incidentu novēršanas institūcijām par konstatētajām neatbilstībām un drošības incidentiem.

(3) Pēc tam kad no Drošības incidentu novēršanas institūcijas saņemta informācija par konstatētajām neatbilstībām vai drošības incidentu, uzraudzības institūcija ir tiesīga veikt vienu vai vairākas šādas darbības:

1) ierosināt, lai pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs noteiktā termiņā novērš konstatētās neatbilstības tām drošības prasībām, kuras noteicis Ministru kabinets saskaņā ar šā likuma 8. panta sesto daļu;

2) pieņemt lēmumu, ar kuru uzdod 6. panta 2.[1] daļā minētajam pamatpakalpojuma sniedzējam vai digitālā pakalpojuma sniedzējam novērst drošības incidentu, tostarp izpildīt Drošības incidentu novēršanas institūcijas rekomendācijas.

(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

9.pants. Publisko elektronisko sakaru tīklu drošība

(1) Elektronisko sakaru komersantiem ir šādi pienākumi:

1) ja attiecīgais komersants nodrošina publisko elektronisko sakaru tīklu, — nodrošināt šā sakaru tīkla integritāti, tādējādi panākot pakalpojumu sniegšanas nepārtrauktību, kā arī sastādīt rīcības plānu elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai, tajā norādot tehniskos un organizatoriskos pasākumus, kuru mērķis ir pārvarēt tīkla un pakalpojumu sniegšanas drošības apdraudējumus;

2) ziņot kompetentajai Drošības incidentu novēršanas institūcijai par drošības incidentu, kuram ir būtiska ietekme uz elektronisko sakaru tīklu vai elektronisko sakaru pakalpojuma nepārtrauktību;

3) pēc kompetentās Drošības incidentu novēršanas institūcijas pieprasījuma sniegt tai pakalpojumu un tīkla drošības vai integritātes novērtēšanai nepieciešamo informāciju, tostarp dokumentētu drošības politiku;

4) pēc kompetentās Drošības incidentu novēršanas institūcijas pieprasījuma, ja konstatēti būtiski drošības vai integritātes pārkāpumi, organizēt drošības auditu, ko veic ar kompetento Drošības incidentu novēršanas institūciju saskaņots kvalificēts un no iesaistītajām pusēm neatkarīgs tiesību subjekts. Par audita rezultātiem informē kompetento Drošības incidentu novēršanas institūciju. Audita izmaksas sedz un auditā konstatētos pārkāpumus novērš elektronisko sakaru komersants;

5) pēc kompetentās Drošības incidentu novēršanas institūcijas pieprasījuma īslaicīgi, bet ne ilgāk kā 24 stundas slēgt galalietotājam piekļuvi elektronisko sakaru tīklam, ja galalietotājs būtiski apdraud citu lietotāju tiesības vai informācijas sistēmu, vai elektronisko sakaru tīklu drošību. Pieprasot šādas darbības veikšanu, kompetentā Drošības incidentu novēršanas institūcija norāda pieprasījuma iemeslu.

(2) Ministru kabinets nosaka rīcības plānā elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai ietveramo informāciju, šā plāna izpildes kontroles kārtību un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam.

(3) Ministru kabinets nosaka drošības incidenta būtiskuma kritērijus.

(Ar grozījumiem, kas izdarīti ar 15.06.2017. un 11.10.2018. likumu, kas stājas spēkā 25.10.2018.)

10.pants. Nacionālā informācijas tehnoloģiju drošības padome

Lai koordinētu ar informācijas tehnoloģiju drošību saistītās politikas izstrādi, kā arī attiecīgu uzdevumu un pasākumu plānošanu un īstenošanu, Ministru prezidents izveido Nacionālo informācijas tehnoloģiju drošības padomi, kuras darbību nodrošina vadošā valsts pārvaldes iestāde valsts aizsardzības nozarē.

(06.11.2013. likuma redakcijā, kas stājas spēkā 01.01.2014.)

11. pants. 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 regulatīvos pasākumus, lai panāktu un saglabātu elektronisko sakaru tīklu un informācijas sistēmu augstu drošības līmeni, kas attiecas uz pamatpakalpojuma sniedzējiem, pamatpakalpojumiem, digitālā pakalpojuma sniedzējiem un digitālajiem pakalpojumiem.

(2) Nacionālās kiberdrošības stratēģijas izstrādi reizi četros gados nodrošina Aizsardzības ministrija. Nacionālo kiberdrošības stratēģiju apstiprina Ministru kabinets.

(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

Pārejas noteikumi

1. Šā likuma 9.pants stājas spēkā 2011.gada 1.maijā.

2. Ministru kabinets līdz 2011.gada 1.februārim izdod šā likuma 3.panta trešajā daļā paredzētos noteikumus.

3. Ministru kabinets līdz 2011.gada 1.maijam izdod šā likuma 9.panta otrajā daļā paredzētos noteikumus.

4. Ministru prezidents līdz 2011.gada 1.februārim izveido šā likuma 10.pantā noteikto Nacionālo informācijas tehnoloģiju drošības padomi.

5. Ministru kabinets līdz 2015.gada 15.martam izdod šā likuma 8.panta piektajā daļā paredzētos noteikumus.
(05.02.2015. likuma redakcijā, kas stājas spēkā 04.03.2015.)

6. Ministru kabinets līdz 2019. gada 1. janvārim izdara grozījumus Ministru kabineta 2011. gada 26. aprīļa noteikumos Nr. 327 "Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam" atbilstoši šā likuma 9. panta trešajā daļā noteiktajam.
(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

7. Uzraudzības institūcija šā likuma $8.^1$ panta otrās daļas 2. punktā minēto informāciju pirmo reizi Eiropas Komisijai iesniedz līdz 2018. gada 9. novembrim.
(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

8. Ministru kabinets nacionālo kiberdrošības stratēģiju apstiprina līdz 2019. gada 1. janvārim.
(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

Informatīva atsauce uz Eiropas Savienības direktīvām
(11.10.2018. likuma redakcijā, kas stājas spēkā 25.10.2018.)

Likumā iekļautas tiesību normas, kas izriet no:

1) Eiropas Parlamenta un Padomes 2009. gada 25. novembra direktīvas 2009/140/EK, ar ko izdara grozījumus direktīvā 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem, direktīvā 2002/19/EK par piekļuvi elektronisko komunikāciju tīkliem un ar tiem saistītām iekārtām un to savstarpēju savienojumu un direktīvā 2002/20/EK par elektronisko komunikāciju tīklu un pakalpojumu atļaušanu (Dokuments attiecas uz EEZ);

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

Likums stājas spēkā 2011.gada 1.februārī.

Likums Saeimā pieņemts 2010.gada 28.oktobrī.

Valsts prezidents V.Zatlers

Rīgā 2010.gada 10.novembrī