**Ministru kabineta noteikumu projekta "Grozījumi 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"" sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

| **I. Tiesību akta projekta izstrādes nepieciešamība** | | |
|---|---|---|
| 1. | Pamatojums | Informācijas tehnoloģiju drošības likuma 9. panta pirmās daļas 2. punkts un 9. panta trešā daļa. |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | Saeima 2018. gada 11. oktobrī pieņēma likumprojektu "Grozījumi Informācijas tehnoloģiju drošības likumā" ar kuru grozīti kritēriji, kādi piemērojami, lai noteiktu, ka drošības incidentam ir būtiska ietekme uz elektronisko sakaru tīklu vai elektronisko sakaru pakalpojumu nepārtrauktību. Ar likumprojektu no Informācijas tehnoloģiju drošības likuma svītrots kritērijs, ka par būtisku drošības incidentu uzskatāms incidents, kura rezultātā elektronisko sakaru tīkls nedarbojas vismaz 24 stundas pēc kārtas. Tā vietā ar likumprojektu Ministru kabinets tiek deleģēts noteikt drošības incidenta būtiskuma kritērijus.<br><br>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; turpmāk – direktīva 2009/140/EK) 13.a pants nosaka dalībvalstij pienākumu nodrošināt to, ka uzņēmumi, kas nodrošina publisko sakaru tīklus vai sniedz publiski pieejamus elektronisko sakaru pakalpojumus, paziņo kompetentajai valsts pārvaldes iestādei par drošības vai integritātes pārkāpumiem, kas ir būtiski ietekmējuši tīklu darbību vai pakalpojumu sniegšanu.<br><br>Šobrīd ar Ministru kabineta 2011. gada 26. aprīļa noteikumiem 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" tiek izpildīta direktīvā 2009/140/EK un no tās izrietošajā Informācijas tehnoloģiju drošības likuma 9. panta pirmās daļas 2. punktā noteiktā prasība elektronisko sakaru |

| | | |
|---|---|---|
| | | komersantam ziņot par konstatētu drošības incidentu, kas ir būtiski ietekmējis tīkla darbību vai pakalpojumu sniegšanu, ir nepieciešams noteikt kārtību, kādā elektronisko komersants ziņo par konstatēto incidentu.<br><br>Vienlaikus šobrīd Ministru kabineta 2011. gada 26. aprīļa noteikumi 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” nenosaka termiņu, kādā iesniedzams sākotnējais ziņojums par būtisku drošības incidentu, kas skāris galalietotājus, kā arī informāciju, kas iekļaujama sākotnējā reaģēšanas ziņojumā.<br><br>Noteikumu projekts nosaka, ka pēc būtiska drošības incidenta konstatācijas elektronisko sakaru komersants 24 stundu laikā iesniedz sākotnējo reaģēšanas ziņojumu kompetentajai Drošības incidentu novēršanas institūcijai. Tāpat noteikumu projekts nosaka to, kāda informācija ir iekļaujama sākotnējā reaģēšanas ziņojumā, konstatējot būtisku drošības incidentu.<br><br>Lai noteiktu, kāds drošības incidents ir uzskatāms par incidentu, kuram ir būtiska ietekme uz elektronisko sakaru tīklu vai elektronisko sakaru pakalpojuma nepārtrauktību, noteikumu projekts nosaka drošības incidenta būtiskuma kritērijus. Drošības incidenta būtiskuma kritēriji ir iekļauti kā sliekšņi, kas izstrādāti, pamatojoties uz Eiropas Savienības Tīklu un informācijas drošības aģentūras (ENISA) tehniskajās vadlīnijās par incidentu ziņošanu iekļautajām vadlīnijām. Noteikumu projektā noteikto būtisko drošības incidentu sliekšņi vienlaikus aptver sliekšņus drošības incidentiem, par kuriem Satiksmes ministrija iesniegs ziņojumu ENISA ekspertu darba grupai, kas izveidota direktīvas 2009/140/EK 13.a panta ieviešanas novērtēšanai.<br><br>Noteikumu projekta drošības incidenta būtiskuma kritērijos norādītie elektronisko sakaru pakalpojuma lietotāji ir norādīti procentuāli no kopējā elektronisko sakaru pakalpojuma lietotāju skaita Latvijā, nevis atsevišķa elektronisko komersanta (pakalpojuma sniedzēja) klientu skaita. |
| 3. | Projekta izstrādē iesaistītās institūcijas un publiskas personas kapitālsabiedrības | Aizsardzības ministrija, Satiksmes ministrija, Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV |
| 4. | Cita informācija | Nav. |

| **II. Tiesību akta projekta ietekme uz sabiedrību, tautsaimniecības attīstību un administratīvo slogu** | | |
|---|---|---|
| 1. | Sabiedrības mērķgrupas, kuras tiesiskais regulējums ietekmē vai varētu ietekmēt | Sabiedrība kopumā – noteikumu projekts nosaka drošības incidentu būtiskuma kritērijus, kas var ietekmēt sabiedrības saņemtos elektronisko sakaru pakalpojumus. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Administratīvais slogs sabiedrības mērķgrupām un institūcijām nemainās. |
| 3. | Administratīvo izmaksu monetārs novērtējums | Administratīvās izmaksas sabiedrības mērķgrupām un institūcijām nemainās. |
| 4. | Atbilstības izmaksu monetārs novērtējums | Nav attiecināms. |
| 5. | Cita informācija | Nav. |

| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** |
|---|
| Noteikumu projekts šo jomu neskar. |

| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** | |
|---|---|
| Saistītie tiesību aktu projekti | Likumprojekts "Grozījumi Informācijas tehnoloģiju drošības likumā" (1263/Lp12). |
| Atbildīgā institūcija | Aizsardzības ministrija |
| Cita informācija | Noteikumu projekts izstrādāts atbilstoši likumprojekta "Grozījumi Informācijas tehnoloģiju drošības likumā" (1263/Lp12), kas Saeimā 3. lasījumā pieņemts 2018. gada 11. oktobrī, radītajam regulējumam. |

| **V. Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām saistībām** |
|---|
| Noteikumu projekts šo jomu neskar. |

| **VI. Sabiedrības līdzdalība un komunikācijas aktivitātes** | | |
|---|---|---|
| 1. | Plānotās sabiedrības līdzdalības un komunikācijas aktivitātes saistībā ar projektu | Noteikumu projekts 2018. gada 15. novembrī publicēts Aizsardzības ministrijas mājaslapas sadaļā "Sabiedrības līdzdalība". |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Noteikumu projekts tika nodots sabiedriskajai apspriešanai. |
| 3. | Sabiedrības līdzdalības rezultāti | Sabiedrība nav izteikusi viedokli par noteikumu projektu. |
| 4. | Cita informācija | Nav. |

| VII. Tiesību akta projekta izpildes nodrošināšana un tās ietekme uz institūcijām | | |
|---|---|---|
| 1. | Projekta izpildē iesaistītās institūcijas | Aizsardzības ministrija, Satiksmes ministrija, Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV |
| 2. | Projekta izpildes ietekme uz pārvaldes funkcijām un institucionālo struktūru. Jaunu institūciju izveide, esošu institūciju likvidācija vai reorganizācija, to ietekme uz institūcijas cilvēkresursiem | Noteikumu projekta izpilde notiks esošo pārvaldes funkciju un institucionālās struktūras ietvaros. |
| 3. | Cita informācija | Nav. |

Aizsardzības ministrs Raimonds Bergmanis

Heinrihs Rozēns
Aizsardzības ministrijas
Krīzes vadības departamenta
Civilmilitārās sadarbības nodaļas
vecākais referents
Tālr.: 67335072, e-pasts: Heinrihs.Rozens@mod.gov.lv

875