**Ministru kabineta noteikumu projekta “Grozījumi Ministru kabineta 2015. gada 28. jūlija noteikumos Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”” sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

|  |  |
| --- | --- |
| **Tiesību akta projekta anotācijas kopsavilkums** | |
| Mērķis, risinājums un projekta spēkā stāšanās laiks (500 zīmes bez atstarpēm) | Noteikumu projekta “Grozījumi Ministru kabineta 2015. gada 28. jūlija noteikumos Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”” (turpmāk – noteikumu projekts) mērķis ir pabeigt ieviest 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 (turpmāk – NIS direktīva) prasības daļā par informācijas un komunikācijas tehnoloģiju drošības prasībām pamatpakalpojuma sniedzējiem un digitālo pakalpojumu sniedzējiem, kā arī izpildīt Informācijas tehnoloģiju drošības likuma 8. panta piektajā un sestajā daļā (likumprojekts “Grozījumi Informācijas tehnoloģiju drošības likumā”, ko Saeima pieņēma 2018. gada 11. oktobrī) Ministru kabinetam noteikto deleģējumu.  Noteikumu projekts paredz, ka Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” normas attieksies uz privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji vai digitālā pakalpojuma sniedzēji. Tāpat noteikumu normas ir attiecinātas uz informācijas tehnoloģiju kritisko infrastruktūru.  Noteikumu projekts stājas spēkā parastajā kārtībā (nākamajā dienā pēc Ministru kabineta noteikumu izsludināšanas). |

|  |  |  |
| --- | --- | --- |
| **I. Tiesību akta projekta izstrādes nepieciešamība** | | |
| 1. | Pamatojums | Noteikumu projekts ir izstrādāts, pamatojoties uz:  1) NIS direktīva 25. panta 1. punktā noteikto, ka dalībvalstis līdz 2018. gada 9. maijam pieņem un publicē normatīvos un administratīvos aktus, lai izpildītu NIS direktīvas prasības;  2) Informācijas tehnoloģiju drošības likuma 8. panta piekto un sesto daļu (likumprojekts “Grozījumi Informācijas tehnoloģiju drošības likumā”, ko Saeima pieņēma 2018. gada 11. oktobrī). |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | I. NIS direktīva nosaka pasākumus dalībvalstīm, lai panāktu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību. Lai nodrošinātu minēto, NIS direktīva paredz šādus pasākumus:  1) pieņemt tīklu un informācijas sistēmu drošības stratēģiju (turpmāk – stratēģija);  2) izveidot sadarbības grupu;  3)  izveidot datordrošības incidentu reaģēšanas vienību tīklu (turpmāk – CSIRT tīkls);  4) noteikt paziņošanas un drošības prasības pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem;  5) izraudzīties valsts kompetentās iestādes, vienoto kontaktpunktu un datora apdraudējumu reaģēšanas vienību (turpmāk – CERT).  NIS direktīvas 14. panta 1. punkts un 16. panta 1. punkts nosaka dalībvalstu pienākumu nodrošināt, ka pamatpakalpojuma sniedzēji un digitālo pakalpojumu sniedzēji veic atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmām, ko tie izmanto savās darbībās.  Ar likumprojektu “Grozījumi Informācijas tehnoloģiju drošības likumā” (turpmāk – grozījumi likumā), ko Saeima pieņēma 2018. gada 11. oktobrī un ar ko tika ieviesta NIS direktīva, Informācijas tehnoloģiju drošības likumu (turpmāk – likums) papildināja ar normu, kas deleģē Ministru kabinetam noteikt informācijas tehnoloģiju drošības prasības privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji vai digitālā pakalpojuma sniedzēji (likuma 8. panta sestā daļa). Attiecīgi nepieciešams izstrādāt regulējumu.  Jau šobrīd ir spēkā Ministru kabineta noteikumi, kas nosaka minimālās drošības prasības informācijas un komunikācijas tehnoloģiju sistēmām valsts un pašvaldību institūcijās – 2015. gada 28. jūlija noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” (turpmāk – noteikumi). Izdarot grozījumus noteikumos, to normas tiek attiecinātas uz privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji vai digitālā pakalpojuma sniedzēji. Ir paredzēts, ka šie pakalpojumu sniedzēji informācijas tehnoloģijām, kas tiek izmantotas pamatpakalpojuma vai digitālā pakalpojuma sniegšanā, ievēro noteikumos informācijas un komunikāciju tehnoloģiju sistēmām noteiktās prasības, ciktāl noteikumos nav noteikts citādi.  Saskaņā ar grozījumiem likumā pamatpakalpojuma sniedzējs ir valsts vai pašvaldības institūcija vai privāto tiesību juridiska persona, kas: 1) sniedz 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, kuru sniegšanu var būtiski ietekmēt informācijas tehnoloģiju drošības incidents.  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 kādā no Eiropas Savienības dalībvalstīm; 2) veic saimniecisko darbību ārpus Eiropas Savienības un digitālo pakalpojumu Latvijas Republikā sniedz ar pilnvarota pārstāvja starpniecību.  Ņemot vērā, ka pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja pakalpojumi ir nozīmīgi, lai nodrošinātu sabiedrisku vai ekonomisku darbību, paredzēts, ka sistēmas, ko izmanto pamatpakalpojuma vai digitālā pakalpojuma sniegšanai, ir atzīstamas par paaugstinātas drošības sistēmām.  Papildus jānorāda, ka ņemot vērā to, ka noteikumi tika papildināti ar jaunu subjektu – informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, uz kuru attiecas kārtība, kādā nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām prasībām, tad nepieciešams precizēt noteikumu 3. punktu (likumprojekta 4. punkts), norādot, uz kurām sistēmām konkrēti noteikumi attiecas.  II. Grozījumi likumā paredz likuma 8. panta piektajā daļā noteikto subjektu loku – valsts un pašvaldību institūcijas, uz kurām attiecas Ministru kabineta kompetence noteikt kārtību, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām prasībām – paplašināt ar informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem. Izmaiņas tika veiktas, lai nodrošinātu vienotu minimālās drošības līmeni.  Noteikumu projekts precizē noteikumu tekstu, lai ieviestu un īstenotu attiecīgās izmaiņas likumā, kā arī tiek saskaņota terminoloģija (saskaņā ar Ministru kabineta 2011. gada 1. februāra noteikumiem Nr. 100 “Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība” atbildīgā persona, kura īsteno informācijas tehnoloģiju kritiskās infrastruktūras drošības pārvaldību, ir par infrastruktūras drošību atbildīgā persona, savukārt noteikumos tiek izmantots apzīmējums “par informācijas tehnoloģiju drošības pārvaldību atbildīgā persona”).  Ņemot vērā, ka informācijas tehnoloģiju kritiskā infrastruktūra ir nozīmīga, lai veiktu valstij un sabiedrībai būtiskas pamatfunkcijas, paredzēts, ka šīs informācijas sistēmas būs paaugstinātas drošības sistēmas.  III. Noteikumu projekts paredz arī vairākus esošo normu precizējumus un papildinājumus:  1. Tā kā noteikumi tiek papildināti ar jauniem subjektiem – privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem, esošās normas tiek precizētas redakcionāli un nodalītas no normas, kas attiecas tikai uz konkrētiem tiesību subjektiem. Noteikumu projekts paredz nodalīt atsevišķas prasības, kas attiecas tikai uz valsts un pašvaldību institūcijām (attiecībā uz iepirkumiem izvirzāmajām prasībām). Ar grozījumiem noteikumos ir atdalītas divas institūciju kategorijas ar dažādu pienākumu apjomu:  - valsts un pašvaldību institūcijas;  - institūcijas (jēdziens ietver sevī ne tikai valsts un pašvaldību institūcijas, bet arī kritiskās infrastruktūras īpašniekus vai tiesiskos valdītājus, pamatpakalpojuma sniedzējus un digitālā pakalpojuma sniedzējus), kuriem tiek noteiktas minimālās drošības prasības.  2. Lai mazinātu kibervidē esošo draudu ietekmi uz valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģijām, nepieciešams paredzēt vienotu pieeju, pasākumus kiberdrošības stiprināšanai. Tā kā informācijas un komunikācijas tehnoloģiju attīstība notiek strauji un tikpat strauji mainīgi ir riski un apdraudējumi, nepieciešams paredzēt elastīgu mehānismu risku mazināšanai. Tādēļ ir paredzēts, ka Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas un kompetentās valsts drošības iestādes ir tiesīgas izstrādāt rekomendācijas, pēc kurām valsts un pašvaldību institūcijas vadīsies, izmantojot informācijas un komunikācijas tehnoloģijas. Līdzīgs princips ir iestrādāts Ministru kabineta 2011. gada 1. februāra noteikumos Nr. 100 “Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība”.  Tāpat, lai mazinātu ietekmi no trešajām valstīm, ir paredzēts, ka paaugstinātas drošības sistēmām nepieciešamo iekārtu, pakalpojumu, programmatūras un iekārtu iegādes līgumu var slēgt ar juridisko personu, kas ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomiskās zonas dalībvalstī vai fizisku personu, kura ir minēto dalībvalstu pilsonis.  3. Noteikumi šobrīd paredz, ka parolei jāsastāv no deviņiem simboliem – vismaz viena lielā latīņu alfabēta burta, mazā latīņu alfabēta burta, cipara vai speciālā simbola. Starptautiski un arī Latvijā plaši izmantojamajos risinājumos, piemēram, *Microsoft Active Directory*, iestrādāti paroļu veidošanas algoritmi, kas par korektu uzskata paroli, ja tā satur trīs no četriem noteiktajiem simboliem. Attiecīgi tiek precizētas paroles sastādīšanas prasības, izvirzot prasību, ka parole jāveido no vismaz trijiem simboliem, kur lielais latīņu alfabēta burts un mazais latīņu alfabēta burts ir obligāta prasība, savukārt lietotājam būs izvēle izmantot ciparu vai speciālo simbolu.  4. Noteikumu 15.10. apakšpunkts paredz pienākumu veidot sistēmas auditācijas pierakstus, bet 24.6. apakšpunkts – veidot sistēmas pierakstus, kā arī tos glabāt noteiktu laiku. Šī informācija ir nozīmīga, jo tie ir analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem informācijas sistēmā. Normu piemērošanas procesā ir secināts, ka institūcijas pierakstos ietver dažādu informāciju, tādēļ nepieciešams nodrošināt vienādu pieeju pierakstu veidošanai. Attiecīgi ar noteikumu projektu tiek noteikta pierakstos ietveramā informācija (noteikumu projekta 13. un 16. punkts). Tāpat ir paredzēts noteikt, ka iekšējās sistēmas drošības noteikumos būs jānosaka, kā veido, uzglabā, apstrādā un dzēš sistēmas failus. Termins “Ielaušanās atklāšanas sistēma” (Intrusion detection system, IDS) ir vispārīgs tehnoloģijas apzīmējums, nevis konkrēta produkta nosaukums, jo IDS izveide ir katras iestādes pārziņā un Ministru kabineta noteikumi nereglamentē konkrētu veidu, paņēmienu vai arī arhitektūru, kādā IDS būtu jāizveido, līdz ar to lēmums par to kādā formā vai veidā ieviest IDS ir iestādes izvēle.  5. Veikti redakcionāli precizējumi 25. un 31. punktā, svītrojot 31. punktu, bet tajā noteiktās prasības ietverot noteikumu projekta 16. punktā. Izmaiņas ir veiktas, jo, pēc labās prakses un pārvaldības principiem, ieviešamo sistēmu jauninājumu ietekmes un sistēmu drošības izvērtēšanas procedūrām ir jābūt skaidri noteiktām un vienotām, lai tās konsekventi ievērotu institūcijas. Paredzēts, ka šāda kārtība būs jāietver iekšējās sistēmas drošības noteikumos.  6. Lai institūcijām, kuras izmanto paaugstinātas drošības sistēmas, kas pieejamas, izmantojot publisku datu pārraides tīklu, mazinātu administratīvo slogu, ir paredzēts – ja šīs sistēmas ir sertificētas saskaņā ar starptautiski atzītiem informācijas sistēmu drošības standartiem, nav jāveic šo sistēmu drošības pārbaude, ko paredz noteikumu 34. punkts. Sertifikācija, neatkarīgas trešās puses veikts audits apliecina, ka sistēma atbilst šiem standartiem.  7. Saskaņā ar likuma grozījumiem un Nacionālās drošības likumu attiecīgi pamatpakalpojumu sniedzēju saraksts un informācijas tehnoloģiju kritiskās infrastruktūras saraksts tiek aktualizēti periodiski. Attiecīgi tie var tikt papildināti ar jauniem subjektiem. Tādēļ nepieciešams noteikt samērīgu laiku, kurā pamatpakalpojuma sniedzējam un informācijas tehnoloģiju īpašniekam vai tiesiskajam valdītājam ir jāsakārto konkrētās informācijas sistēmas, lai tās atbilstu noteikumu prasībām. Noteikumu projekts paredz, ka termiņš, kurā informācijas sistēmas ir attiecīgi sakārtojamas, ir seši mēneši.  Tāpat noteikumu projekts paredz arī pārejas posmu, kurā informācijas tehnoloģiju kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam, pamatpakalpojuma sniedzējam un digitālo pakalpojumu sniedzējam būs jāveic pasākumi, lai informācijas sistēmas sakārtotu atbilstoši noteikumu prasībām. Paredzēts, ka noteikumi tiks piemēroti no 2019. gada 1. maija.  Ikvienam, sniedzot pakalpojumus, kas ir atkarīgi no informācijas tehnoloģijām, ir jāapzinās atbildība un kā gādīgam saimniekam jānodrošina sistēmu drošība, īpaši, ja drošības incidents var radīt būtiski traucējošu ietekmi pakalpojuma saņēmējam. Turklāt pakalpojuma sniedzējam dārgāk izmaksā drošības incidenta seku novēršana nekā sistēmas drošības sakārtošana. Informācijas tehnoloģiju sistēmām noteiktās minimālās drošības prasības būtu jāievēro ikvienai institūcijai, privāto tiesību juridiskai personai, kas sniedz pakalpojumus, izmantojot informācijas tehnoloģijas. |
| 3. | Projekta izstrādē iesaistītās institūcijas un publiskas personas kapitālsabiedrības | Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV). Konsultācijas tika veiktas ar Satiksmes ministriju, Finanšu ministriju, Veselības ministriju, Vides aizsardzības un reģionālās attīstības ministriju, Zemkopības ministriju un Latvijas Pašvaldību savienību. |
| 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 | Noteikumu projekts ietekmēs informācijas tehnoloģiju kritiskās infrastruktūras īpašniekus vai tiesiskos valdītājus un privāto tiesību juridiskās personas, kas ir pakalpojuma sniedzēji, kurus nozari uzraugošā ministrija identificēs kā pamatpakalpojuma sniedzējus vai kuri būs identificējuši sevi kā digitālā pakalpojuma sniedzējus, kā arī valsts un pašvaldību institūcijas. Tiem būs jāievēro noteikumos noteiktie pienākumi un drošības prasības. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Noteikumu projekta tiesiskais regulējums sabiedrības mērķgrupām izvirza jaunas veicamās darbības, kas pozitīvi ietekmē tautsaimniecību.  Pamatpakalpojuma sniedzēji aptver tādas sabiedrībai svarīgas jomas kā finanšu pakalpojumi Kredītiestāžu likuma izpratnē un finanšu tirgus infrastruktūras pakalpojumi, dzeramā ūdens piegādes vai izplatīšanas pakalpojumi, interneta plūsmas apmaiņas punkta pakalpojumi, domēnu nosaukumu sistēmas pakalpojumi, augstākā līmeņa domēna nosaukumu reģistra pakalpojumi vai pakalpojumi enerģētikas, transporta vai veselības nozarēs (NIS direktīvas II pielikums), kā arī digitālo pakalpojumu jomā. Prasība pēc tīklu un informācijas sistēmu drošības ir īpaši nozīmīga pakalpojuma sniedzējiem, kuri nodrošina apjomīgu konkrētās nozares sniegtā pakalpojuma tirgus daļu. Tas ir sabiedrības interesēs, lai šo nozaru pakalpojuma sniedzēji ievērotu informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošību.  Nosakot minimālās drošības prasības informācijas tehnoloģiju kritiskajai infrastruktūrai, pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem tiks nodrošināta sabiedrībai svarīgu pakalpojumu nepārtrauktība, tas mazinās risku, ka drošības incidentu rezultātā tiks neatgriezeniski vai ilglaicīgi traucēta sabiedrībai kritiski svarīgu pakalpojumu saņemšana, un mazinās citu negatīvu ietekmi uz sabiedrībai ikdienā svarīgiem pakalpojumiem.  Noteikumu projekts var palielināt administratīvo slogu privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji, digitālā pakalpojuma sniedzējiem un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem, kuru informācijas tehnoloģijas neatbilst labajai praksei un minimālajām drošības prasībām. Administratīvais slogs palielināsies, jo noteikumu projekts nosaka, kādas konkrētas drošības prasības jāievēro.  Pamatpakalpojuma sniedzējus paredzēts noteikt Ministru kabineta noteiktajā kārtībā, savukārt informācijas tehnoloģiju kritisko infrastruktūru nosaka atbilstoši Nacionālās drošības likumam. |
| 3. | Administratīvo izmaksu monetārs novērtējums | Ievērojot, ka pašreiz nav iespējams noteikt precīzu subjektu skaitu, uz kuriem regulējums attieksies, administratīvās izmaksas nav iespējams noteikt.  Paredzams, ka izmaksas veidos pakalpojuma sniedzēju sistēmu pielāgošana drošības prasībām, bet, tā kā drošības prasības ir minimālas un atbilst informācijas un komunikācijas tehnoloģiju pārvaldības labajai praksei, noteikumu projektā paredzēto pienākumu izpilde neradīs būtiskas izmaiņas un izmaksas.  Tā kā noteikumu projekts paredz, ka kritiskās infrastruktūras informācijas sistēmas vai sistēmas, ko izmanto pamatpakalpojuma vai digitālā pakalpojuma sniegšanai, ir atzīstamas par paaugstinātas drošības sistēmām, saskaņā ar noteikumu 34. punktu tām sistēmām, kas pieejamas, izmantojot publisku datu pārraides tīklu, reizi divos gados jāveic ārējais drošības dokumentācijas audits un ielaušanās tests. Vienas sistēmas drošības dokumentācijas audita un ielaušanās testa vidējās izmaksas ir 10 000 *euro*. |
| 4. | Atbilstības izmaksu monetārs novērtējums | *Skat. anotācijas II sadaļas 3. punktu.* |
| 5. | Cita informācija | Nav. |

|  |
| --- |
| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** |
| Projekts nerada ietekmi uz valsts vai pašvaldību budžetiem. |

|  |
| --- |
| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** |
| Projekts šo jomu neskar. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **V. Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām saistībām** | | | | | |
| 1. | Saistības pret Eiropas Savienību | | Ar noteikumu projektu tiek ieviesta NIS direktīvas prasība noteikt atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem. NIS direktīvas prasības jāievieš nacionālajos normatīvajos aktos līdz 2018. gada 9. maijam. Saņemts Eiropas Komisijas 2018. gada 19. jūlija formālais paziņojums pārkāpuma procedūras lietā Nr. 2018/0203, sagatavota Latvijas Republikas nostāja (Ministru kabineta 2018. gada 4. septembra sēdes protokola Nr. 41 36. §). | | |
| 2. | Citas starptautiskās saistības | | Projekts šo jomu neskar. | | |
| 3. | Cita informācija | | Nav. | | |
| **1. tabula Tiesību akta projekta atbilstība ES tiesību aktiem** | | | | | |
| Attiecīgā ES tiesību akta datums, numurs un nosaukums | | Ar noteikumu projektu tiek ieviestas 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 (NIS direktīva) prasības. | | | |
| A | | B | | C | D |
| 1. panta 2. punkta d) apakšpunkts  1. panta 2. punkta e) apakšpunkts  1. panta 3. punkts  5. panta 1. punkts  5. panta 2. punkts  5. panta 3. punkts  5. panta 4. punkts  5. panta 5. punkts  5. panta 7. punkts  6. pants 1. un 2. punkts  7. panta 1. punkts  7. panta 3. punkts  8. panta 1. punkts  8. panta 3. punkts  8. panta 4. punkts  8. panta 6. punkts  9. pants 1., 2., 3. punkts  10. panta 1. punkts  10. panta 2. punkts  10. panta 3. punkta pirmā daļa  10. panta 3. punkta otrā daļa  14. panta 1. punkts  14. panta 2. punkts  14. panta 3. punkts  14. panta 4. punkts  14. panta 5. punkta pirmā daļa  14. panta 5. punkta otrā daļa  14. panta 5. punkta trešā daļa  14. panta 6. punkts  15. panta 1. punkts  15. panta 2. punkts  15. panta 3. punkts  16. panta 1. punkts  16. panta 2. punkts  16. panta 3. punkts  16. panta 4. punkts  16. panta 5. punkts  16. panta 6. punkts  16. panta 7. punkts  16. panta 11. punkts  17. panta 1. punkts  17. panta 2. punkts  17. panta 3. punkts  18. panta 1. punkts  18. panta 2. punkts  19. panta 1. punkts  20. panta 1. punkts  20. panta 2. punkts  21. pants | | 1., 3., 6., 9., 10., 19. un 20. punkts  1., 3., 6., 9., 10., 19. un 20. punkts  1., 3., 6., 9., 10., 19. un 20. punkts    1., 3., 6., 9., 10., 19. un 20. punkts | | Ieviests pilnībā daļā par drošības prasību noteikšanu.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviests pilnībā.  Ieviests pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviests pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviests pilnībā daļā par drošības prasību noteikšanu.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā ar MK noteikumiem, kuru izdošanu paredz grozījumi likumā. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā. |  |
| Kā ir izmantota ES tiesību aktā paredzētā rīcības brīvība dalībvalstij pārņemt vai ieviest noteiktas ES tiesību akta normas? Kādēļ? | | Projekts šo jomu neskar. | | | |
| Saistības sniegt paziņojumu ES institūcijām un ES dalībvalstīm atbilstoši normatīvajiem aktiem, kas regulē informācijas sniegšanu par tehnisko noteikumu, valsts atbalsta piešķiršanas un finanšu noteikumu (attiecībā uz monetāro politiku) projektiem | | Projekts šo jomu neskar. | | | |
| Cita informācija | | Nav. | | | |
| **2. tabula Ar tiesību akta projektu izpildītās vai uzņemtās saistības, kas izriet no starptautiskajiem tiesību aktiem vai starptautiskas institūcijas vai organizācijas dokumentiem. Pasākumi šo saistību izpildei** | | | | | |
| Projekts šo jomu neskar. | | | | | |
| Cita informācija | | Nav. | | | |

|  |  |  |
| --- | --- | --- |
| **VI. Sabiedrības līdzdalība un komunikācijas aktivitātes** | | |
| 1. | Plānotās sabiedrības līdzdalības un komunikācijas aktivitātes saistībā ar projektu | Atbilstoši Ministru kabineta 2009. gada 25. augusta noteikumiem Nr. 970 “Sabiedrības līdzdalības kārtība attīstības plānošanas procesā”, lai informētu sabiedrību par projektu un dotu iespēju izteikt viedokli, projekts pirms tā iesniegšanas Valsts sekretāru sanāksmē ievietots Aizsardzības ministrijas mājaslapā. |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Lai informētu sabiedrību par projektu un dotu iespēju izteikt viedokli, projekts pirms tā iesniegšanas Valsts sekretāru sanāksmē 2018. gada 3. oktobrī ievietots Aizsardzības ministrijas mājaslapā http://www.mod.gov.lv/Ministrija/Sab\_lidzdaliba/Apd\_Tap.aspx. |
| 3. | Sabiedrības līdzdalības rezultāti | Priekšlikumi noteiktajā laika periodā netika sniegti. |
| 4. | Cita informācija | Nav. |

|  |  |  |
| --- | --- | --- |
| **VII. Tiesību akta projekta izpildes nodrošināšana un tās ietekme uz institūcijām** | | |
| 1. | Projekta izpildē iesaistītās institūcijas | Aizsardzības ministrija. |
| 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 neietekmēs pārvaldes funkcijas vai institucionālo struktūru. Jaunu institūciju izveide, esošu institūciju likvidācija vai reorganizācija nav nepieciešama. Noteikumu projekts tiks īstenots esošo cilvēkresursu ietvaros. |
| 3. | Cita informācija | Nav. |

Aizsardzības ministrs Raimonds Bergmanis

S. Žogota, 67335353

[Sanita.Zogota@mod.gov.lv](mailto:Sanita.Zogota@mod.gov.lv)