**Likumprojekta “Grozījumi Informācijas tehnoloģiju drošības likumā” sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

|  |  |
| --- | --- |
| **Tiesību akta projekta anotācijas kopsavilkums** | |
| Mērķis, risinājums un projekta spēkā stāšanās laiks (500 zīmes bez atstarpēm) | Likumprojekta “Grozījumi Informācijas tehnoloģiju drošības likumā” (turpmāk – likumprojekts) mērķis ir ieviest Eiropas Parlamenta un Padomes 2016. gada 6. jūlija direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (turpmāk – NIS direktīva).  NIS direktīva nosaka pasākumus Eiropas Savienības dalībvalstīm (turpmāk – dalībvalstis), lai panāktu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību.  Likumprojekts nosaka jaunus subjektus – pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, kuriem tiek noteikti divi galvenie pienākumi – ievērot konkrētas informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošības prasības un ziņot par drošības incidentiem.  Lai nodrošinātu iepriekš minētos pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju pienākumus, tiek noteikti jauni uzdevumi esošajām institūcijām – Informācijas tehnoloģiju drošības incidentu novēršanas institūcijai (turpmāk – CERT.LV), Digitālās drošības uzraudzības komitejai (turpmāk – komiteja), Aizsardzības ministrijai un atsevišķu nozaru uzraugošajām ministrijām.  Likumprojekts stājas spēkā 2018. gada 9. maijā. |

|  |  |  |
| --- | --- | --- |
| **I. Tiesību akta projekta izstrādes nepieciešamība** | | |
| 1. | Pamatojums | Likumprojekts ir izstrādāts, pamatojoties uz:  1) NIS direktīvas 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) Ministru kabineta 2017. gada 26. septembra sēdes protokola Nr. 48 56. § 13. punktā noteikto uzdevumu (ierobežota pieejamība). |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | 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 datorapdraudējumu reaģēšanas vienību (turpmāk – CERT).  Ņemot vērā, ka Informācijas tehnoloģiju drošības likums (turpmāk – likums) nacionāli jau regulē daļu no NIS direktīvā paredzētajiem pasākumiem, piemēram, CERT.LV uzdevumus un tiesības, informācijas tehnoloģiju drošības incidenta (turpmāk – drošības incidents) būtību. Tāpat jau šobrīd likuma 6.panta otrā daļa paredz, ka valsts un pašvaldību institūcijām, informācijas tehnoloģiju kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam drošības incidenta gadījumā ir pienākums tūlīt informēt par notikušo kompetento Drošības incidentu novēršanas institūciju. Valsts un pašvaldības institūcijām ir jānodrošina informācijas un komunikāciju tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām, ko noteicis Ministru kabinets (likuma 8.panta piektā daļa). Attiecīgi šīs prasības paredzēts saglabāt un ar likumprojektu tiek pārņemtas tās NIS direktīvas normas, kas nacionālajā līmenī nav regulētas, kā arī attiecīgi precizētas esošās tiesību normas.  Lai skaidrotu un aprakstītu, kā nacionāli tiek ieviesti iepriekš minētie NIS direktīvas pasākumi, nepieciešams norādīt, ka galvenie subjekti, uz kuriem gan tieši, gan netieši attiecas arī visi pieci pasākumi, ir **pamatpakalpojuma sniedzēji** un **digitālā pakalpojuma sniedzēji**. Tātad likums tiek papildināts ar jauniem subjektiem, kuri tiek izskaidroti.  **Pamatpakalpojuma sniedzējs**  Ar likumprojektu tiek noteikts, ka pakalpojuma sniedzējs uzskatāms par pamatpakalpojuma sniedzēju un tā pakalpojums par pamatpakalpojumu tikai tad, ja enerģētikas, transporta, banku, finanšu tirgus infrastruktūras, veselības, dzeramā ūdens piegādes vai izplatīšanas, elektronisko sakaru un digitālās infrastruktūras nozari uzraugošā ministrija (turpmāk – nozari uzraugošā ministrija) to ir identificējusi pēc noteiktiem kritērijiem.  Pamatpakalpojuma sniedzēja un pamatpakalpojuma kritēriji tiek noteikti likumprojekta 1. pantā – likuma 3.1panta pirmā daļa: 1) pakalpojuma sniedzējs ir valsts vai pašvaldības institūcija vai privāto tiesību juridiska persona; 2) tas veic saimniecisko darbību Latvijas Republikā; 3) tas sniedz pakalpojumu Eiropas Savienībā konkrētā nozarē; 4) tā sniegtais pakalpojums ir svarīgs sabiedrisku vai ekonomisku darbību nodrošināšanai; 5) tā pakalpojuma sniegšana ir atkarīga no tīklu un informācijas sistēmām; 6) tā drošības incidents var radīt būtiski traucējošu ietekmi uz pakalpojuma sniegšanu.  Savukārt kārtību, kādā iepriekš minēto identificēšanu veiks nozari uzraugošā ministrija, noteiks Ministru kabineta noteikumi (deleģējums Ministru kabinetam noteikts likumprojekta 1. pantā – likuma 3.1 panta piektā daļa). Kārtība, kādā tiek veikta identificēšana, ietver, piemēram, nozari uzraugošās ministrijas pienākumu identificēšanas procesā apspriesties ar tām dalībvalstīm, kurās vēl šis pakalpojums tiek sniegts, reizi divos gados pārskatīt identificētos pakalpojuma sniedzējus un pakalpojumus un iesniegt sarakstu Digitālās drošības uzraudzības komitejā, kā arī Digitālās drošības uzraudzības komitejas pienākumu nosūtīt informāciju identificētajiem pakalpojuma sniedzējiem, ka tie uzskatāmi par pamatpakalpojuma sniedzējiem un kuri no viņu sniegtajiem pakalpojumiem uzskatāmi par pamatpakalpojumiem.  Ministru kabineta noteikumos tiks noteikti arī drošības incidenta būtiski traucējošās ietekmes identificējošie faktori NIS direktīvas II pielikumā minētajās nozarēs – enerģētikas, transporta, banku, finanšu tirgus infrastruktūras, veselības, dzeramā ūdens piegādes vai izplatīšanas, elektronisko sakaru un digitālās infrastruktūras (deleģējums Ministru kabinetam noteikts likumprojekta 1. pantā – likuma 3.1 panta piektā daļa). Ar faktoru saprot noteiktus kritērijus, kas ir par pamatu, lai noteiktu, vai drošības incidentam būtu būtiski traucējoša ietekme, piemēram, pakalpojuma lietotāju skaits, citu nozaru atkarība no konkrētā pakalpojuma, pakalpojuma sniedzēja tirgus daļa un citi faktori. Iespējamie faktori ir minēti NIS direktīvas 6.pantā, paredzot dalībvalstu tiesības noteikt drošības incidenta būtiski traucējošās ietekmes identificējošos faktorus, ņemot vērā nozares īpatnības. Piemēram, veselības nozarē identificējošie faktori (piemēram, nozīmīgs ārstniecības pakalpojumu sniedzējs reģionā) būs atšķirīgi no banku nozares identificējošiem faktoriem (piemēram, pēc banku klientu skaita), tādēļ katra nozare tiks vērtēta atsevišķi un tai raksturīgākiem kritēriji tiks identificēti un ietverti noteikumos.  Ja nozari uzraugošā ministrija konstatē, ka pakalpojuma sniedzējs atbilst visiem likuma 3.1panta pirmās daļas kritērijiem, tas tiek uzskatīts par pamatpakalpojuma sniedzēju un uz to attiecas visi šajā likumā noteiktie pamatpakalpojuma sniedzēja pienākumi un tiesības.  **Digitālā pakalpojuma sniedzējs**  Ar likumprojektu tiek noteikts, ka digitālā pakalpojuma sniedzējs ir 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, kā arī sniedz tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai mākoņdatošanas pakalpojumu (turpmāk – digitālie pakalpojumi) kādā no dalībvalstīm (likumprojekta 1. pants – likuma 3.1 panta otrās daļas 1. punkts). Pakalpojuma sniedzējs identificē pats sevi pēc likuma 3.1 panta otrās daļas 1. punktā norādītajiem kritērijiem. Ja tas atbilst kritērijiem, tam jāievēro visi likumā norādītie digitālā pakalpojuma sniedzēja pienākumi un uz to attiecas digitālā pakalpojuma sniedzēja tiesības. Papildus jānorāda, ka likuma 3.1 panta ceturtā daļa (likumprojekta 1. pants) paredz izņēmuma gadījumu, kad pakalpojuma sniedzējs netiek uzskatīts par digitālā pakalpojuma sniedzēju, lai arī tas atbilst iepriekš norādītajiem kritērijiem, t. i., nodarbināto personu skaits, apgrozījums vai gada bilances kopsumma nesasniedz konkrētos rādītājus.  Likumprojektā norādīts, ka digitālā pakalpojuma sniedzēja pārstāvis arī uzskatāms par digitālā pakalpojuma sniedzēju šā likuma izpratnē (likumprojekta 1. pants – likuma 3.1 panta trešā daļa). Likumprojekts attiecībā uz digitālā pakalpojuma sniedzēja pārstāvi nosaka, ka trešās valsts digitālā pakalpojuma sniedzējam, kurš saimniecisko darbību veic ārpus Eiropas Savienības, bet digitālo pakalpojumu sniedz Latvijā, nepieciešams pārstāvis. Digitālā pakalpojuma sniedzēja pārstāvis ir fiziska vai juridiska persona, kas veic saimniecisko darbību Latvijā un rīkojas trešās valsts digitālā pakalpojuma sniedzēja interesēs Latvijā.  **1. Stratēģija**  NIS direktīva katrai valstij paredz pienākumu pieņemt stratēģiju, kura nosaka valsts stratēģiskos mērķus, prioritātes, politikas un regulatīvos pasākumus, lai panāktu un saglabātu augsta līmeņa tīklu un informācijas sistēmu drošību attiecībā uz pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem. Latvijā Ministru kabinets ar 2014. gada 21. janvāra rīkojumu Nr. 40 apstiprināja pamatnostādnes “Latvijas kiberdrošības stratēģija 2014.–2018. gadam”, nosakot Latvijas kiberdrošības politikas mērķi, rīcības virzienus un sasniedzamos uzdevumus, kas arī daļēji aptver NIS direktīvā stratēģijai izvirzītās prasības.  Aizsardzības ministrija ir noteikta par atbildīgo institūciju pamatnostādņu izpildes koordinācijā. Tā kā normatīvie akti neparedz kiberdrošības stratēģijas izstrādi, ar likuma 11. pantu (likumprojekta 6. pantu) ir paredzēts noteikt, ka Aizsardzības ministrija reizi četros gados nodrošina Nacionālās kiberdrošības stratēģijas izstrādi un to apstiprina Ministru kabinets. Nacionālā kiberdrošības stratēģija noteiks kiberdrošības politikas veidošanas pamatprincipus, mērķi un stratēģiskās prioritātes, tajā skaitā NIS direktīvā paredzēto – stratēģiskos mērķus, politikas un regulējošos pasākumus, lai panāktu un saglabātu augsta līmeņa tīklu un informācijas sistēmu drošību pamatpakalpojuma sniedzējiem, pamatpakalpojumiem, digitālā pakalpojuma sniedzējiem un digitālajiem pakalpojumiem. Ņemot vērā kiberjomas mainīgo dabu, kiberdrošības stratēģijas termiņš tiek mainīts no pieciem uz četriem gadiem.  **2. Sadarbības grupa**  NIS direktīva nosaka, ka tiek izveidota sadarbības grupa. Sadarbības grupa sastāv no dalībvalstu pārstāvjiem, Eiropas Komisijas un ES Tīklu un informācijas drošības aģentūras (turpmāk – ENISA*)*. Aizsardzības ministrija pārstāv Latviju sadarbības grupā. NIS direktīvā saistībā ar sadarbības grupu galvenie pienākumi tiek uzdoti Eiropas Komisijai, kura nodrošina sadarbības grupas sekretariātu, un ENISA, kura palīdz dalībvalstīm spēju veidošanā, lai nodrošinātu vienādi augstu tīklu un informācijas sistēmu drošību visās dalībvalstīs. Sadarbības grupa ir izveidota, lai ar dalībvalstu palīdzību atbalstītu un atvieglotu stratēģisko sadarbību, apmainītos ar informāciju, nodrošinātu paļāvību un uzticēšanos starp dalībvalstīm.  Ar likumprojektu tiek noteikts, ka Aizsardzības ministrijai ir pienākums vienu reizi gadā iesniegt sadarbības grupai ziņojumu par pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju drošības incidentiem, t. i., sniegt informāciju par pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju iesniegto ziņojumu skaitu, pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju drošības incidentu raksturu un drošības incidentiem, kuri skāruši citas dalībvalstis (likumprojekta 3. pants – likuma 5.2 panta 2. punkts).  **3. CSIRT tīkls**  NIS direktīva nosaka, ka tiek izveidots CSIRT tīkls. CSIRT tīkls sastāv no dalībvalstu CERT vienībām. Saistībā ar CSIRT tīklu galvenie pienākumi tiek uzdoti Eiropas Komisijai, kura CSIRT tīklā ir novērotāja statusā, un ENISA, kura nodrošina CSIRT tīkla sekretariātu un aktīvi atbalsta sadarbību starp dalībvalstu CERT.  CSIRT tīkls tiek veidots, lai palīdzētu attīstīt paļāvību, uzticēšanos un veicinātu ātru un efektīvu operatīvo sadarbību starp dalībvalstu CERT. Tas palīdzēs dalībvalstu CERT apmainīties ar informāciju, dalīties ar savas valsts pieredzi, piemēram, apspriest reaģēšanu uz incidentiem, pieredzi saistībā ar tīklu un informācijas sistēmu drošību, CERT spējas un sagatavotību.  Ar likumprojektu tiek noteikts, ka CERT.LV sadarbojas ar CSIRT tīklu (likumprojekta 2. pants – likuma 5. panta pirmās daļas 7.5 punkts).  **4. Paziņošanas un drošības prasības**  NIS direktīva uzliek par pienākumu pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem nacionālajā regulējumā noteikt divus galvenos pienākumus: 1) pamatpakalpojuma sniedzēja un digitālā pakalpojuma sniedzēja pienākums ziņot par konkrētiem drošības incidentiem; 2) ievērot noteiktas drošības prasības attiecībā uz savām informācijas tehnoloģijām, tostarp tīklu un informācijas sistēmām.  **4.1. Paziņošanas prasības**  Ar likumprojektu tiek noteikts pienākums pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējam ziņot CERT.LV par drošības incidentiem, kuriem ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu (likumprojekta 4. panta pirmā daļa – likuma 6. panta otrā prim daļa). Ja pamatpakalpojuma sniedzējs ir valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, uz to neattiecas jaunā likuma 6. panta otrā prim daļa, bet attiecas iepriekš noteiktās ziņošanas prasības un tas ziņo, kā parasti, par likuma 6. panta pirmajā daļā norādīto drošības incidentu. Drošības incidents, par kuru jāziņo saskaņā ar likuma 6. panta pirmo daļu (likumā esošā norma), ir ar plašāku nozīmi nekā drošības incidents, par kuru jāziņo saskaņā ar likuma 6. panta otrā prim daļu (ar likumprojektu noteiktā jaunā norma).  Likumprojekts nosaka, ka pamatpakalpojuma sniedzējs ziņo tikai par tādu drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību, bet digitālā pakalpojuma sniedzējs ziņo par tādu drošības incidentu, kuram ir būtiska ietekme uz pakalpojuma sniegšanu. Ņemot vērā minēto, Ministru kabinets noteiks drošības incidenta būtiskuma kritērijus gan pamatpakalpojuma sniedzējam, gan digitālā pakalpojuma sniedzējam (deleģējums Ministru kabinetam noteikts likumprojekta 4. panta trešajā daļā –likuma 6. panta septītā daļa). Ar būtiskuma kritērijiem saprot, piemēram, pamatpakalpojuma vai digitālā pakalpojuma traucējumu skarto lietotāju skaitu, incidenta ilgumu, incidenta ģeogrāfisko izplatību, cik lielā mērā ietekmētas ekonomiskās un sabiedriskās darbības. Konkrētie kritēriji ļaus pakalpojuma sniedzējam saprast, vai tam jāziņo par radušos drošības incidentu. Ministru kabineta noteikumi noteiks arī informēšanas kārtību un ziņojuma saturu (deleģējums Ministru kabinetam noteikts likumprojekta 4. panta trešajā daļā – likuma 6. panta septītā daļa), kas ietvers, piemēram, to, cik ilgā laikā jāziņo CERT.LV par radušos drošības incidentu un kāda informācija par drošības incidentu jānorāda.  Ņemot vērā to, ka likums valsts vai pašvaldības institūcijām, informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem jau uzliek par pienākumu ziņot par jebkuru drošības incidentu, un iepriekš minētie subjekti saskaņā ar jaunajām likumprojekta normām var tikt identificēti kā pamatpakalpojuma sniedzēji, tad daļēji NIS direktīvas ziņošanas pienākums jau nacionāli tiek pildīts (likuma 6.panta otrā daļa).  **4.2. Drošības prasības**  Ar likumprojektu tiek noteikts pienākums pamatpakalpojuma sniedzējiem, digitālā pakalpojuma sniedzējiem un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem ievērot konkrētas informācijas tehnoloģiju drošības prasības.  Likuma 8. panta piektā daļa attieksies arī uz informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem (likumprojekta 5. panta piektā daļa), noteiktās minimālās drošības prasības un kārtība, kādā to nodrošina attieksies arī uz minētajiem subjektiem. Šādi grozījumi netiek veikti saistībā ar NIS direktīvu, bet tie tiek veikti tādēļ, ka Ministru kabineta 2011. gada 1. februāra noteikumos Nr. 100 “Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība” nav noteiktas konkrētas drošības prasības, kādām jāatbilst kritiskās infrastruktūras informācijas tehnoloģijām. Lai nodrošinātu vienotu minimālo drošības līmeni visos sektoros, prasība ievērot minimālos noteikumus, tagad attieksies arī uz kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem. Jānorāda, ka tie ir tikai minimālie noteikumi un drošības līmenis, protams, drīkst būt arī augstāks.  Savukārt 8. pants tiek papildināts ar sesto daļu, nosakot, ka arī NIS direktīvas subjektiem – pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem, uz kuriem neattiecas 8. panta piektajā daļā norādītās drošības prasības – jāievēro konkrētas drošības prasības (likumprojekta 5. panta sestā daļa). Panta sestā daļa un uz tā pamata izdotie Ministru kabineta noteikumi regulēs tikai minimālās drošības prasības, bet ne kārtību, kādā minētie subjekti to nodrošina, jo NIS direktīva uzliek par pienākumu nacionālajā regulējumā noteikt tikai drošības prasības.  Ņemot vērā to, ka likums jau nosaka minimālās drošības prasības valsts un pašvaldības institūcijām un iepriekš minētie subjekti var tikt identificēti kā pamatpakalpojuma sniedzēji, tad daļēji NIS direktīvas drošības prasību ievērošanas pienākums jau nacionāli tiek pildīts (likuma 8.panta piektā daļa).  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 izmaksā dārgāk drošības incidenta seku novēršana, nekā sakārtot sistēmu drošību. Informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmām tiks noteiktas minimālās drošības prasības, kas būtu jāievēro ikvienai institūcijai, privāto tiesību juridiskai personai, kas sniedz pakalpojumus, izmantojot informācijas tehnoloģijas. Normas tiks iekļautas Ministru kabineta 2015.gada 28.jūlija noteikumos Nr.442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” un drošības prasības netiks noteiktas stingrākas, kādas tās ir valsts un pašvaldības institūcijām.  **5. Kompetentā iestāde, vienotais kontaktpunkts un CERT**  NIS direktīva paredz dalībvalstīm pienākumu izraudzīties kompetento iestādi, vienoto kontaktpunktu un CERT, uzticot tiem uzdevumus un pienākumus saistībā ar tīklu un informācijas sistēmu drošību. Anotācijas V sadaļā – Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām tiesībām – ir iespējams iepazīties ar informāciju par to, kuras nacionālās iestādes veic NIS direktīvā norādītās kompetentās iestādes, kontaktpunkta un CERT funkcijas. NIS direktīva neaizliedz, piemēram, kompetentās iestādes funkcijas nacionāli sadalīt vairākām institūcijām.  **5.1. Kompetentā iestāde**  Ar likumprojektu NIS direktīvā noteiktās kompetentās iestādes funkcijas veic komiteja. Saistībā ar kompetento iestādi likums papildināts ar 5.1pantu (likumprojekta 3. pants), kurš nosaka komitejas kā kompetentās iestādes uzdevumus un tiesības. Piemēram, komiteja sadarbojas ar nozari uzraugošajām ministrijām pamatpakalpojuma sniedzēju un pamatpakalpojumu identificēšanas procesā un sagatavo pamatpakalpojuma sniedzēju un pamatpakalpojumu sarakstu, reizi divos gados nosūta informāciju Eiropas Komisijai par to, kā Latvijā tiek identificēti pamatpakalpojuma sniedzēji (likumprojekta 1. pants – likuma 3.1 panta pirmā daļa), identificēto pamatpakalpojumu sarakstu, pamatpakalpojumu sniedzēju skaitu, neminot konkrētus pakalpojuma sniedzējus (šo informāciju katrai valstij ir tiesības neizpaust), un drošības incidenta būtiski traucējošās ietekmes identificējošos faktorus (likumprojekta 1. pants – likuma 3.1 panta piektā daļa), jo tie katrā valstī atšķiras. Komiteja ir tiesīga prasīt, lai pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji novērš drošības neatbilstības un ziņo par drošības incidentiem, par kuriem tiem saskaņā ar likumu ir jāziņo. Ja minētie subjekti nepilda komitejas norādījumus, komitejai ir tiesības Administratīvā procesa likuma noteiktajā kārtībā veikt lēmuma piespiedu izpildi, komiteja ir tiesīga sagatavot brīdinājumu par lēmuma piespiedu izpildi, kurā ietver norādi par piemērojamiem piespiedu izpildes līdzekļiem, piemēram, piespiedu nauda. Ar lēmuma piespiedu izpildi tiek realizēts NIS direktīvas 21. pants par sankcijām.  **5.2. Vienotais kontaktpunkts**  Ar likumprojektu NIS direktīvā noteiktās vienotā kontaktpunkta (turpmāk – kontaktpunkts) funkcijas veic Aizsardzības ministrija. Saistībā ar kontaktpunktu likums papildināts ar 5.2 pantu (likumprojekta 3. pants), kurš nosaka Aizsardzības ministrijas, kā kontaktpunkta, uzdevumus, piemēram, sadarbību ar citu dalībvalstu kontaktpunktiem un sadarbības grupu.  **5.3. CERT**  Ar likumprojektu tiek paplašinātas likumā noteiktās CERT.LV funkcijas (papildināta likuma 5. panta pirmā daļa – likumprojekta 2. panta otrā daļa). CERT.LV noteikti šādi papildus uzdevumi: 1) informēt Aizsardzības ministriju par pamatpakalpojuma sniedzēju un digitālā pakalpojuma sniedzēju drošības incidentiem, lai Aizsardzības ministrija šo informāciju var nodot sadarbības grupai; 2) informēt arī citas dalībvalstis vai lūgt, lai Aizsardzības ministrija informē citu dalībvalstu kontaktpunktus, ja atklātajam drošības incidentam ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu konkrētajā valstī; 3) informēt komiteju par pamatpakalpojumu sniedzēju vai digitālā pakalpojuma sniedzēju drošības prasību neatbilstībām vai atklātajiem gadījumiem, kad tie nav saskaņā ar likumu ziņojuši par drošības incidentiem, savukārt komiteja tālāk ar šo informāciju var rīkoties, lai veiktu likumā noteiktās administratīvās procedūras; 4) sadarboties ar CSIRT tīklu. NIS direktīvā norādīts, ka sadarbību ar CSIRT tīklu veic kontaktpunkts, bet, ņemot vērā CERT.LV funkcijas, šī funkcija nacionāli vairāk atbilst CERT.LV funkcijām.  Ņemot vērā to, ka saskaņā ar likuma 4. panta pirmo daļu Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas uzdevumus veic ne vien CERT.LV, bet arī Militārā izlūkošanas un drošības dienests (attiecībā uz Aizsardzības ministriju, tās padotībā esošajām iestādēm un Nacionālajiem bruņotajiem spēkiem), tad tiek papildināta likuma 5. panta pirmā prim daļa nosakot jaunus uzdevumus arī Militārā izlūkošanas un drošības dienestam (likumprojekta 2.panta trešā daļa). |
| 3. | Projekta izstrādē iesaistītās institūcijas un publiskas personas kapitālsabiedrības | CERT.LV, Satversmes aizsardzības birojs. |
| 4. | Cita informācija | Aizsardzības ministrija, CERT.LV, komiteja un Militārās izlūkošanas un drošības dienests likumprojektā paredzēto jauno pienākumu izpildi nodrošinās Aizsardzības ministrijas budžeta ietvaros no budžeta programmas 30.00.00 “Valsts aizsardzības politikas realizācija”.  Nozari uzraugošās ministrijas likumprojekta paredzēto jauno pienākumu izpildi nodrošinās attiecīgo nozari uzraugošo ministriju budžeta ietvaros.  Valsts un pašvaldību institūcijas, kuras nozari uzraugošās ministrijas identificēs Ministru kabineta noteiktajā kārtībā kā pamatpakalpojuma sniedzējus vai kuras sevi identificēs kā digitālā pakalpojuma sniedzējus, likumprojektu īstenos sava budžeta ietvaros. |

|  |  |  |
| --- | --- | --- |
| **II. Tiesību akta projekta ietekme uz sabiedrību, tautsaimniecības attīstību un administratīvo slogu** | | |
| 1. | Sabiedrības mērķgrupas, kuras tiesiskais regulējums ietekmē vai varētu ietekmēt | Likumprojekts ietekmēs:  1) **nozari uzraugošās ministrijas**, kuru pienākums ir identificēt pamatpakalpojuma sniedzējus Ministru kabineta noteiktajā kārtībā (deleģējums likumprojekta 1. pantā – likuma 3.1 panta pirmā daļa);  2) **pakalpojuma sniedzējus**, kurus nozari uzraugošā ministrija identificēs kā pamatpakalpojuma sniedzējus vai kuri sevi būs identificējuši kā digitālā pakalpojuma sniedzējus. Minētajiem pakalpojuma sniedzējiem būs jāievēro šajā likumprojektā un uz tā pamata izdotajos Ministru kabineta noteikumos noteiktie pienākumi drošības prasību ievērošanā un ziņošanā par drošības incidentiem;  3) **CERT.LV un Militārās izlūkošanas un drošības dienests**, kurai saskaņā ar NIS direktīvu tiek uzdoti jauni pienākumi;  4) **komiteju**, kurai saskaņā ar likumprojektu ir jāveic NIS direktīvā noteiktie kompetentās iestādes uzdevumi;  5) **Aizsardzības ministriju**, kurai saskaņā ar likumprojektu ir jāveic NIS direktīvā noteiktie kontaktpunkta uzdevumi. |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Likumprojekta tiesiskais regulējums sabiedrības mērķgrupām uzliek jaunus pienākumus un izvirza jaunas veicamās darbības, kas pozitīvi **ietekmē tautsaimniecību**.  Likumprojektā norādītie pamatpakalpojuma sniedzēji aptver tādas sabiedrībai svarīgas nozares kā enerģētika, transports, bankas, finanšu tirgus infrastruktūra, veselība un citas nozares (NIS direktīvas II pielikums). Tīklu un informācijas sistēmu drošība ir īpaši nozīmīga pamatpakalpojuma sniedzējiem, kuri nodrošina apjomīgu tirgus daļu no konkrētajā nozarē sniegtā pakalpojuma. Tas ir sabiedrības interesēs, lai šo nozaru pakalpojuma sniedzēji ievēro informācijas tehnoloģiju, tostarp tīklu un informācijas sistēmu, drošību un ziņo par to drošības incidentiem.  Nosakot minimālās drošības prasības pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem, tas nodrošinās sabiedrībai svarīgu pakalpojumu nepārtrauktību, mazinās risku, ka drošības incidentu rezultātā tiks neatgriezeniski vai ilglaicīgi traucēta sabiedrībai kritiski svarīgu pakalpojumu saņemšana, un citu negatīvo ietekmi uz sabiedrībai ikdienā svarīgiem pakalpojumiem.  Pienākums pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem ziņot par drošības incidentiem stiprinās reaģētspēju uz drošības incidentiem un veicinās pakalpojumu sniedzēju atbildības kultūru par savu tīklu un informācijas sistēmu drošību.  Ņemot vērā CERT.LV kompetenci, likumprojektā noteiktā CERT.LV iesaiste drošības incidentu novēršanā uzlabos drošības incidentu novēršanas pasākumu kvalitāti, jo pašam pakalpojuma sniedzējam var nebūt pietiekama kompetence vai informācija, lai risinātu drošības incidentu novēršanu bez papildu ekspertu iesaistes. CERT.LV, pamatojoties uz pamatpakalpojuma sniedzēja vai digitāla pakalpojuma sniedzēja savlaicīgi iesniegto informāciju, varēs sniegt nepieciešamās rekomendācijas un atbalstu drošības incidentu novēršanā.  Likumprojektā noteiktais CERT.LV pienākums sadarboties ar citu valstu kompetentajām iestādēm un Aizsardzības ministrijas pienākums sadarboties ar citu dalībvalstu kontaktpunktiem uzlabos sadarbībspēju ar citām valstīm drošības incidentu novēršanā.  Likumprojekta tiesiskais regulējums paredz **administratīvā sloga palielināšanos** visām anotācijas II sadaļas 1. punktā minētajām sabiedrības mērķgrupām.  **Pamatpakalpojuma sniedzējam un digitālā pakalpojuma sniedzējam** palielināsies administratīvais slogs, jo tiek noteikts pienākums ziņot par konkrētiem drošības incidentiem (likumprojekta 4. panta pirmā daļa – likuma 6. panta otrā prim daļa), precīzāk, drošības incidentus, par kuriem jāziņo CERT.LV, regulēs saskaņā ar likuma 6. panta septīto daļu izdotie Ministru kabineta noteikumi (likumprojekta 4. panta trešā daļa).  Administratīvais slogs palielināsies arī pamatpakalpojuma sniedzējiem, digitālā pakalpojuma sniedzējam un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem, jo ar likumprojektu tiek noteikts pienākums ievērot konkrētas drošības prasības (papildināts likuma 8. pants ar jauniem subjektiem), precīzāk, drošības prasības regulēs saskaņā ar likuma 8. panta piekto un sesto daļu izdotie Ministru kabineta noteikumi (likumprojekta 5. panta piektā un sestā daļa).  Arī **CERT.LV** administratīvais slogs palielināsies, jo tai būs jāapstrādā lielāks skaits ziņojumu, nekā tas bija iepriekš, kad ziņošanas prasība bija obligāta tikai valsts, pašvaldības institūcijām un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem. Likumprojekts palielinās CERT.LV administratīvo slogu, jo tai tiek uzlikti jauni pienākumi, piemēram, sadarbība ar Eiropas CSIRT tīklu, citu dalībvalstu kompetentajām iestādēm un komiteju.  **Komitejas** administratīvā sloga palielināšanās saistīta ar pamatpakalpojumu sniedzēju identificēšanu, pienākumu prasīt, lai pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji ievēro likumā noteiktos pienākumus par ziņošanu un drošības prasību ievērošanu. Komitejai administratīvais slogs palielināsies arī saistībā ar lēmuma piespiedu izpildi, ja tas būs nepieciešams.  **Aizsardzības ministrijai** palielināsies administratīvais slogs, nodrošinot sadarbību ar citu dalībvalstu kontaktpunktiem un NIS direktīvas sadarbības grupu, kā arī izstrādājot nacionālās kiberdrošības stratēģiju, kura tagad ietvers arī sadaļu par regulējošajiem pasākumiem, lai panāktu un saglabātu augsta līmeņa tīklu un informācijas sistēmu drošību pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem.  **Nozari uzraugošajām ministrijām** palielināsies administratīvais slogs saistībā ar pamatpakalpojuma sniedzēju identificēšanu. |
| 3. | Administratīvo izmaksu monetārs novērtējums | Ņemot vērā, ka pašreiz likumprojektā ietvertais tiesiskais regulējums nenosaka precīzu subjektu skaitu, uz kuriem tas attieksies, t. i., attieksies regulējums par ziņošanu un drošības prasību ievērošanu (to noteiks uz likuma 3.1panta pamata izdotie Ministru kabineta noteikumi – likumprojekta 1. pants), administratīvās izmaksas nav iespējams noteikt.  Paredzams, ka izmaksas veidos pakalpojuma sniedzēju sistēmu pielāgošana drošības prasībām, bet, tā kā drošības prasības ir minimālās atbilst informācijas un komunikācijas tehnoloģiju pārvaldības labajai praksei, valsts un pašvaldību institūcijām un privāto tiesību juridiskajām personām, kuras nozari uzraugošās ministrijas identificēs kā pamatpakalpojuma sniedzēju vai kuras identificēs sevi kā digitālā pakalpojuma sniedzējus, likumprojektā paredzēto pienākumu izpilde neradīs būtiskas izmaiņas un izmaksas.  Valsts un pašvaldību institūcijas, privāto tiesību juridiskās personas, kuras nozari uzraugošās ministrijas būs identificējušas Ministru kabineta noteiktajā kārtībā kā pamatpakalpojuma sniedzējus vai kuras sevi identificēs kā digitālā pakalpojuma sniedzējus, likumprojektu īstenos sava budžeta ietvaros.  Aizsardzības ministrija, CERT.LV un komiteja likumprojektā paredzēto jauno pienākumu izpildi nodrošinās Aizsardzības ministrijas budžeta ietvaros no budžeta programmas 30.00.00 “Valsts aizsardzības politikas realizācija”.  Militārās izlūkošanas un drošības dienests jauno pienākumu izpildi nodrošinās esošo finanšu resursu ietvaros.  Nozari uzraugošās ministrijas likumprojekta paredzēto jauno pienākumu izpildi nodrošinās attiecīgo nozari uzraugošo ministriju budžeta ietvaros. |
| 4. | Atbilstības izmaksu monetārs novērtējums | *Skat. anotācijas II sadaļas 3. punktu.* |
| 5. | Cita informācija | Likumprojekta tiesiskais regulējums neattiecas uz elektronisko sakaru komersantiem Elektronisko sakaru likuma izpratnē un uz uzticamiem sertifikācijas pakalpojumu sniedzējiem Elektronisko dokumentu likuma izpratnē.  Likumprojekta tiesiskais regulējums neattiecas uz privāto tiesību juridisko personu, kas uzskatāma par digitālā pakalpojumu sniedzēju likuma 3.1 panta otrās daļas izpratnē, taču nodarbina mazāk par 250 personām un tās gada apgrozījums nepārsniedz 50 miljonus *euro* vai gada bilances kopsumma nepārsniedz 43 miljonus *euro*. |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** | | | | | | | | | | |
| Rādītāji | n-gads | | Turpmākie trīs gadi (*euro*) | | | | | | | |
| n+1 | | | n+2 | | | n+3 | |
| saskaņā ar valsts budžetu kārtējam gadam | izmaiņas kārtējā gadā, salīdzinot ar valsts budžetu kārtējam gadam | saskaņā ar vidēja termiņa budžeta ietvaru | | izmaiņas, salīdzinot ar vidēja termiņa budžeta ietvaru n+1 gadam | | saskaņā ar vidēja termiņa budžeta ietvaru | izmaiņas, salīdzinot ar vidēja termiņa budžeta ietvaru n+2 gadam | | izmaiņas, salīdzinot ar vidēja termiņa budžeta ietvaru n+2 gadam |
| 1 | 2 | 3 | 4 | | 5 | | 6 | 7 | | 8 |
| 1. Budžeta ieņēmumi | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 1.1. valsts pamatbudžets, tai skaitā ieņēmumi no maksas pakalpojumiem un citi pašu ieņēmumi | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 1.2. valsts speciālais budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 1.3. pašvaldību budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 2. Budžeta izdevumi | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 2.1. valsts pamatbudžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 2.2. valsts speciālais budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 2.3. pašvaldību budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 3. Finansiālā ietekme | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 3.1. valsts pamatbudžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 3.2. speciālais budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 3.3. pašvaldību budžets | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 4. Finanšu līdzekļi papildu izdevumu finansēšanai (kompensējošu izdevumu samazinājumu norāda ar "+" zīmi) | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 5. Precizēta finansiālā ietekme | 0 | 0 | 0 | | 0 | | 0 | 0 | | 0 |
| 5.1. valsts pamatbudžets | 0 | 0 | | 0 | | 0 |
| 5.2. speciālais budžets | 0 | 0 | | 0 | | 0 |
| 5.3. pašvaldību budžets | 0 | 0 | | 0 | | 0 |
| 6. Detalizēts ieņēmumu un izdevumu aprēķins (ja nepieciešams, detalizētu ieņēmumu un izdevumu aprēķinu var pievienot anotācijas pielikumā) | CERT.LV, Aizsardzības ministrija, Militārās izlūkošanas un drošības dienests, komiteja un nozaru uzraugošās ministrijas ar NIS direktīvu uzliktos jaunos pienākumus veic esošo finanšu resursu ietvaros. | | | | | | | | | |
| 6.1. detalizēts ieņēmumu aprēķins |
| 6.2. detalizēts izdevumu aprēķins |
| 7. Amata vietu skaita izmaiņas | CERT.LV, Militārās izlūkošanas un drošības dienests, Aizsardzības ministrija, komiteja un nozaru uzraugošās ministrijas ar NIS direktīvu uzliktos jaunos pienākumus veic esošo cilvēkresursu ietvaros. | | | | | | | | | |
| 8. Cita informācija | Nav. | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** | | |
| 1. | Saistītie tiesību aktu projekti | Likumprojekts paredz izstrādāt:  1. Ministru kabineta noteikumus, kas nosaka kārtību, kādā nozari uzraugošā ministrija identificē pamatpakalpojuma sniedzējus un pamatpakalpojumus un iesniedz informāciju par identificētajiem pamatpakalpojuma sniedzējiem un pamatpakalpojumiem komitejā (deleģējums noteikts likumprojekta 1. pantā – likuma 3.1panta piektā daļa).  2. Ministru kabineta noteikumus, kas nosaka drošības incidenta būtiski traucējošās ietekmes identificējošos faktorus (deleģējums noteikts likumprojekta 1. pantā – likuma 3.1 panta piektā daļa). Likuma 3.1panta pirmā daļa nosaka vairākus kritērijus, kurus izmantos nozari uzraugošā institūcija, lai identificētu pamatpakalpojuma sniedzējus, un viens no šiem kritērijiem ir drošības incidenta būtiski traucējošā ietekme. Šie Ministru kabineta noteikumi noteiks būtiski traucējošās ietekmes faktorus katrā no nozarēm, lai nozari uzraugošā ministrija varētu noteikt, vai konkrētais pakalpojuma sniedzējs ir pamatpakalpojuma sniedzējs. Šos Ministru kabineta noteikumus lietderīgi būtu apvienot ar pirmajā punktā norādītajiem Ministru kabineta noteikumiem, jo tie abi attieksies uz nozari uzraugošajām ministrijām pamatpakalpojuma sniedzēju identificēšanas procesā.  3. Ministru kabineta noteikumus, kas nosaka drošības incidenta būtiskuma kritērijus, informēšanas kārtību un ziņojuma saturu (deleģējums noteikts likumprojekta 4. panta trešajā daļā – likuma 6. panta septītā daļa). Likuma 6. panta otrā prim daļa nosaka, ka pamatpakalpojuma sniedzējs un digitālā pakalpojuma sniedzējs ziņo CERT.LV par tādu drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu. Šie Ministru kabineta noteikumi noteiks drošības incidenta būtiskuma kritērijus gan pamatpakalpojuma sniedzējam, gan digitālā pakalpojuma sniedzējam. Ar būtiskuma kritērijiem saprot, piemēram, pamatpakalpojuma vai digitālā pakalpojuma traucējumu skarto lietotāju skaitu, incidenta ilgumu, incidenta ģeogrāfisko izplatību, cik lielā mērā ietekmētas ekonomiskās un sabiedriskās darbības. Konkrētie kritēriji ļaus pakalpojuma sniedzējam saprast, vai tam jāziņo par radušos drošības incidentu. Ministru kabineta noteikumi noteiks arī informēšanas kārtību un ziņojuma saturu, kas ietvers, piemēram, to, cik ilgā laikā jāziņo CERT.LV par radušos drošības incidentu un kāda informācija par drošības incidentu jānorāda.  Likumprojekts paredz izdarīt grozījumus Ministru kabineta noteikumos, kas nosaka informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā valsts un pašvaldību institūcijas nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām (deleģējums noteikts likumprojekta 5. panta piektajā un sestajā daļā – likuma 8. panta piektā daļa; Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”). Grozījumi šajos Ministru kabineta noteikumos jāizdara tāpēc, ka minimālās drošības prasības attieksies arī uz pamatpakalpojuma sniedzējiem, digitālā pakalpojuma sniedzējiem, konkrēti privāto tiesību juridiskajām personām, un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem. Noteikumos tiks paredzēts arī pārejas posms, lai pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji varētu sakārtot savas informācijas tehnoloģiju sistēmas, lai tās atbilstu noteiktām drošības prasībām. |
| 2. | Atbildīgā institūcija | Aizsardzības ministrija. |
| 3. | Cita informācija | Ar likumprojekta 7. pantu tiek papildināti likuma Pārejas noteikumi, kuru 6. punkts nosaka, ka Ministru kabinets līdz 2018. gada 1. augustam izdod šā likuma 3.1panta piektajā daļā paredzētos noteikumus. Pārejas noteikumu 6. punkts izstrādāts, pamatojoties uz NIS direktīvas 5. panta 1. punktu. Pārējos Ministru kabineta noteikumus saskaņā ar NIS direktīvu jāizdod līdz 2018. gada 9. maijam. |

|  |  |  |
| --- | --- | --- |
| **V. Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām saistībām** | | |
| 1. | Saistības pret Eiropas Savienību | Ar likumprojektu 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. NIS direktīvas prasības jāievieš nacionālajos normatīvajos aktos līdz 2018. gada 9. maijam. Izņēmums ir nozari uzraugošās institūcijas pienākums identificēt pamatpakalpojuma sniedzējus – šis pienākums saskaņā ar NIS direktīvu ir jāveic līdz 2018. gada 9. novembrim. |
| 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 likumprojektu 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 a) apakšpunkts  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 | 6. pants  4. panta pirmā daļa, trešā daļa un 5. pants    Likuma 6.panta otrā daļa un 8.panta piektā daļa  2. panta otrā daļa un 3. pants  1. pants  1. pants un 7. pants  1. pants un 7. pants  1. pants un 7. pants  1. pants un 7. pants  1. pants un 7. pants  3. pants un 7. pants  1. pants un 7. pants  6. pants  3. pants  3. pants  3. pants  3. pants  Valsts pārvaldes iekārtas likuma 54. panta pirmā daļa  likuma 4. pants un 5. pants  Valsts pārvaldes iekārtas likuma 54. panta pirmā daļa  4. panta pirmā daļa  2. panta otrā daļa  3. pants un 7. pants  5. pants  Likuma 8.panta piektā daļa  4. panta pirmā un trešā daļa  Likuma 6.panta otrā daļa  4. panta pirmā un trešā daļa  Likuma 6.panta otrā daļa  4. panta trešā daļa  2. panta otrā daļa  4. panta pirmā daļa  3. pants  4. panta pirmā daļa  likuma 4. pants un 5. pants  likuma 4. panta piektā daļa, likuma 5. panta otrās daļas 1. un 2. punkts,  likumprojekta 2. panta ceturtā daļa  likuma 6. panta otrās daļas 4. punktu  5. pants  4. panta pirmā un trešā daļa  4. panta pirmā un trešā daļa  4. panta trešā daļa  4. panta trešā daļa  2. panta otrā daļa  4. panta pirmā daļa  1. pants  likuma 5. panta pirmās daļas 6. punkts;  likumprojekta 2. panta ceturtā daļa  likuma 4. panta piektā daļa, likuma 5. panta otrās daļas 1. un 2. punkts,  likumprojekta 2. panta ceturtā daļa  2. panta otrā daļa  1. pants  1. pants  5. pants  likuma 6. panta trešā daļa  4. panta trešā daļa  3. pants un  Administratīvā procesa likuma 361. panta trešās daļas 6. punkts un 368. panta  pirmā daļa | Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 1. augustam, kad tiks izdoti MK noteikumi. 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 daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviests pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā.  Ieviesta daļēji, norma tiks ieviesta pilnībā līdz 2018. gada 9. maijam, kad tiks izdoti MK noteikumi. Atbildīgā – Aizsardzības ministrija.  Ieviesta pilnībā. | Likumprojekta vienības neparedz stingrākas prasības. |
| Kā ir izmantota ES tiesību aktā paredzētā rīcības brīvība dalībvalstij pārņemt vai ieviest noteiktas ES tiesību akta normas? Kādēļ? | 1. **8. panta 1. punkts** ieviests ar likumprojekta 3. pantu, un kontaktpunkta funkcijas ir uzticētas esošajai institūcijai – Aizsardzības ministrijai, jo tā koordinē informācijas tehnoloģiju drošības politikas veidošanu un īstenošanu; 2. **10. panta 2. punkts** ieviests ar likumprojekta 4. panta pirmo daļu, paziņojumus par drošības incidentiem saņem CERT.LV, jo nacionāli arī valsts, pašvaldības un informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks un tiesiskais valdītājs par drošības incidentiem ziņo CERT.LV (likuma 6. panta otrā daļa); 3. **10. panta 3. punkta pirmā daļa** ieviesta ar likumprojekta 2. panta otro daļu, ņemot vērā, ka ziņojumus par drošības incidentiem saņem CERT.LV, tad CERT.LV arī pārsūta šo informāciju kontaktpunktam – Aizsardzības ministrijai; 4. **14. panta 3. punkts** ieviests ar likumprojekta 4. panta pirmo un trešo daļu, paziņojumus par drošības incidentiem saņem CERT.LV, jo nacionāli arī valsts, pašvaldības un informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks un tiesiskais valdītājs par drošības incidentiem ziņo CERT.LV (likuma 6. panta otrā daļa); 5. **14. panta 5. punkta pirmā daļa** ieviesta ar likumprojekta 2. panta otro daļu, ņemot vērā, ka informāciju par drošības incidentiem nosūta CERT.LV, tad CERT.LV informēs citas dalībvalstis, ja incidents tās būs skāris; 6. **14. panta 5. punkta otrā daļa** ieviesta ar likumprojekta 4. panta pirmo daļu, ņemot vērā, ka informāciju par drošības incidentiem nosūta CERT.LV, tad CERT.LV informēs par pēcpasākumiem saistībā ar paziņojumu; 7. **14. panta 5. punkta trešā daļa** ieviesta ar likumprojekta 3. pantu, ņemot vērā, ka ziņojumus par drošības incidentiem saņem CERT.LV, tad CERT.LV pieprasa kontaktpunktam – Aizsardzības ministrijai – pārsūtīt šo informāciju citiem kontaktpunktiem; 8. **14. panta 6. punkts** ieviests ar likumprojekta 4. panta pirmo daļu, ņemot vērā, ka ziņojumus par drošības incidentiem saņem CERT.LV, tad CERT.LV, ja nepieciešams, var informēt sabiedrību. Nacionāli jau iepriekš CERT.LV bija noteiktas šādas tiesības attiecībā uz elektronisko sakaru komersantiem (likuma 6. panta ceturtā daļa); 9. **15. panta 3. punkts** ieviests ar esošā likuma 6. panta otrās daļas 4. punktu, NIS direktīvas 15. pantā minētie pienākumi un tiesības nacionāli ir uzlikti CERT.LV. Ņemot vērā, ka CERT.LV saņem informāciju par drošības incidentiem un ir informēta par drošības prasību ievērošanu, saistošu norādījumu izdošana ir veids, kā CERT.LV veic tai likumā noteiktos uzdevumus; 10. **16. panta 3. punkts** ieviests ar likumprojekta 4. panta pirmo un trešo daļu – paziņojumus par drošības incidentiem saņem CERT.LV, jo nacionāli arī valsts, pašvaldības un informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks un tiesiskais valdītājs par drošības incidentiem ziņo CERT.LV (likuma 6. panta otrā daļa); 11. **16. panta 6. punkts** ieviests ar likumprojekta 2. panta otro daļu. Ņemot vērā, ka informāciju par drošības incidentiem nosūta CERT.LV, tad CERT.LV informēs citas dalībvalstis, ja incidents tās būs skāris; 12. **16. panta 7. punkts** ieviests ar likumprojekta 4. panta pirmo daļu. Ņemot vērā, ka ziņojumus par drošības incidentiem saņem CERT.LV, tad CERT.LV, ja nepieciešams, var informēt sabiedrību. Nacionāli jau iepriekš CERT.LV bija noteiktas šādas tiesības attiecībā uz elektronisko sakaru komersantiem (likuma 6. panta ceturtā daļa); 13. **20. panta 1. punkts** ieviests ar jau esošā likuma 6. panta trešo daļu, jo arī līdz šim jebkura privāto tiesību juridiskā persona brīvprātīgi varēja ziņot par drošības incidentu CERT.LV. | | |
| 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 | **5. panta 7. punkts** ieviests ar likumprojekta 3. pantu, kas nosaka pienākumu komitejai reizi divos gados iesniegt Eiropas Komisijai NIS direktīvā norādīto informāciju, savukārt likumprojekta 7. pants – pārejas noteikumi – norāda, ka informācija pirmo reizi jāiesniedz līdz 2018. gada 9. novembrim.  **7. panta 3. punkts** ieviests ar likumprojekta 3. pantu, kas nosaka, ka Aizsardzības ministrija informē Eiropas Komisiju par nacionālās kiberdrošības stratēģijas apstiprināšanu ne vēlāk kā trīs mēnešus pēc tās apstiprināšanas.  **10. panta 3. punkta otrā daļa** ieviesta ar likumprojekta 3. pantu, kas nosaka, ka Aizsardzības ministrija vienu reizi gadā iesniedz NIS direktīvas sadarbības grupai ziņojumu, savukārt likumprojekta 7. pants – pārejas noteikumi – norāda, ka ziņojumu pirmo reizi jāiesniedz līdz 2018. gada 9. augustam. | | |
| 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 | Likumprojekts tika publicēts tīmekļa vietnē *[www.mod.gov.lv](http://www.mod.gov.lv)* sadaļā „Sabiedrības līdzdalība”. |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Likumprojekts tika publicēts tīmekļa vietnē *[www.mod.gov.lv](http://www.mod.gov.lv)* sadaļā „Sabiedrības līdzdalība”. |
| 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, CERT.LV, komiteja, nozari uzraugošās ministrijas. |
| 2. | Projekta izpildes ietekme uz pārvaldes funkcijām un institucionālo struktūru. Jaunu institūciju izveide, esošu institūciju likvidācija vai reorganizācija, to ietekme uz institūcijas cilvēkresursiem | Jaunas institūcijas netiek veidotas, netiek likvidētas un reorganizētas esošās institūcijas   1. **Tiek paplašināti CERT.LV uzdevumi**, ņemot vērā, ka ar likumprojektu tiek noteikts, ka pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji ziņos CERT.LV par drošības incidentiem, kuri ir skāruši viņu informācijas tehnoloģiju sistēmas (likumprojekta 4. panta pirmā daļa), un CERT.LV uzraudzīs, kā pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji ievēro to informācijas tehnoloģiju drošības prasības (likumprojekta 5. pants), turklāt CERT.LV tiek paplašinātas funkcijas – saņemto informāciju jānodod Aizsardzības ministrijai, citu dalībvalstu kompetentajām iestādēm, komitejai, kā arī jāsadarbojas ar Eiropas CSIRT tīklu (likumprojekta 2. panta otrā daļa). CERT.LV jaunos uzdevumus veiks esošo cilvēkresursu ietvaros. 2. **Tiek paplašināti Aizsardzības ministrijas uzdevumi**. Aizsardzības ministrija NIS direktīvas izpratnē tiek uzskatīta par kontaktpunktu, un tai tiek noteikts uzdevums sadarboties ar citu dalībvalstu kontaktpunktiem, NIS direktīvas sadarbības grupu (likumprojekta 3. pants) un izstrādāt nacionālās kiberdrošības stratēģiju, un informēt Eiropas Komisiju par tās apstiprināšanu (likumprojekta 6. pants). Aizsardzības ministrija minētos uzdevumus veiks esošo cilvēkresursu ietvaros. 3. **Tiek paplašināti komitejas uzdevumi un tiesības**. Komiteja NIS direktīvas izpratnē tiek uzskatīta par kompetento iestādi, un tai tiek noteikts uzdevums sadarboties ar nozari uzraugošajām ministrijām pamatpakalpojumu sniedzēju identificēšanas procesā un sniegt informāciju Eiropas Komisijai par identificēšanas procesiem Latvijā (likumprojekta 3. pants). Komitejai tiek noteiktas tiesības pieprasīt, lai pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji novērš informācijas tehnoloģiju sistēmu drošības prasību nepilnības un izpilda tiem noteikto ziņošanas pienākumu (likumprojekta 3. pants). Nepieciešamības gadījumā komitejai ir tiesības veikt lēmuma piespiedu izpildi, ja iepriekš minētās prasības netiek izpildītas (likumprojekta 3. pants). Komiteja minētos uzdevumus veiks un noteiktās tiesības realizēs esošo cilvēkresursu ietvaros. 4. **Tiek noteikts nozaru uzraugošo ministriju uzdevums** identificēt pamatpakalpojuma sniedzējus un pamatpakalpojumus. Nozaru uzraugošās ministrijas uzdevumu veiks esošo cilvēkresursu ietvaros. |
| 3. | Cita informācija | Nav. |

Aizsardzības ministrs Raimonds Bergmanis

Z. Beļavska, 67335354

[zane.belavska@mod.gov.lv](mailto:zane.belavska@mod.gov.lv)

S.Žogota, 67335353

Sanita.Zogota@mod.gov.lv