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)	Papildināt Ministru kabineta 2015. gada 28. jūlija noteikumus Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" ar papildu nosacījumiem, kas ir jāievēro valsts un pašvaldību institūcijām, kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem un pamatpakalpojuma sniedzējiem un digitālā pakalpojuma sniedzējiem, iepērkot informācijas un komunikācijas tehnoloģiju sistēmu produktus un pakalpojumus.

I. Tiesību akta projekta izstrādes nepieciešamība		
1.	Pamatojums	Ministru kabineta noteikumu projekts "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) sagatavots pēc Aizsardzības ministrijas iniciatīvas, ņemot vērā Nacionālās informācijas tehnoloģiju drošības padomes 2019. gada 24. jūlija sēdē nolemto.
2.	Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība	Pašlaik valsts un pašvaldību institūcijām uzsākot iepirkuma procedūru par informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) produktu un pakalpojumu iepirkšanu ir jāņem vērā Publisko iepirkumu likumā vai IKT produktu un pakalpojumu iepirkumiem, kuri saistīti ar aizsardzības nozari – Aizsardzības un drošības jomas iepirkumu likumā noteiktās prasības. Šie likumi nosaka vispārīgas prasības veicamajiem publiskajiem iepirkumiem, lai nodrošinātu to atklātumu, piegādātāju brīvu konkurenci, vienlīdzīgu un taisnīgu attieksmi pret tiem, kā arī, nodrošinātu, ka pasūtītāja līdzekļi tiek efektīvi izmantoti. Tomēr savas specifikas un augsto drošības risku dēļ IKT ir nepieciešams noteikt detalizētas prasības IKT produktu un pakalpojumu iepirkšanai, lai nodrošinātu pēc iespējas augstāku drošības līmeni. Šīs prasības pašlaik ir ietvertas vairākos normatīvajos aktos. Galvenais kiberdrošības jomu regulējošais tiesību akts ir Informācijas tehnoloģiju drošības likums

		(turpmāk – IT drošības likums). Tā mērķis ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas šīs tehnoloģijas. Likuma normas par drošības prasībām ir jāpiemēro ne tikai valsts un pašvaldību institūcijām, bet arī informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem, kā arī pamatpakalpojuma un digitālā pakalpojuma sniedzējiem. Uz IT drošības likuma 8. panta piektās un sestās daļas izdotie Ministru kabineta 2015. gada 28. jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (turpmāk – MK noteikumi Nr. 442) nosaka vienotus standartus valsts un pašvaldību institūcijām, informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem, kā arī privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, IKT drošības jomā, lai nodrošinātu vienādi augstu drošības līmeni visās valsts un pašvaldību institūciju IKT sistēmās. Noteikumos ir iekļautas arī atsevišķas prasības publiskajiem iepirkumiem un iepirkumu līgumiem, īpaši pievēršoties prasībām, kuras jāievēro attiecībā uz paaugstinātas drošības informācijas sistēmām. Tā, piemēram, valsts un pašvaldību institūcijām, pasūtot ārējās drošības pārbaudi paaugstinātas drošības sistēmai, obligāta prasība ir, ka uzņēmums, kurš veic auditu ir reģistrēts Eiropas Savienības (turpmāk – ES), Ziemeļatlantijas Līguma organizācija (turpmāk – NATO) vai Eiropas Ekonomikas zonas (turpmāk – EEZ) dalībvalstī. Tomēr pašreizējā MK noteikumu Nr. 442 redakcija vairs nespēj pilnībā nodrošināt un garantēt to, ka valsts un pašvaldību institūcijas iegādājas pietiekami drošus produktus un pakalpojumus. Tas lielā mērā saistīts ar faktu, ka pēdējo gadu laikā pasaules valstu politiskajā dienaskārtībā ir nonākuši vairāki būtiski ar IKT drošību saistīti jautājumi, tajā skaitā, tirgū esošu ražotāju piedāvāto IKT ierīču un programmatūru lietošanas iespējamie draudi ne tikai institūciju iekšējām IKT sistēmām, bet arī valstu drošībai. Šie notikumi pierāda to, ka ar IKT saistītie drošības riski pieaug, kā arī tie kļūst sarežģītāki un grūtāk atpazīstami. Tādēļ aizvien aktuālāks kļūst jautājums par valsts un pašvaldību institūciju spējām nodrošināt savā pārziņā esošo IKT drošību, tajā skaitā, uzsākot iepirkuma procedūru, nodrošināt pēc iespējas detalizētāku un precīzāku iepirkuma procedūras

		dokumentāciju un līgumu sastādīšanu, lai pretendenti un to piedāvātie produkti atbilstu drošības prasībām un radītu pēc iespējas mazāku apdraudējumu. Tādā veidā jau savlaicīgi novēršot pēc iespējas vairāk potenciālo risku, kas varētu negatīvi ietekmēt IKT drošību. Pašreizējais tiesiskais regulējums jau ietver būtiskas prasības, kuru ievērošana spēj nodrošināt institūciju IKT drošību augstā līmenī. Tomēr IKT joma attīstās ļoti strauji un, ņemot vērā jau minēto drošības risku pieaugumu, ir nepieciešamas papildu prasības, kuras valsts un pašvaldību institūcijām būtu jāņem vērā, lai izvērtētu IKT iepirkumu pretendentus, tajā skaitā, sniedzot priekšroku ne tikai finansiāli visizdevīgākajam piedāvājumam, bet tam, kurš spēj pierādīt visaugstākās drošības prasības. Tāpēc grozījumi MK noteikumos Nr. 442 paredz**:** 1. Prasību valsts un pašvaldību institūcijām datus glabāt ES vai EEZ dalībvalstī, kā arī interneta datu plūsmu virzīt ES un EEZ teritorijas ietvaros, ja datu apmaiņa notiek šajā teritorijā. Šāda prasība nodrošinās stingrākas prasības dažādu ierobežotas pieejamības datu privātumam, t.sk. fizisko personu datiem. Kā arī ierobežos iespēju informācijas pārtveršanai un nesankcionētai izmantošanai. 2. Prasību valsts un pašvaldību institūcijas vadītājam noteikt atbildīgo personu, kura uzrauga sistēmu izstrādi, ieviešanu un uzturēšanas pakalpojuma līguma izpildi. Atbildīgās personas noteikšana līguma izpildes uzraudzībai izriet no labas pārvaldības prakses informācijas tehnoloģiju pārvaldībā. Papildu uzraudzība garantēs atbilstošu līgumā noteikto prasību izpildi. 3. Papildu prasības institūcijai, ja tā slēdz ārpakalpojuma līgumu sistēmas uzturēšanai. Piemēram, līgumā ir jānosaka, ka ir nekavējoties jāziņo par drošības incidentu, pienākumu informēt par apakšuzņēmējiem un veicamās drošības pārbaudes. Prasība nodrošinās, ka pasūtītājs jau laikus ir informēts par riskiem, kas saistīti ar IKT produktu un pakalpojuma drošību, kā arī izvērtējot riskus, tiks noteiktas veicamās drošības pārbaudes, lai izvairītos no potenciālajiem riskiem. 4. Prasības valsts un pašvaldību institūcijām, iegādājoties pamata drošības sistēmām tādas

		kritiskās komponentes kā maršrutētājus, komutatorus, ārējos ugunsmūrus, ielaušanās atklāšanas sistēmas, pretielaušanās sistēmas, antivīrusu programmatūru, kā arī pakalpojumus, programmatūru vai iekārtas, kas nodrošina institūcijai aizsardzības un uzraudzības funkcijas. Attiecībā uz šīm pamata drošības sistēmu IKT komponentēm, valsts un pašvaldību institūcijām ir jāievēro vēl papildu prasības, kas noteiktas 36.[1] punktā kā prasības paaugstinātas drošības sistēmām. Tas paredz, ka līgumu par pakalpojumu, programmatūru vai iekārtu iegādi atļauts slēgt tikai ar juridisku personu, kas ir reģistrēta NATO, ES vai EEZ dalībvalstī un šīs juridiskās personas patiesā labuma guvējs (Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma, un proliferācijas finansēšanas novēršanas likuma izpratnē) ir NATO, ES, EEZ valsts pilsonis vai Latvijas Republikas nepilsonis vai fizisku personu, kas ir Latvijas Republikas valstspiederīgais, NATO, ES vai EEZ valsts pilsonis. **Attiecībā uz paaugstinātas drošības sistēmām, grozījumi paredz papildināt MK noteikumus Nr. 442, nosakot papildu prasības institūcijām**, slēdzot ārpakalpojuma līgumu un līgumu par pakalpojumu, programmatūru vai iekārtu iegādi – identificēt uzņēmuma, ar kuru plānots slēgt līgumu, patiesā labuma guvēju un lai tas ir ES, NATO vai EEZ dalībvalstu pilsonis vai Latvijas nepilsonis. Ņemot vērā, ka drošības prasībām atbilstošus IKT produktus var piedāvāt arī juridiskas un fiziskas personas no valstīm ārpus ES, NATO un EEZ teritorijas, tad noteikumu projektā ir iekļauts punkts par izņēmumiem attiecībā uz līgumu slēgšanu, ja ir saņemts kompetentās valsts drošības iestādes saskaņojums. Tas ir, kompetentā valsts drošības iestāde ir izvērtējusi konkrēto iepirkuma gadījumu un iespējamos drošības riskus un devusi savu slēdzienu vai ir pietiekami droši slēgt iepirkumu ar konkrēto juridisko vai fizisko personu. **Citi grozījumi:** 1. MK noteikumu Nr. 442 10. punkts pašlaik nosaka, ka visus dokumentus, kuri minēti noteikumu 8. pantā ir jāapstiprina institūcijas vadītājam. Jaunā 10. punkta redakcija paredz, ka institūcijas vadītājam ir obligāti jāapstiprina sistēmas drošības politika (8.1. apakšpunkts), bet pārējos

		dokumentus (8.2.-8.5. apakšpunkts), piemēram, sistēmas darbības atjaunošanas plānu vai sistēmas drošības riska pārvaldības plānu, drīkstēs apstiprināt institūcijas vadītājs vai tā pilnvarota persona. Šie dokumenti, atšķirībā no sistēmas drošības politikas, ir saistīti jau ar tehniskām un detalizētākām informācijas sistēmas prasībām, kurus praksē bieži vien apstiprina par informācijas tehnoloģiju drošību atbildīgā persona institūcijā. Līdz ar to grozījumi paredz, ka šos dokumentus drīkstēs apstiprināt arī institūcijas vadītāja pilnvarota persona, piemēram, persona, kura pārvalda institūcijas IKT drošības jautājumus. 2. No MK noteikumu Nr. 442 15.12. apakšpunkta tiek svītrots vārds "visiem", lai novērstu pretrunu starp 15.12. apakšpunkta pirmo teikumu, kurā ir noteikts, ka sistēmai ir jābūt uzliktiem visiem pieejamajiem atjauninājumiem un otro teikumu, kurš savukārt nosaka, ka ir jāizvērtē to nepieciešamība jeb, citiem vārdiem sakot, tomēr nedrīkst uzstādīt pilnīgi visus pieejamos programmatūras atjauninājumus, jo var būt situācijas, kad atjauninājums nevis novērš informācijas sistēmas nepilnības, bet rada jaunus riskus. 3. Noteikumi papildināti ar papildu prasībām, kuras jāievēro institūcijām, izstrādājot drošības politiku. Noteikumi tiek papildināti ar 15.15. un 15.16. apakšpunktiem, kuri nosaka papildu prasības elektronisko adrešu sistēmām. Turpmāk kā obligāta prasība institūcijām būs jānodrošina, ka ienākošie elektroniskie ziņojumi tiek apstrādāti vismaz atbilstoši DMARC (*Domain-based Message Authentication, Reporting and Conformance*) protokola prasībām. DMARC protokols ir izstrādāts, lai nodrošinātu e-pastu autentifikāciju un primāri izvairītos no e-pastiem, kuru sūtītājam ir izveidota viltus identitāte (t.s. "*e-mail spoofing"*), līdz ar to mazinot risku, mēstuļu un pikšķerēšanas uzbrukumiem. Tāpat tiek noteikts ka institūcija, kas ir e-pasta domēna īpašnieks, publicē DMARC protokolam atbilstošu ierakstu savā domēna vārdu sistēmā (DNS), norādot striktu atteikuma politiku (p=reject), ievieš procedūru DMARC ziņojumu saņemšanai un to analīzei. Šī prasība ir nepieciešama DMARC implementēšanai. 4. Noteikumu projekts papildināts arī ar 15.17. apakšpunktu, kurš nosaka, ka institūcijai,

		izstrādājot informācijas sistēmu drošības politiku, ir jāparedz prasība datu rezerves kopiju veidošanai un atjaunošanai. Veidot datu rezerves kopijas ir būtiski, lai situācijā, kad tomēr ir noticis drošības incidents, kura rezultātā ir zaudēti dati, tos ir iespējams atgūt.
3.	Projekta izstrādē iesaistītās institūcijas un publiskas personas kapitālsabiedrības	Aizsardzības ministrija, Ārlietu ministrija, Ekonomikas ministrija, Finanšu ministrija, Iekšlietu ministrija, Izglītības un zinātnes ministrija, Kultūras ministrija, Labklājības ministrija, Satiksmes ministrija, Tieslietu ministrija, Vides aizsardzības un reģionālās attīstības ministrija, Veselības ministrija, Zemkopības ministrija, Valsts kanceleja, CERT.LV, Iepirkumu uzraudzības birojs, VAS "Latvijas Valsts radio un televīzijas centrs", Tiesu namu aģentūra, Latvijas Banka.
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: 1) Valsts un pašvaldību institūcijas un atsevišķas prasības arī informācijas tehnoloģiju kritiskās infrastruktūras īpašniekus un tiesiskos valdītājus, kā arī privāto tiesību juridiskās personas, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji un, kurām uzsākot publiskā iepirkuma procedūru par IKT produktu vai pakalpojumu iepirkšanu, būs iepirkuma specifikācijā un līgumā jāietver noteikumos izvirzītās prasības un jāvērtē pretendentu atbilstība tām. 2) Publisko iepirkumu pretendentus jeb IKT produktu un pakalpojumu sniedzējus, kuriem ir jāatbilst MK noteikumos Nr. 442 minētajām prasībām, lai pretendētu uz iepirkuma līguma slēgšanu par savu piedāvāto produktu vai pakalpojumu.
2.	Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu	Noteikumu projektā ietvertās prasības palielinās to IKT uzņēmumu izdevumus un pienākumus, kuru produkti un pakalpojumu neatbildīs noteikumu projektā minētajām prasībām, bet, kuri vēlēsies savu produkciju un pakalpojumus sniegt valsts un pašvaldību institūcijām un virzīs savu uzņēmumu kā pretendentu ar IKT saistītā publiskajā iepirkumā. Uzņēmumiem attiecīgi vajadzēs ieviest un nodrošināt augstākas drošības prasības saviem produktiem un

		pakalpojumiem, kas var prasīt papildu finanšu kā arī cilvēkresursus. Administratīvais slogs nemainās. Sabiedrības grupām un institūcijām noteikumu projekta tiesiskais regulējums nemaina tiesības un pienākumus, kā arī veicamās darbības.
3.	Administratīvo izmaksu monetārs novērtējums	Noteikumu projektam nav ietekmes uz administratīvajām izmaksām.
4.	Atbilstības izmaksu monetārs novērtējums	Paredzams, ka izmaksas veidos 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.
5.	Cita informācija	Nav

III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem
Projekts šo jomu neskar.

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

V. Tiesību akta projekta atbilstība Latvijas Republikas starptautiskajām saistībām
Projekts šo jomu neskar.

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" 13. punktu, 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 noteikumu projektu un dotu iespēju izteikt viedokli, projekts pirms tā iesniegšanas Valsts sekretāru sanāksmē, 2020. gada 17. janvārī tika ievietots Aizsardzības ministrijas tīmekļa vietnes sadaļā "Sabiedrības līdzdalība".
3.	Sabiedrības līdzdalības rezultāti	
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	Ministru kabineta 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

Ministru prezidenta biedrs,
aizsardzības ministrs A. Pabriks

Vīza:
Aizsardzības ministrijas valsts sekretārs J. Garisons