



**Nacionālais
kibersdrošības
centrs**

<https://cyber.gov.lv>, NIS2@mod.gov.lv, 67335131

BIEŽĀK UZDOTIE JAUTĀJUMI PAR ĀRPAKALPOJUMU PRASĪBĀM

saistībā ar Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397

“Minimālās kibersdrošības prasības” 4. nodaļu



1. *Vai prasības attiecībā uz ārpakalpojumiem attiecināmas uz pilnīgi visiem ārpakalpojuma līgumiem? Teorētiski scenārijus attiecībā uz kiberincidentu draudiem var piemēklēt jebkuram ārpakalpojuma līgumam.*

Saskaņā ar MK noteikumu Nr. 397 2.3. punktu par ārpakalpojumu tiek uzskatīta jebkura veida vienošanās starp subjektu un pakalpojuma sniedzēju IKT jomā, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu, veic tehnisko resursu piegādi vai veic citu darbību subjekta uzdevumā IKT infrastruktūrā. MK noteikumos Nr. 397 ietvertās prasības attiecas uz būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem. Ja ir ārpakalpojums, ir jāslēdz ārpakalpojuma līgums un nepieciešams ievērot MK noteikumos Nr. 397 ietvertās prasības ārpakalpojuma sniedzējam.

2. *Vai MK noteikumu Nr. 397 4. nodaļas (Ārpakalpojumu prasības) piemērojamas arī jau noslēgtiem līgumiem? Piemēram, ar dažādu piegāžu laiku; VV ietvaros slēdzamiem līgumiem; EIS iegādēm?*

Jāņem vērā, ka gadījumā, ja noslēgta vispārīgā vienošanās, kurā par katru jaunu darba uzdevumu tiek slēgts jauns ārpakalpojuma līgums, uz to attieksies MK noteikumu Nr. 397 4. nodaļā ietvertās prasības. Vienlaikus norādām, ka attiecībā uz jau noslēgtiem līgumiem, kuri ir noslēgti pirms MK noteikumu Nr. 397 pieņemšanas, aicinām iepazīties ar noteikumu [noslēguma jautājumu sadalu](#), kurā ir skaidrots pārejas posms un nosacījumi.

3. *Kādas ir minimālās darbības, kas jāveic, lai nodrošinātu atbilstību kiberdrošības prasībām jau noslēgtajiem līgumiem ar ārpakalpojumu sniedzējiem?*

MK noteikumu Nr. 397 153. punkts noteic, ka ārpakalpojumu līgumi, kas noslēgti pirms šo noteikumu stāšanās spēkā un neatbilst šajos noteikumos noteiktajām ārpakalpojumu prasībām, var palikt spēkā līdz pilnīgai saistību izpildei, bet ne ilgāk kā piecus gadus no konkrētā ārpakalpojuma līguma noslēgšanas dienas. Piecu gadu ierobežojums ir skaitāms no sākotnējā līguma noslēgšanas brīža. Gadījumos, kad ārpakalpojuma līguma saistības ir izpildītas vai kopš ārpakalpojuma noslēgšanas dienas ir pagājuši pieci gadi, un ja ārpakalpojuma līgums neatbilst MK noteikumos noteiktajām ārpakalpojumu prasībām, uzskatāms, ka ārpakalpojuma līgums vairs nevar palikt spēkā.

MK noteikumu 153. punkts konkrēti noteic, ka ārpakalpojuma līgums var palikt spēkā ne ilgāk kā piecus gadus no konkrētā ārpakalpojuma noslēgšanas dienas, nevis no MK noteikumu spēkā stāšanās brīža, vai no līguma ikgadējā pagarinājuma brīža.

4. *Precēs ražotāja un piegādātāja atbilstība MK not. Nr. 397 "Minimālās kiberdrošības prasības" (tiem Pircējiem, kuri atbilst šo noteikumu 1.1. punkta prasībām) 1) 86. punktam; 2) 86. un 94. punktam?*

Skaidrojam, ka MK noteikumi Nr. 397 attiecas uz Nacionālās kiberdrošības likuma (turpmāk – NKDL) 3. pantā definēto subjektu loku. Attiecīgi, katram NKDL subjektam, slēdzot ārpakalpojuma līgumu, ir jāievēro MK noteikumu Nr. 397 4. nodaļā ietvertais regulējums attiecībā uz ārpakalpojumu prasībām. MK noteikumu Nr. 397 4.1. apakšnodaļā ietvertas vispārīgās prasības, kas attiecas uz visiem subjektiem, savukārt, 4.2. apakšnodaļā ietvertas īpašās prasības attiecībā uz IKT KI un 4.3. apakšnodaļā ietvertas prasības, kas attiecas uz būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

5. *Kā praktiski pārbaudīt ārpakalpojuma sniedzēja, tā īpašnieku, apakšuzņēmēju un patiesā labuma guvēju atbildību valstiskās piederības, reputācijas un drošības prasībām, īpaši, ja ķēde ir gara vai starptautiska?*

Gadījumā, ja subjekts ir būtisko pakalpojumu sniedzējs, attiecībā uz tehnisko resursu kritisko infrastruktūru, subjekts pārbauda noskaidrojamu informāciju, kas tam ir publiski pieejama, izmantojot subjektam vispārpieejamus līdzekļus un metodes. Gadījumā, ja rodas aizdomas par iespējamu neatbilstību prasībām, subjekts nosūta atzinuma pieprasījuma veidlapu SAB, kurā apraksta konstatēto/potenciālo neatbilstību, par ko SAB sniegs savu atzinumu saskaņā ar MK noteikumu Nr. 397 4.2. apakšnodalā noteikto kārtību. Vienlaikus skaidrojam, ka attiecībā uz IKT KI subjekts pats nepārbauda ārpakalpojuma sniedzēju, jo saskaņā ar MK noteikumu Nr. 397 IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai atļauts slēgt tikai pēc SAB atzinuma saņemšanas un SAB veic attiecīgas pārbaudes.

6. *Ja, iegādājoties programmatūru, tiks piegādāta tikai programmatūras uzstādīšanas atslēga, vai šajā gadījumā piegādātājs ir jāuzskata kā pakalpojumu sniedzējs un jāpārbauda SAB atbilstoši MK noteikumiem Nr. 397, vai arī ir jāpārbauda tikai programmatūra atbilstoši minētajiem noteikumiem? Ja esošai programmatūrai katru gadu tiek iegādāts lietošanas pagarinājums (licences atslēga), vai programmatūra ir atkārtoti jāpārbauda SAB? Vai arī licences pagarināšanai nav nepieciešams saņemt saskaņojumu no SAB?*

Iegādājoties programmatūru, tās atbilstību MK noteikumu Nr. 397 prasībām ir jāpārbauda atbilstoši prasībām par IKT resursa iegādi, kas ietvertas MK noteikumu Nr. 397 86. punktā (vispārīgās prasības), 94. punktā (īpašās ārpakalpojumu prasības IKT KI) un 101. punktā (īpašās ārpakalpojumu prasības būtisko pakalpojumu sniedzējiem). Skaidrojam, ka saņemot programmatūras uzstādīšanas atslēgu, līdzīgi, kā iegādājoties programmatūras licenci, nav nepieciešams atzinums no SAB, ņemot vērā, ka programmatūras atslēga un licence ir programmatūras iegādes sastāvdaļa, lai programmatūru varētu izmantot.

7. *Atbilstoši MK noteikumu Nr. 397 87. punktam – iegādājoties ārpakalpojumu, subjekts: 87.2. sniedz norādes uz Nacionālās kiberdrošības likumā un šajos noteikumos noteiktajām prasībām – Uz kurām no Nacionālās kiberdrošības likumā noteiktajām prasībām norādes būtu jāsniedz?*

Attiecīgā noteikumu punkta nozīme ir, ka katrs subjekts ārpakalpojuma līgumā iekļauj to informāciju, kuru saskaņā ar NKDL vai MK noteikumiem Nr. 397 nepieciešams saņemt no pakalpojumu sniedzēja, piemēram, iesniegt informāciju par izmaiņām personālā, ārpakalpojuma sniedzēja pienākumu subjektam ziņot par konstatētiem kiberincidentiem atbilstoši MK noteikumiem Nr. 397, informēt subjektu par apakšuzņēmējiem, ievērot konfidencialitātes saistības u.tml.

8. *MK noteikumu Nr. 397 88.3. punkts paredz, ka A un B konfidencialitātes klases informācijas sistēmu: 88.3.1. testa vidē tiek izmantoti tikai sintētiski dati. Kā šādā situācijā ar sintētiskiem datiem testa vidēs nodrošināt ārējo trešo pušu sistēmu integrāciju pārbaudes, ja ārējās sistēmas strādā ar reāliem personu datiem (piemēram, SmartID demo, u.c.)?*

Skaidrojam, ka, lai testa vidē ar sintētiskiem datiem nodrošinātu ārējo trešo pušu sistēmu integrācijas pārbaudi gadījumos, kad ārējās sistēmas strādā ar reāliem personu datiem, ir jāievēro MK noteikumu Nr. 397 88.3.1. un 88.3.2. apakšpunktā noteiktais. Proti, subjekts paredz, ka A un B konfidencialitātes klases informācijas sistēmu testa vidē tiek izmantoti tikai sintētiski dati, kā arī ārpakalpojuma līguma izpilde netiek veikta attiecīgās informācijas sistēmas produkcijas vidē. Līdz ar to ir nepieciešams izmantot mākslīgi ģenerētus, sintētiskus datus.

9. Vai MK noteikumu Nr.397 88.3.2. punkta vārdi "ārpakalpojuma līguma izpilde netiek veikta produkcijas vidē" un apakšpunkta mērķis bijis nodrošināt, ka ārpakalpojuma sniedzējs nemaz vispār netiek pie produkcijas vides? Respektīvi, vai drīkst pieļaut situāciju, ka ārpakalpojuma sniedzējs vismaz piegādi veic produkcijas vidē?

Saskaņā ar MK noteikumu Nr. 397 88.3.1. apakšpunktā noteikto, slēdzot ārpakalpojuma līgumu par jaunas informācijas sistēmas izstrādi vai esošās informācijas sistēmas izmaiņām, subjekts paredz, ka A un B konfidencialitātes klases informācijas sistēmu testa vidē tiek izmantoti tikai sintētiski dati (no sākotnējiem datiem izveidoti mākslīgi dati, kas attēlo sākotnējo datu īpašības un struktūru un, veicot vienu un to pašu datu analīzi, sniedz līdzvērtīgus rezultātus), savukārt, noteikumu 88.3.2. apakšpunkts nosaka, ka ārpakalpojuma līguma izpilde netiek veikta attiecīgās informācijas sistēmas produkcijas vidē. Tādējādi tiek īstenots mērķis ārpakalpojuma sniedzējam nepiešķirt piekļuvi A un B konfidencialitātes klases informācijas sistēmu produkcijas videi.

10. Kā pirms ārpakalpojuma iegādes apzināt un novērtēt piegādes ķēdes drošības riskus, kā arī izstrādāt ārpakalpojuma izbeigšanas stratēģiju, ja nav vienotas metodikas un piemēru?

Skaidrojam, ka MK noteikumi Nr. 397 nav instrukcija, līdz ar to nav iespējams paredzēt un aprakstīt visus iespējamās scenārijus. Subjektiem tiek piešķirta rīcības brīvība izvēlēties un pašiem noteikt, kā noteikumos ietvertās prasības tiek praktiski piemērotas katrā attiecīgā gadījumā, ievērojot mērķi uzlabot informācijas un komunikācijas tehnoloģiju drošību. Saskaņā ar MK noteikumu Nr. 397 89. punktā noteikto subjekta pienākums ir pārbaudīt minētajā punktā norādīto informāciju tiktāl, ciktāl subjektam ir iespējams pārbaudīt noskaidrojamu informāciju, kas tam ir publiski pieejama, lai pārliecinātos, piemēram, par to, ka piegādes ķēde ir droša un pakalpojuma sniegšanā vai IKT resursu iegādē nav saskatāmi drošības riski. MK noteikumu attiecīgais punkts paredz ietvaru tam, kas no subjekta puses ir jāpārbauda, bet pārbaudes veidu un detalizāciju subjekts nosaka pats, piemēram, iekļaujot ārpakalpojuma līgumā ārpakalpojuma izbeigšanas stratēģiju.

11. Kādos gadījumos ir jāpieprasa ārpakalpojuma sniedzējiem darbinieku saraksts un izmaiņas darbiniekos? Piemēram, ja mēs izmantojam Office 365 mākoņpakalpojumus, mums no Microsoft ir jāieprasa kāda informācija? Vai, ja TET nodrošina interneta pieslēgumu vai LMT – mobilo sakarus un datu pārraidi, mums ir jāpieprasa kāda informācija?

Skaidrojam, ka ārpakalpojuma izpildē iesaistīto darbinieku saraksts ar skaidrojumu attiecīgās fiziskās personas iesaistei ārpakalpojuma līguma izpildē būtu jāpieprasa gadījumos, ja, piemēram, tiek veikti uzturēšanas pakalpojumi ar piekļuvi subjekta sistēmām vai ja tiek veikta fizisko serveru apkope, jo tiek nodrošināta pieeja IKT fiziskai infrastruktūrai, un tāpēc arī ir nepieciešams nodrošināt piekļuves kontroli. Arī nodrošinot datu apstrādes ārpakalpojumus (piemēram, grāmatvedība, klientu atbalsts u.c.) būtu jāpieprasa darbinieku saraksts, jo, ņemot vērā piekļuves iespējas personas datiem, ir iespējama arī datu noplūde.

Vienlaikus, attiecībā uz mākoņpakalpojumiem bez konkrētu darbinieku piesaistes, darbinieku saraksts nav nepieciešams, ņemot vērā to, ka līgums/DPA (Datu apstrādes līgums (*Data Protection Addendum*)) nodrošina atbilstību.

Attiecībā uz minētajiem piemēriem par interneta pieslēgumu vai mobilajiem sakariem, skaidrojam, ka tas ir infrastruktūras pakalpojums un nav nepieciešams pieprasīt darbinieku sarakstu, ja vien nav līgumiski noteikts, ka pakalpojuma sniedzējs veic attālinātu sistēmu administrēšanu vai datu apstrādi. Līgumā iespējams būtu jāparedz kādos gadījumos un cik bieži pakalpojuma sniedzējs sniedz informāciju par piekļuvi saistītajiem darbiniekiem, kā arī pieprasīt informāciju tikai par tiem, kam ir reāla piekļuve sistēmām vai datiem.

12. *Vai kiberdrošības prasības attiecas arī uz grāmatvedības ārpakalpojumu sniedzējiem un finanšu sistēmām (ERP, e-rēķinu platformām)?*

Minimālās kiberdrošības prasības attiecas arī uz grāmatvedības ārpakalpojumu sniedzējiem un finanšu sistēmām, ja minētajiem ārpakalpojumu sniedzējiem ir informācijas sistēmas. Piemēram, grāmatvedības ārpakalpojumu sniedzēji var piekļūt personas datiem (darbinieku vārdi, uzvārdi, personas kodi, algas utt.) un finanšu datiem (piemēram, konti, rēķini utt.), un piekļūstot šiem datiem, rodas risks, ka tie var tikt nopludināti vai ļaunprātīgi izmantoti.

13. *Vai ir kādi valsts noteikti drošības standarti vai sertifikāti, kas būtu jāprasa finanšu un grāmatvedības pakalpojumu sniedzējiem?*

Skaidrojam, ka jautājums par standartiem un sertifikātiem finanšu un grāmatvedības pakalpojumu sniedzējiem neskar IKT un netiek regulēts MK noteikumu Nr. 397 ietvarā, izņemot ciktāl noteikumos noteiktās minimālās kiberdrošības prasības ir piemērojamas Nacionālās kiberdrošības likuma subjektiem.

14. *Uzņēmumā, sniedzot ārpakalpojumus, tiek nodarbināti ap 800 darbinieku. Uz bojājuma novēršanu vai iekārtu (maršrutētāja, komutatora, ugunsмūra, datora, printera) apkopi pie klienta tiek norīkots pirmais brīvais eksperts. Prasība atklāt pirms līguma noslēgšanas visu 800 darbinieku vārdus, uzvārdus, kuri potenciāli varētu tikt nodarbināti pakalpojuma sniegšanā ir nesamērīgi. Vai ir pieņemams, ka konkrētais ārpakalpojumu sniedzējs savam klientam (NKDL subjektam) informāciju par aktuālo darbinieku, kurš ir norīkots konkrētā uzturēšanas vai apkopes uzdevuma izpildei, sniedz SMS vai elektroniskā pieteikumu/darba uzdevumu sistēmā (piem., Jira Service Desk).*

Jā, ir pieņemams un nepieciešams informēt par darbinieku, kurš norīkots konkrētā uzturēšanas vai apkopes uzdevuma izpildei, dokumentējot konkrēto saskaņojumu iespējamās atbilstības MK noteikumu Nr. 397 nodrošināšanai (līdz ar to, piemēram, SMS var nebūt piemērotākais risinājums personu saskaņošanai). Informējot par darbinieku, kurš norīkots uzturēšanas vai apkopes uzdevuma izpildei, iesakām vienoties ar pakalpojuma saņēmēju izmantot tādu informēšanas kanālu, kurā informēšanas fakts tiek saglabāts noteiktu laiku un ir nolasāmas būtiskās sastāvdaļas: kas, kam, kad un par ko ir sūtījis informāciju.

15. *Vai ir ieteikumi kādā veidā būtu organizējamās apmācības ārpakalpojumu sniedzēju darbiniekiem?*

Atbilstoši MK noteikumu Nr. 397 77.3. apakšpunktā noteiktajam IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs organizē ārpakalpojuma sniedzēja darbiniekiem, kas ir iesaistīti līguma izpildē, kiberdrošības instruktāžas pirms līguma izpildes uzsākšanas. Minētais noteikumu punkts ļauj subjektam pašam nolemt kādā formātā (klātienē vai attālināti, prezentācijas formā, iepazīšanās ar materiāliem un noslēgumā tests par zināšanu pārbaudi u. tml.) apmācības organizējamās. Tas pats attiecībā uz to, vai nepieciešams veikt jebkāda veida uzskaiti par veiktajām apmācībām vai instruktāžu.

16. *Kā piemērojams MK noteikumu Nr. 397 90. punkts? Vai pareizi saprotams, ka subjektam nav uzlikts pienākums nodrošināt, ka apakšuzņēmējs atbilst 4.1.nodaļā noteiktajām prasībām?*

Saskaņā ar MK noteikumu Nr. 397 89. punktu pirms ārpakalpojuma iegādes subjekts apzina un novērtē ar ārpakalpojuma iegādi saistītos drošības riskus, tostarp piegādes ķēdes drošības riskus, un nosaka ārpakalpojuma kvalitātes, drošības un pieejamības prasības minēto risku mazināšanai, kā arī ārpakalpojuma apturēšanas vai izbeigšanas stratēģiju. Subjekts un ārpakalpojuma sniedzējs ir atbildīgs arī par apakšuzņēmējiem deleģēto pakalpojumu uzraudzību un atbilstību minēto noteikumu 4.1. apakšnodaļā noteiktajām prasībām. Ņemot vērā norādīto, subjektam ir jāīsteno atbilstošs mehānisms, lai realizētu atbildību par apakšuzņēmēju atbilstību prasībām.

17. *Vai MK noteikumos Nr. 397 ir paredzēti noteikumi ārpakalpojuma sniedzējiem pakalpojumu nodrošināšanai izmantot programmatūru vai iekārtu, kuru ražotājs uz līguma noslēgšanas dienu ir reģistrēts NATO, Eiropas Savienības vai Eiropas Brīvās tirdzniecības asociācijas dalībvalstī vai NATO Indijas un Klusā okeāna reģiona sadarbības valstī, kā tas bija noteikts līdz šim spēkā esošajos noteikumos? Vai to ir jāparedz iepirkuma dokumentācijā?*

MK noteikumos Nr. 397 prasība ārpakalpojuma sniedzēja un tehniskā resursa ražotājam būt reģistrētam NATO, Eiropas Savienības vai EBTA dalībvalstī vai NATO Indijas un Klusā okeāna reģiona sadarbības valstī ir noteikta: 1) IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam, slēdzot ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi un 2) būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, slēdzot ārpakalpojuma līgumu A klases informācijas sistēmai.

Savukārt, MK noteikumu Nr.397 87.3.3. punktā noteikts, ka, iegādājoties ārpakalpojumu, subjekts paredz subjekta un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā, ārpakalpojuma sniedzēja pienākumu informēt subjektu par ārpakalpojuma sniedzēja ārpakalpojuma izpildei piesaistītu citu pakalpojuma sniedzēju (apakšuzņēmēju) un viņa atbilstību šajos noteikumos un ārpakalpojuma līgumā noteiktajām prasībām. Līdz ar to subjekts, noslēdzot ārpakalpojuma līgumu, ārpakalpojuma sniedzējam uzliek par pienākumu informēt par apakšuzņēmēju atbilstību MK noteikumiem Nr. 397 un ārpakalpojuma līgumā noteiktajām prasībām.

Vienlaikus skaidrojam, ka šādu punktu subjekts var iekļaut iepirkuma dokumentācijā, ņemot vērā aktuālos drošības riskus.

18. *MK noteikumu Nr. 397 4.1. apakšnodaļa nosaka vispārīgās ārpakalpojumu prasības, savukārt 4.2. apakšnodaļa nosaka īpašās ārpakalpojumu prasības IKT kritiskajai infrastruktūrai, līdz ar ko lūdzu skaidrot, vai, slēdzot līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai, jāievēro 4.1. apakšnodaļā noteiktās prasības. Vai visas 4.1. apakšnodaļā noteiktās prasības attiecināmas uz A klases informācijas sistēmām vai tikai tās, kuras nav noteiktas 4.2. apakšnodaļā?*

MK noteikumu Nr. 397 4.1. apakšnodaļā ir ietvertas vispārīgās ārpakalpojumu prasības, kas attiecas uz visiem subjektiem un visu klašu informācijas sistēmām, savukārt noteikumu 4.2. apakšnodaļā ietvertas īpašās ārpakalpojumu prasības IKT KI, kas ir papildu prasības MK noteikumu Nr. 397 4.1. apakšnodaļā noteiktajam un attiecas uz IKT kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju un to slēgtiem ārpakalpojuma līgumiem par pakalpojuma sniegšanu A klases informācijas sistēmai un IKT kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju un to slēgtiem ārpakalpojuma līgumiem par A klases informācijas sistēmas tehnisko resursu iegādi. Tātad uz IKT KI attieksies gan MK noteikumu Nr. 397 4.1. apakšnodaļā ietvertās prasības, gan 4.2. apakšnodaļā ietvertās prasības.

19. *Bieži pasūtītājiem, kas izmanto ārpakalpojumus, pašiem nav kompetences šajā jomā, un tie uzticas savam pakalpojumu sniedzējam un viņa pieredzei. Kādus punktus jūs ieteiktu iekļaut līgumā ar ārpakalpojumu sniedzējiem? Vai pietiek ar vispārīgo punktu, ka pakalpojumu sniedzējs visus darbus un pakalpojumus veiks, ievērojot Latvijas Republikas normatīvo aktu prasības?*

Ar vienu vispārīgu punktu, kas noteiks, ka darbi un pakalpojumi tiks veikti ievērojot LR normatīvo aktu prasības, nepietiek. Skaidrojam, ka subjektā ir jānosaka kibers drošības pārvaldnieks. Tāpat nepieciešams līgumā iekļaut tos punktus no MK noteikumiem Nr. 397, kuri attiecas uz konkrētiem pakalpojumu sniedzējiem un informācija, kas pakalpojumu sniedzējam jāsniedz, kā arī MK noteikumu Nr. 397 4. nodaļā ietvertās prasības, atkarībā no tā, kas subjekts ir pēc statusa (būtisko pakalpojumu sniedzējs, svarīgo pakalpojumu sniedzējs vai IKT KI). Turklāt norādām, ka uzticēties vien pakalpojumu sniedzējam nevar, jo subjekta pienākums saskaņā ar MK noteikumos Nr. 397 noteikto ir nodrošināt un pārbaudīt pakalpojumu sniedzēja atbilstību šo noteikumu prasībām.

20. Kā pasūtītājs var kontrolēt pakalpojumu sniedzēju jomās, kurās pašam nav kompetences? Vai pietiek līgumā atrunāt pakalpojuma sniedzēja pienākumu ziņot par incidentiem, darbības pārtraukumiem vai datu noplūdēm? Varbūt šiem ziņojumiem ir jānosaka periodiskums?

Subjekts uzrauga pakalpojumu sniedzēju caur NKDL un MK noteikumos Nr. 397 noteiktajām prasībām, saņem un sniedz attiecīgu informāciju uzraugošajām iestādēm. Vienlaikus norādām, ka subjekta pienākums saskaņā ar MK noteikumos Nr. 397 noteikto ir nodrošināt un pārbaudīt pakalpojumu sniedzēja atbilstību šo noteikumu prasībām. Ziņošanu par incidentiem var iekļaut ārpakalpojuma līgumā, proti, nosakot, ka pakalpojuma sniedzējs ziņo par incidentiem subjektam un subjekts veic visas nepieciešamās darbības attiecībā uz incidentu ziņošanu. Vienlaikus vēršam uzmanību uz MK noteikumu Nr. 397 87.3. apakšpunktā noteikto, proti, iegādājoties ārpakalpojumu, subjekts paredz subjekta un ārpakalpojuma sniedzēja tiesības un pienākumus, tostarp - ārpakalpojuma sniedzēja pienākumu nekavējoties ziņot subjektam par konstatēto kiberincidentu, ja tas ietekmē vai var ietekmēt subjekta darbību vai ārpakalpojuma sniedzēja sniegto pakalpojumu, kā arī veikt visas kiberincidenta novēršanai nepieciešamās darbības (MK noteikumu Nr. 397 87.3.2. apakšpunkts).

21. Subjektam būtu nepieciešams apzināt un uzskaitīt ārpakalpojuma sniedzējus. Vai nebūtu loģiski, ka šāda uzskaitē tiktu veikta IKT resursu un informācijas sistēmu katalogā? Pēc NKDC sniegtā skaidrojuma saprotu, ka šāds uzskaitījums nav jāietver. Kādi ir Jūsu ieteikumi, kur šādu sarakstu būtu jāiekļauj?

Subjektam nekas neliedz minēto informāciju fiksēt IKT resursu katalogā, ja tas subjektam ir būtiski kiberdrošības nodrošināšanai, bet normatīvais regulējums šādu prasību, proti, apzināt un uzskaitīt ārpakalpojumu sniedzējus, neparedz.

22. Lūdzam paskaidrot un/vai sniegt ieteikumus par korektu mākoņpakalpojumu aprakstīšanu Informācijas resursu klasifikācijas dokumentā. Kā šādā dokumentā precīzi norādīt resursa īpašnieku mākoņpakalpojuma gadījumā (piemēram, Microsoft SharePoint), ja attiecīgais resurss tiek izmantots globāli visā uzņēmumā un tam nav iespējams noteikt vienu konkrētu lomu vai amatu uzņēmuma struktūrā?

IKT resursu un informācijas sistēmu kataloga dokumentā mākoņpakalpojumu (piemēram, Microsoft SharePoint) gadījumā kā resursa īpašnieku nav nepieciešams norādīt konkrētu amatu vai personu, bet gan organizācijas līmeņa atbildīgo struktūrvienību vai funkciju, kas nodrošina pakalpojuma izmantošanas pārvaldību. Ja pakalpojumu izmanto visa organizācija, īpašnieks tiek definēts organizatoriski, nevis individuāli.

23. Kādas prasības Būtisko pakalpojumu sniedzējam būtu jānosaka pakalpojumu sniedzējiem, ar kuriem ir piegādes ķēdes, kas attiecas uz biznesa specifisku IS, IKT resursu izstrādi un piegādi? Pat ja šie uzņēmumi NAV MK noteikumu subjekti.

Būtisko pakalpojumu sniedzējam ir jānosaka vienotas kiberdrošības prasības visiem piegādes ķēdes dalībniekiem, kas iesaistīti IS un IKT resursu izstrādē vai piegādē, tostarp, MK noteikumu Nr. 397 4. nodaļā ietvertajām prasībām, kas attiecas uz ārpakalpojumiem. Tas attiecas arī uz tiem piegādes ķēdes uzņēmumiem, kas paši nav MK noteikumu Nr. 397 subjekti, jo atbildība IS un IKT resursu izstrādē vai piegādē par drošību saglabājas pie būtiskā pakalpojuma sniedzēja.

24. Vai subjektam ārpakalpojuma sniedzējam būtu jānosaka pienākums informēt subjektu par notikušajiem kiberdrošības incidentiem? Vai subjektam būtu jāinformē NKDC, ja ir noticis kiberincidents ārpakalpojuma sniegtajiem IKT resursiem? Piemēri: Horizon, Office365, E-klase, Datamed, Vienotā pašvaldības sistēma, kas izvietoti uz ārpakalpojuma sniedzēja serveriem.

Vēršam uzmanību uz MK noteikumu Nr. 397 87.3. apakšpunktā noteikto, proti – iegādājoties ārpakalpojumu, subjekts paredz subjekta un ārpakalpojuma sniedzēja tiesības un pienākumus, tostarp – ārpakalpojuma

sniedzēja pienākumu nekavējoties ziņot subjektam par konstatēto kiberincidentu, ja tas ietekmē vai var ietekmēt subjekta darbību vai ārpakalpojuma sniedzēja sniegto pakalpojumu, kā arī veikt visas kiberincidenta novēršanai nepieciešamās darbības (MK noteikumu Nr. 397 87.3.2. apakšpunkts).

25. *Lūdzu nosaukt konkrētus piemērus pārbaužu veidiem, kas veicamas 87.4. punkta ietvaros.*

Nacionālās kiberdrošības likumā un MK noteikumos Nr. 397 noteikto kiberdrošības organizatorisko un tehnisko pasākumu pārbaude, piemēram, cik regulāri tiek veiktas datu rezerves kopijas, žurnālu uzskaitē, atbilstoši nodrošināta piekļuves kontrole u.c. pārbaudes, kuras subjekts ir pats noteicis atbilstoši kiberdrošības politikai un kiberrisku pārvaldības un IKT darbības nepārtrauktības plānam.

26. *Kāda procedūra ir jāievēro iegādājoties jau gatavu programmatūru? Vai pats var veikt programmatūras īpašnieku izpēti pēc publiski pieejamas informācijas vai arī nepieciešams visu programmatūru saskaņot ar SAB pirms iegādes un pats nedrīkst veikt nekādu izpēti?*

Pirms ārpakalpojuma iegādes jebkuram subjektam jāapzina un jānovērtē ar ārpakalpojuma iegādi saistītos riskus, tostarp piegādes ķēdes drošības riskus, un jānosaka ārpakalpojuma kvalitātes, drošības un pieejamības prasības minēto risku mazināšanai, kā arī ārpakalpojuma izbeigšanas stratēģiju. Subjektam ir arī pienākums nodrošināt, ka pirms ārpakalpojuma līguma slēgšanas, tas tiek saskaņots ar subjekta kiberdrošības pārvaldnieku un tiek noteikta atbildīgā persona par līguma izpildes uzraudzību kiberdrošības jomā.

Ja netiek slēgts tāds ārpakalpojuma līgums, kuru nedrīkst slēgt bez SAB atzinuma saņemšanas, piemēram, ja IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, slēdz ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi, tad subjektam pašam jāpārliedz par ārpakalpojuma sniedzēja un tehniskā ražotāja atbilstību gan MK noteikumu Nr. 397 vispārīgajām ārpakalpojumu prasībām (4.1. apakšnodaļā), gan īpašajām ārpakalpojumu prasībām IKT KI (4.2. apakšnodaļā) vai īpašajām ārpakalpojumu prasībām būtisko pakalpojumu sniedzējiem (4.3. apakšnodaļā), t.sk., 94. punktam, balstoties uz publiski pieejamu informāciju.

Gadījumā, ja rodas aizdomas, ka attiecīgais tehniskais resurss varētu neatbilst prasībām un nav pašu spēkiem gūta pilnīga pārliecība par atbilstību, ir jāaizpilda un jānosūta SAB MK noteikumu Nr. 397 8. pielikumā pievienotā veidlapa tikai par tiem tehniskajiem resursiem, kas neatbilst MK noteikumu Nr. 397 94. punktā ietvertajām prasībām, norādot visu informāciju, kuru tam izdevies noskaidrot par konstatēto vai potenciālo neatbilstību.

27. *Vai MK noteikumu Nr. 397 86. punkta apakšpunktos un 94. punkta apakšpunktos noteikto subjektu pārbaudi veic IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs pastāvīgi, tas ir pats?*

MK noteikumu Nr. 397 86., 89., un 94. punkts paredz, ka subjekts patstāvīgi veic pārbaudi, un tāpēc subjekts ir atbildīgs par to, ka pārbaude tiek veikta. Vienlaikus tas nenozīmē, ka pārbaudi fiziski jāveic subjekta vadītājam vai IKT kritiskās infrastruktūras īpašniekam, vai tiesiskajam valdītājam patstāvīgi. Pārbaudes veikšanu var uzticēt citai personai, piemēram, kiberdrošības pārvaldniekam. Saskaņā ar NKDL 25. panta pirmajā daļā noteikto, subjekta kiberdrošības pārvaldību nodrošina un par to atbild subjekta vadītājs. Katra subjekta vadītājs nosaka atbildīgo personu, kura īsteno un pārbauda kiberdrošības pasākumu īstenošanu attiecīgajā subjektā, jeb kiberdrošības pārvaldnieku Attiecīgi, arī MK noteikumu NR. 397 92. punkts paredz, ka pirms ārpakalpojuma līguma slēgšanas tas tiek saskaņots ar kiberdrošības pārvaldnieku un ir jānosaka atbildīgo personu par līguma izpildes uzraudzību kiberdrošības jomā.

MK noteikumu Nr. 397 86. punkts nosaka vispārīgās prasības, kas attiecas uz visiem subjektiem un paredz, ka subjekts ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi nedrīkst slēgt gadījumā, ja izpildās kāds

no 86. punktā ietvertajiem kritērijiem (attiecībā uz B un C klases informācijas sistēmas tehnisko resursu iegādi). Savukārt saskaņā ar MK noteikumu Nr. 397 94. punktā noteikto, IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi atļauts slēgt, ja ārpakalpojuma sniedzējs un tehniskā resursa ražotājs atbilst noteikumu 94. punktā ietvertajiem kritērijiem. Gadījumā, ja ārpakalpojuma sniedzējs neatbilst 94. punktā ietvertajām prasībām vai, ja ir radušās aizdomas, ka tas varētu neatbilst minētajām prasībām, IKT KI īpašnieks vai tiesiskais valdītājs nosūta SAB elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu atzinuma pieprasījuma veidlapu (pieejama MK noteikumu Nr. 397 8. pielikumā). Norādītā veidlapa aizpildāma tikai par tiem tehniskajiem resursiem, kas neatbilst MK noteikumu Nr. 397 94. punktā ietvertajām prasībām.

28. Vai nav plānots mīkstināt prasības attiecībā uz IKT kritiskās infrastruktūras ārpakalpojumu līgumu saskaņošanu ar Satversmes aizsardzības biroju, paredzot saskaņošanas derīguma termiņu (piemēram, uz noteiktu laiku vai konkrētām personām)? Pašreizējā kārtība paredz atkārtotu vienu un tā paša uzņēmuma un personu pārbaudi katram līgumam, kas būtiski palielina administratīvo slogu un pagarina procesu, pat ja pārbaude veikta nesen un apstākļi nav mainījušies.

Skaidrojam, ka saskaņā ar Ministru kabineta noteikumu Nr. 397 93. punktu IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai ir atļauts slēgt tikai pēc SAB atzinuma saņemšanas. Minētā prasība ir pamatota ar drošības apsvērumiem, proti, lai katrā konkrētajā sadarbības gadījumā identificētu iespējamās aktuālos drošības riskus un izvērtētu atbilstību normatīvajos aktos noteiktajām prasībām. Pat ja uzņēmums vai pakalpojumā iesaistītās personas jau iepriekš ir bijušas pārbaudītas un SAB atzinums ir saņemts, apstākļi var mainīties, piemēram, uzņēmuma īpašnieku struktūra, iesaistīto personu sastāvs, drošības incidenti vai citi būtiski riski. Drošības risku izvērtējums tiek veikts saistībā ar konkrēto pakalpojumu un sadarbības ietvaru, tādēļ to nav iespējams vispārināt uz noteiktu termiņu vai attiecināt uz personām neatkarīgi no konkrētā līguma. Līdz ar to saskaņā ar šobrīd spēkā esošo regulējumu SAB atzinums ir jāsaņem katrā gadījumā pirms attiecīgā ārpakalpojuma līguma slēgšanas, arī tad, ja pakalpojuma sniedzējs vai iesaistītās personas jau iepriekš ir tikušas pārbaudītas.

29. Vai subjektam ir tiesības prasīt un pārbaudīt MK noteikumu Nr. 397 91. punktā norādīto fizisko personu pases (personu identifikācijas dokumentus), lai pārliecinātos, ka šīs personas nav MK 86.1. punktā norādītajās valstīs reģistrētas un ir reģistrētas MK 94. punktā norādītajās valstīs? Vai to pieļauj Fizisko personu datu aizsardzības likums?

Subjekts pārbauda noskaidrojamu informāciju, kas tam ir publiski pieejama tiktāl, ciktāl tas ir iespējams. Gadījumā, ja rodas aizdomas par iespējamu neatbilstību prasībām, subjekts nosūta atzinuma pieprasījuma veidlapu (pievienota MK noteikumu Nr. 397 8. pielikumā) SAB, kurā apraksta konstatēto/iespējamo neatbilstību, par ko SAB sniegs savu atzinumu.

30. Kur Subjektam iegūt informāciju par ārpakalpojuma sniedzēja amatpersonām, fiziskām personām, kas iesaistītas ārpakalpojuma sniegšanā un ir reģistrētas Krievijas Federācijā, Baltkrievijas Republikā vai valstī, kuru Eiropas Parlaments vai Latvijas Republikas Saeima ir atzinusi par terorismu atbalstošu valsti? Kā rīkoties, ja šīs personas ir dubultpilsoņi? Vai ir oficiāls saraksts ar terorismu atbalstošām valstīm?

Subjekts pārbauda noskaidrojamu informāciju, kas tam ir pieejama tiktāl, ciktāl tas ir iespējams, t.sk. no publiski pieejamām informācijas sistēmām un datu bāzēm. Gadījumā, ja rodas aizdomas par iespējamu neatbilstību prasībām, subjekts sūta atzinuma pieprasījuma veidlapu SAB, kurā apraksta konstatēto/potenciālo neatbilstību, par ko SAB sniegs savu atzinumu. Attiecībā uz jautājuma daļu par to, kur subjektam iegūt informāciju par ārpakalpojuma sniedzēja amatpersonām, fiziskām personām, kas iesaistītas ārpakalpojuma sniegšanā un ir reģistrētas Krievijas Federācijā, Baltkrievijas Republikā vai valstī, kuru Eiropas Parlaments vai Latvijas Republikas Saeima ir atzinusi par terorismu atbalstošu valsti, skaidrojam, ka subjekts var, piemēram, uzlikt par pienākumu pakalpojumu sniedzējam iesniegt par to pieejamo informāciju no Komercreģistra. Komercreģistrā ir iespējams iegūt informāciju par uzņēmuma amatpersonām (īpašnieki, valdes locekļi), patiesā labuma guvējiem.

Gadījumā, ja persona ir Krievijas vai Baltkrievijas pilsonis, un subjekts noskaidro dubultpilsonības faktu (neatkarīgi no tā, vai tā ir kā pirmā vai otrā pilsonība) un saistību ar Krievijas Federāciju, Baltkrievijas Republiku vai valsti, kuru Eiropas Parlaments vai Latvijas Republikas Saeima ir atzinusi par terorismu atbalstošu valsti, ārpakalpojumu līgumu slēgt nedrīkst.

Kā arī norādām, ka Latvijas Republikā nav izveidots oficiāls saraksts ar valstīm, kuras uzskatāmas par terorismu atbalstošām. Līdzīgi kā Igaunijā, Lietuvā un Polijā, **LR Saeima 2022. gada 11. augustā ir pieņēmusi paziņojumu, kurā Krievija tika atzīta par terorismu atbalstošu valsti.** Iesakām iepazīties ar Eiropas Komisijas publicēto un regulāri aktualizēto augsta riska trešo valstu sarakstu, kuru nelikumīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas režīmā ir stratēģiskas nepilnības. Lai uzzinātu, vai sarakstā iekļautajā valstī ir paaugstināts terorisma atbalstīšanas risks, ir iespējams iepazīties ar metodoloģiju un iemesliem, kādēļ katra valsts ir iekļauta augsta riska trešo valstu sarakstā. Augsta riska trešo valstu saraksts un metodoloģija ir pieejama Eiropas Komisijas mājaslapā: [šeit](#).

Norādām, ka īpaša uzmanība ir jāpievērš arī Eiropas Savienības sankciju mehānismiem, kas paredz sarakstu ar konkrētām personām, uzņēmumiem, grupām u.c., uz kurām attiecas ierobežojošie pasākumi (līdzekļu iesaldēšana u.c.). Šo sarakstu veido un uztur Eiropas Savienības Padome. Papildus informāciju par sankciju izpildi var atrast Finanšu izlūkošanas dienesta mājaslapā: [šeit](#).

31. Kādi priekšdarbi pasūtītājam ir jāizdara, lai komersanta un tā personāla saskaņošana SAB noritētu ātrāk kā 3 mēnešu laikā un kādu informāciju pasūtītājam ir jāpieprasa no pretendentiem (gan Latvijā, gan ārvalstīs reģistrētajiem) piedāvājumā, zinot, ka līguma slēgšanas tiesības ieguvušais pretendents būs jāpārbauda, lai saīsinātu atzinuma sniegšanas laiku?

Atbilstoši MK noteikumu Nr. 397 4.1. apakšnodaļā "Vispārīgās ārpakalpojumu prasības" noteiktajam, subjekts atbilstoši 86. punktā ietvertajām prasībām izvērtē ārpakalpojuma līguma slēgšanu par IKT resursa vai pakalpojuma iegādi. Savukārt saskaņā ar MK noteikumu Nr. 397 93. punktā noteikto, IKT KI īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai atļauts slēgt tikai pēc SAB atzinuma saņemšanas. SAB atzinumu sniedz triju mēnešu laikā, nepieciešamības gadījumā atzinuma sniegšanu var pagarināt uz vēl vienu mēnesi (3+1). Norādītais termiņš ir maksimālais termiņš, kas nepieciešams drošības iestādei, lai rūpīgi izvērtētu un pārbaudītu iesniegto informāciju, turklāt iepirkuma procedūras iespēju robežās vēlams organizēt un plānot savlaicīgi, ierēķinot to, ka atzinums no drošības iestādes būs nepieciešams.

Subjekts, pieprasot SAB atzinumu, var uzreiz norādīt informāciju, kuru tas pats ir noskaidrojis par komersantu un/vai tā personālu, vienlaikus termiņš ir tāds, kāds tas MK noteikumos Nr. 397 ir norādīts un ar norādīto termiņu ir jāērēķinās.

Pasūtītājam no pretendentiem ir jāpieprasa iespējamo noskaidrojamo informāciju, kas primāri nepieciešama MK noteikumu Nr.397 8. pielikuma aizpildīšanai. Vienlaikus norādām, ka par pretendentiem no ārvalstīm var tikt pieprasīta papildu informācija bez MK noteikumu Nr. 397 8. pielikumā noteiktās, tostarp dzimšanas datums un vieta (pilsēta, valsts), aktuālā faktiskās dzīvesvietas adrese, kā arī personu apliecinoša dokumenta veids, izdošanas iestāde, datums un numurs.

32. Vai saskaņojumam par personas pārbaudi ir derīguma termiņš? Vai, ja tiks konstatēti fakti par personu pēc pārbaudes, kas liedz dalību, saņemsim informāciju?

Norādām, ka saskaņojumam/atzinumam par personas pārbaudi derīguma termiņš nav noteikts. Vienlaikus norādām, ka drošības apsvērumu dēļ, slēdzot jaunu ārpakalpojuma līgumu pat ar jau zināmiem pakalpojuma sniedzējiem, pakalpojumu sniegšanas pretendents ir jāsaņem ar SAB. Turklāt, norādām arī, ka IKT KI tiesiskā īpašnieka vai valdītāja un paša subjekta pienākums ir pārbaudīt vai ārpakalpojuma līguma izpildē iesaistītās personas atbilst prasībām. Attiecībā uz to vai, ja tiks konstatēti fakti par personu pēc pārbaudes, kas liedz personai dalību, skaidrojam, ka attiecīgā gadījumā subjekts tiks informēts tad, kad drošības iestāde sniegs savu atzinumu.

33. Jautājums par ārpakalpojuma izpildē iesaistīto speciālistu saskaņošanu ar SAB un iespēju subjektam un SAB nonākt pie saprātīga risinājuma (atkarībā no iesaistīto pakalpojumu nozīmības, iesaistīto speciālistu lomas) nosakot kritērijus saskaņošanas biežumam? Šobrīd lielai iestādei, kur viens piegādātājs nodrošina pakalpojumu vairākos projektos, kuros tiek slēgti vairāki darba uzdevumi, vai darbi tiek iepirkti caur EIS, prasība ir saskaņot katra darba uzdevuma iesaistītos speciālistus pirms darbu uzsākšanas. Tādējādi par vairākiem speciālistiem šī gada laikā (8 mēnešos) saskaņojums prasīts un saņemts jau vairāk kā piecas reizes. Ja darba uzdevuma izpildē iesaistīti piemēram 10 speciālisti, no kuriem 8 saskaņoti iepriekš, bet 2 (piemēram testētāji) ir jauni, tad komanda nevar neko uzsākt līdz nav saņemts saskaņojums. Tas atstāj lielu iespaidu uz darbu izpildes termiņiem. Pie tam pieprasījumu sagatavošana prasa resursus gan subjekta pusē, un noteikti arī SAB pusē.

Skaidrojam, ka vispārīgās vienošanās gadījumā ir nepieciešams saskaņot komersantu un pakalpojuma sniegšanā iesaistīto personālu. Savukārt, ja tiek slēgts ārpakalpojuma līgums un līguma ietvaros paredzēti vairāki darba uzdevumi, tas nenozīmē, ka pie katra darba uzdevuma izpildes iesaistītie speciālisti ir jāsaņemo, ja vien par katru darba uzdevumu netiek slēgts jauns/atsevišķs līgums.

Taču, ja 1) IKT kritiskās infrastruktūras īpašnieks vai tiesiskajam valdītājs ir noslēdzis 93. punktā minēto ārpakalpojuma līgumu vai 2) Būtisko pakalpojumu sniedzējs, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs ir noslēdzis 101.2. apakšpunktā minēto ārpakalpojuma līgumu, tad pirms izpildē iesaistīto fizisko personu izmaiņām līguma izpildes laikā, pirms attiecīgo personu iesaistes izpildē, subjektam ir jāinformē SAB.

34. Par MK 397 8. pielikumu un pakalpojuma izpildē iesaistītajiem speciālistiem – praksē ir situācijas, kur pakalpojums būt. pak. sniedzēja sistēmām tiek daļēji nodrošināts ar attālinātu pieslēgšanos (speciālisti citā valstī, on-site atrodas neliela komanda). Lielie starptautiskie uzņēmumi algo speciālistu komandas desmitos vai simtos cilvēku, no kuriem pieslēdzas tajā brīdī brīvie/pieejamie. Kā šādā situācijā pasūtītājam iepirkuma laikā pieprasīt informāciju par pakalpojuma izpildē iesaistītajām personām, ja ņem vērā, ka pats pakalpojuma sniedzējs, iespējams, nevarēs skaidri pateikt, kuras personas tiks iesaistītas? Pieprasīt informāciju par pilnīgi visām personām, no kurām daļa tikai teorētiski varētu būt iesaistītas pakalpojuma sniegšanā nozīmētu apjomīgus sarakstus un pretendenti varētu iebilst, ka šāda prasība nav samērīga.

Šo jautājumu ieteicams skatīt no drošības prasību perspektīvas. Skaidrojam, ka subjektam jebkurā gadījumā ir jāaizpilda MK noteikumu Nr. 397 8. pielikumā pievienotā veidlapa un pašam subjektam jānodrošina drošības risku mazināšanas pasākumi, piemēram, ka attiecīgais speciālists, kas iesaistīts pakalpojuma izpildē tiks pielaists darbam tikai, ja no subjekta puses tas tiks monitorēts. Praksē šādās situācijās bieži vien darbinieku saraksts darbu veikšanai tiek iesniegts ar rezervi (lai nepieciešamības gadījumā kādu var aizstāt) un risku pārvaldības ietvaros speciālistu darbība var tikt elektroniski uzraudzīta.

35. Ja esoša līguma (slēgts 2024. gada rudenī) ietvaros līguma izpildē tiek iesaistīti papildus speciālisti, vai, sūtot šos speciālistus izvērtēšanai SAB, nepieciešams aizpildīt 8. pielikumu un pievienot papildus speciālistu piekrišanas? Vai uz šo speciālistu izvērtēšanu attiecas trīs mēnešu termiņš?

Katra iesaistītā speciālista piekrišanu nav nepieciešams sūtīt, SAB sagaida, ka subjekts sūtot atzinuma pieprasījuma veidlapu SAB, pavadvēstulē norāda, ka ir saņemta noteikumu 96.2. apakšpunktā minētā piekrišana pārbaudes veikšanai – brīvā formā, pavadvēstulē rakstiski norāda, ka piekrišana ir saņemta. Uz šo speciālistu pārbaudēm attiecas MK noteikumu Nr. 397 93. punktā noteiktais termiņš – trīs mēneši, nepieciešamības gadījumā atzinuma sniegšanu pagarinot vēl uz vienu mēnesi.

36. *Vai nerodas pretruna - no vienas puses KI neaīšē savu statusu, no otras puses ārpakalpojumu sniedzējam jāsniedz piekrišana pārbaudes veikšanai, kas jau ļauj izsecināt, ar kādu sistēmu un kāda statusa infrastruktūrā būs jāstrādā.*

Administratīvā sloga mazināšanas nolūkos, kā arī, ņemot vērā to, ka iepirkumu procedūras norit vairākās kārtās un arī pretendentu apjoms mēdz būt liels, skaidrojam, ka SAB savu saskaņojumu sniedz tad, kad subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu. Tad subjekts saņem SAB saskaņojumu, lai var virzīties tālāk ar iepirkuma procedūru. Gala saskaņošanas posmā izvēlētais pretendents tāpat uzzinās ar kādu sistēmu un kāda statusa infrastruktūrā tam būs jāstrādā. Lai mazinātu apsvērumus, uz kuriem vērsta uzmanība, aicinām, izvirzot prasības pretendentiem, iepirkumu dokumentācijā norādīt pēc iespējas mazāk informācijas un izvērtēt norādāmās informācijas detalizācijas apjomu.

37. *Uzņēmums ir iekļauts kritiskās infrastruktūras kopumā, kuram īpašumā un valdījumā ir A klases informācijas sistēmas. Iegādājoties mākoņpakalpojumu (piemēram, automašīnu stāvvietas rezervēšanas sistēma, kas nav integrēta ar uzņēmuma informācijas tehnoloģiju infrastruktūru), kur attiecīga sistēma nav uzņēmuma īpašumā, valdījumā vai kontrolē – vai un kādas prasības būtu jāiekļauj no MK noteikumu Nr. 397 4.2.sadaļas? Ņemot vērā, ka MK noteikumu Nr. 397 93. punkts nosaka pienākumu atzinuma saņemšanai pakalpojumam A klases sistēmai, bet 94. punkts paredz iespēju saņemt atzinumu, ja tiek slēgts ārpakalpojuma līgums tehnisko resursu iegādei A klases informācijas sistēmai, pēc kādiem kritērijiem MK noteikumu Nr. 397 izpratnē nosakāms, ka ārpakalpojuma sniedzēja informācijas sistēma ietilpst kritiskās infrastruktūras kopumā?*

Attiecībā uz mākoņpakalpojumu saņemšanu, skaidrojam, ka MK noteikumu Nr. 397 4.2. sadaļa ir jāpiemēro, ja mākoņpakalpojumi tiek izmantoti IKT infrastruktūras A drošības klases informācijas sistēmas vajadzībām. Attiecībā uz jautājuma daļu par to, pēc kādiem kritērijiem MK noteikumu Nr. 397 izpratnē nosakāms, ka ārpakalpojuma sniedzēja informācijas sistēma ietilpst KI kopumā, skaidrojam, ka Ministru kabinets apstiprina kritiskās infrastruktūras kopumu saskaņā ar Nacionālās drošības likuma 10. panta pirmās daļas 3. punktā noteikto. Attiecīgi valsts drošības iestāde (SAB, MIDD vai VDD) informē kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju par kritiskās infrastruktūras iekļaušanu kritiskās infrastruktūras kopumā. Valsts drošības iestādes atbilstoši kritiskās infrastruktūras kopumā noteiktajai kompetencei informē A, B vai C kategorijas kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju par kritiskās infrastruktūras iekļaušanu kritiskās infrastruktūras kopumā.

38. *MK noteikumu Nr. 397 93. punkts un 94. punkts – Ja uzņēmums, kas ir iekļauts kritiskās infrastruktūras kopumā, izmanto dinamisko iepirkumu sistēmu (DIS) un ir kvalificējies pretendents, kas turpmāk var piedalīties konkrēta iepirkuma sniegšanā par pakalpojumu vai preču iegādi, vai šos pretendents var iesniegt izvērtēšanai SAB un saņemt atzinumu, un pie katra iepirkuma vairs neprasīt atzinumu? Kādā termiņā tiks sniegts atzinums ārpakalpojuma līgumam par tehnisko resursu iegādi (94. punkts)?*

Saskaņā ar MK noteikumu Nr. 397 86. punktā noteikto subjekts ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi nedrīkst slēgt, ja izpildās 86. punktā ietvertie kritēriji. Gadījumā, ja netiek konstatētas neatbilstības MK noteikumu Nr. 397 86. punktā noteiktajam, tad vispārīgās vienošanās gadījumā ar SAB jāaskaņo tikai komersants, savukārt, slēdzot ārpakalpojuma līgumu, ar SAB ir jāaskaņo gan komersants, gan tā personāls. Turklāt vēršam uzmanību, ka vispārīgās vienošanās gadījumā ir jāatsaucas uz MK noteikumu Nr. 397 93. un 94. punktu. Noteikumu 94. punkts nosaka, ka IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi atļauts slēgt, ja ārpakalpojuma sniedzējs un tehniskā resursa ražotājs atbilst 94.1. apakšpunktā ietvertajām prasībām.

Vienlaikus administratīvā sloga mazināšanas nolūkos, kā arī ņemot vērā to, ka iepirkumu procedūras norit vairākās kārtās un arī pretendentu skaits mēdz būt apjomīgs, skaidrojam, ka SAB saskaņojumu sniedz tad, kad

subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu un tad saņem SAB saskaņojumu, lai var virzīties tālāk ar iepirkuma procedūru. SAB atzinumu sniedz triju mēnešu laikā, nepieciešamības gadījumā atzinuma sniegšanu var pagarināt uz vēl vienu mēnesi.

39. Vēlos noskaidrot, kā būtu korekti piemērot MK noteikumu Nr. 397 96. punkta otrajā daļā noteikto prasību par piekrišanas iegūšanu, ņemot vērā Vispārīgās datu aizsardzības regulas (VDAR) noteikumus. Datu nodošana SAB un pārbaūžu veikšana personas datu aizsardzības kontekstā ir darbība, kuras apstrādes tiesiskais pamats ir juridiskā pienākuma izpilde, nevis piekrišana. Saskaņā ar VDAR prasībām piekrišanai ir jābūt informētai un brīvprātīgi dotai, turklāt tiesiskais pamats "juridiskā pienākuma izpilde" nevar vienlaikus balstīties uz piekrišanu. Tas rada jautājumu par vārda "piekrišana" interpretāciju, kā arī par to, kā praktiski piemērot 96. punkta otrajā daļā noteikto pienākumu iegūt juridiskās personas un ārpakalpojuma izpildē iesaistīto apakšuzņēmēju (ja attiecināms) piekrišanu pārbaudes veikšanai, kā arī ārpakalpojuma izpildē iesaistīto fizisko personu vai fiziskas personas kā ārpakalpojuma sniedzēja piekrišanu pārbaudes veikšanai. Lūdzu sniedziet viedokli arī par to, kā rīkoties situācijās, ja fiziskā persona sākotnēji piekrišanu sniedz, bet vēlāk to atsauc. Kā šādos gadījumos būtu nodrošināma noteikumu prasību izpilde, vienlaikus ievērojot VDAR principus un nepieļaujot neatbilstošu personas datu apstrādi.

MK noteikumu Nr. 397 96. punktā minētā piekrišana ir praktisks apliecinājums par informētību, kas ir piekrišana pārbaudes veikšanai šo noteikumu izpratnē. Gadījumā, ja persona piekrišanas parakstīšanas brīdī par paredzamo datu apstrādi, nevēlas, lai šāda pārbaude tiktu veikta un atsakās parakstīt apliecinājumu, persona nevar tikt iesaistīta pakalpojumu sniegšanā IKT KI.

40. 96. punkts un 100.2. punkts - Ja uzņēmums ir iekļauts kritiskās infrastruktūras kopumā un ir nepieciešams piesaistīt papildus ārpakalpojuma darbiniekus, kuriem nav veikta pārbaude, avārijas novēršanā – kā uzņēmumam rīkoties, jo darbi jāveic nekavējoties un nav laika gaidīt atzinumu.

Skaidrojam, ka MK noteikumos Nr. 397 noteiktajiem termiņiem nav paredzētas atkāpes. Vēršam Jūsu uzmanību uz to, ka SAB jebkurā gadījumā ir nepieciešams veikt personu pārbaudes. Vienlaikus norādām, ka atbilstoši minimālajām kiberdrošības prasībām, subjektam kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā jāiekļauj arī rīcības plāns darbības atjaunošanai nozīmīga kiberincidenta vai krīzes gadījumā. Katrā šādā individuālā gadījumā (tostarp ārpuskārtas gadījumos, piemēram, avārijas novēršana u.tml.) subjektam jāsaazinās ar uzraugošo iestādi, un kiberincidentu gadījumos subjekts nekavējoties veic visas nepieciešamās darbības tā novēršanai un par to informē kompetento kiberincidentu novēršanas institūciju – CERT.LV.

41. Ja iepriekš prasīts un saņemts SAB atzinums par ārpakalpojuma sniedzēju iepirkumā, kas sastāv no vairākām daļām, kur par katru atsevišķu daļu tiek slēgts līgums, vai SAB atzinums jāsaņem par katru līgumu atsevišķi, ja ārpakalpojuma sniedzējs paliek nemainīgs?

Apstiprinām, ka gadījumā, ja iepriekš prasīts un saņemts SAB atzinums par ārpakalpojuma sniedzēju iepirkumā, kas sastāv no vairākām daļām, kur par katru atsevišķu daļu tiek slēgts līgums, ir jāsaņem atzinums par katru daļu atsevišķi. Norādām, ka vispārīgas vienošanās gadījumā ir jānorāda atbilstība MK noteikumu Nr. 397 93. un 94. punktā noteiktajam. Vienlaikus SAB skaidro, ka subjekts var izvērtēt iepirkuma dalīšanu daļās, proti, nedalīt to vairākās atsevišķās daļās.

42. Vai Satversmes aizsardzības biroja atzinuma termiņš atšķiras, ja tiek vērtēts Latvijas uzņēmums, Eiropas uzņēmums vai trešo valstu uzņēmums?

SAB atzinuma termiņš ir noteikts MK noteikumu Nr. 397 93. punktā un tas ir maksimālais MK noteikumos Nr. 397 paredzētais termiņš, kas nepieciešams drošības iestādei, lai rūpīgi izvērtētu un pārbaudītu iesniegto informāciju un tas attiecas gan uz Latvijas uzņēmumiem, gan Eiropas uzņēmumiem.

43. MK noteikumu Nr. 397 8. pielikums - Kritiskās infrastruktūras kopumā iekļauts uzņēmums līgumos pretendentiem ir iekļāvis prasību iesniegt ārpakalpojuma līguma izpildē iesaistīto speciālistu datus: vārds, uzvārds, personas kods, specialitāte. Vai atzinuma saņemšanai pietiks ar šo datu apjomu vai arī var tikt pieprasīts iesniegt papildus datus? Ja jā, tad kāds datu apjoms var tikt pieprasīts un kādos gadījumos tas tiks pieprasīts? Vai uzņēmumam noteiktas valsts vai reģiona pakalpojuma sniedzēja līgumos nevajadzētu iekļaut papildus nepieciešamo datu apjoma pieprasīšanu?

Skaidrojam, ka norādītais datu apjoms ir pietiekošs, ņemot vērā to, ka MK noteikumu Nr. 397 8. pielikumā pie ārpakalpojuma līguma izpildē iesaistīto speciālistu norādāmās informācijas ir lūgts norādīt personu vārdu, uzvārdu, personas kodu un specialitāti. Vienlaikus attiecībā uz ārvalstu komersantiem var būt nepieciešama plašāka informācija par noteikumu 8. pielikumā noteikto, tostarp dzimšanas datums un vieta (pilsēta, valsts), aktuālā faktiskās dzīvesvietas adrese, kā arī personu apliecinoša dokumenta dati (dokumenta veids, izdevēja iestāde, izdošanas datums un numurs).

44. *Ja es katru nedēļu veicu iepirkumu EIS un tajā tiesības slēgt līgumu iegūst viens un tas pats uzņēmējs ar vienu un to pašu izstrādes komandu, tad cik racionāli ir katru nedēļu sūtīt uz SAB vēstules ar lūgumu izvērtēt uzņēmēju un tā komandu. Manuprāt, tas ir gan slogs SAB personālam, gan ļoti apgrūtina plānoto darbu veikšanu noteiktā termiņā.*

Arī gadījumā, ja pakalpojuma sniedzējs jau iepriekš ir bijis pārbaudīts un SAB atzinums ir ticis saņemts, minētā prasība pamatojama ar drošības apsvērumiem – lai identificētu aktuālos iespējamās drošības riskus, kā arī izvērtētu atbilstību normatīvajos aktos noteiktajām prasībām. Turklāt, jāņem vērā, ka pat ar jau zināmu pakalpojuma sniedzēju apstākļi un situācija var mainīties, tāpēc atzinumu ir nepieciešams saņemt pat, ja pakalpojuma sniedzējs jau iepriekš ir bijis pārbaudīts.

45. *Vai jāsaskaņo arī visi EIS veiktie pirkumi? Varbūt EIS varētu ieviest funkcionalitāti SAB saskaņojuma saņemšanai – pārkot preces vai pakalpojumus, atzīmēt "Saņemt saskaņojumu no SAB" un pieprasījums saskaņojumam uz SAB aiziet automātiski?*

Jā, saskaņojums jāsaņem arī iepirkumiem, kas tiek veikti Elektroniskajā iepirkumu sistēmā. EIS funkcionalitātes nodrošināšana nav NKDC un SAB kompetences jautājums, taču vienlaikus vēršam uzmanību, ka, lai atvieglotu SAB uzraudzībā esošajiem NKDL subjektiem pieprasījuma veidlapas aizpildīšanu un iesniegšanu, SAB ir izveidojis saiti, ko var aizpildīt šeit: [Satversmes aizsardzības biroja atzinuma veidlapas ģenerācijas rīks](#).

46. *Jautājums par EIS katalogā veicamām iegādēm, kur EIS paredz termiņu komersanta pārbaudei 15 dienas, savukārt, MK noteikumu Nr. 397 93. punkts pieļauj 3 mēnešus +1 papildus mēnesi ilgu pārbaudi. Kā pasūtītājam rīkoties situācijā, ja EIS katalogā esošā komersanta pārbaude ieilgst?*

Saskaņā ar MK noteikumu Nr. 397 93. punktā noteikto, IKT KI īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai atļauts slēgt tikai pēc SAB atzinuma saņemšanas. SAB atzinumu sniedz triju mēnešu laikā, nepieciešamības gadījumā atzinuma sniegšanu var pagarināt uz vēl vienu mēnesi (3+1). Norādītais termiņš ir maksimālais termiņš, kas nepieciešams drošības iestādei, lai rūpīgi izvērtētu un pārbaudītu iesniegto informāciju, turklāt iepirkuma procedūras iespēju robežās vēlams organizēt un plānot savlaicīgi, ierēķinot to, ka atzinums no drošības iestādes būs nepieciešams.

Vienlaikus subjekts, pieprasot SAB atzinumu var uzreiz norādīt informāciju, kuru tas pats ir noskaidrojis par komersantu un/vai tā personālu, vienlaikus termiņš ir tāds, kāds tas MK noteikumos Nr. 397 ir norādīts un ar norādīto termiņu ir jāērēķinās.

47. *Kā noteikt, kurā gadījumā kiberdrošības prasības jāpiemēro arī ne-IT iepirkumos (piem., drukas pakalpojumi, mārketinga ārpakalpojumi)?*

Gadījumā, ja iepirkumu ietvars neatbilst MK noteikumu 397 2.3 apakšpunkta definīcijai, t.i., ārpakalpojuma līgums nav paredzēts par IKT resursa vai pakalpojuma iegādi, tad vispārīgas kiberdrošības prasības var tikt piemērotas pēc pasūtījuma veicēja ieskatiem, novērtējot, piemēram, iespējamo iepirkumā norādīto pakalpojumu ietekmi uz uzņēmuma reputāciju, finansēm, darbības nepārtrauktību vai personu datu aizsardzības nodrošināšanu.

48. VDAA uztur Elektronisko iepirkumu sistēmu (EIS). Vai publiskās pārvaldes iestāde var būt pārliecināta, ka uzņēmumi, kas piedāvā pakalpojumus un preces EIS atbilst MK noteikumu Nr. 397 "Minimālās kiberdrošības prasības" 86. punkta prasībām?

Publiskās pārvaldes iestāde var būt pārliecināta par IKT resursu vai pakalpojumu iegādes atbilstību kiberdrošības prasībām gadījumā, ja iepirkuma organizēšanā tā nodrošina Nacionālās kiberdrošības likumā un MK noteikumos Nr. 397 noteikto prasību ievērošanu. EIS platforma nodrošina iepirkumu veikšanu, savukārt konkrētā iepirkuma nosacījumu un prasību noteikšana ir attiecīgās publiskās pārvaldes iestādes kompetencē, tostarp ievērojot nosacījumus par pretendenta atbilstību MK noteikumu Nr. 397 86. punktā noteiktajiem kritērijiem. Katra iepirkuma organizēšanā, kas paredz IKT resursa vai pakalpojuma iepirkumu, ir nosakāmas prasības pretendentiem atbilstoši Nacionālās kiberdrošības likuma un MK noteikumu Nr. 397, t.sk. gadījumā, ja iepirkumu paredzēts veikts kritiskās infrastruktūras funkciju nodrošināšanai, veicot atbilstošas papildus darbības, iesniedzot attiecīgu pieteikumu par pretendenta pārbaudi SAB.

49. Kādos resursos ir ieteicams veikt pārbaudi iepirkuma laikā par pretendenta atbilstību "Minimālās kiberdrošības prasības" noteikumu 12. punktam?

Būtisko pakalpojumu sniedzējs, kas nav IKT kritiskās infrastruktūras īpašnieks vai valdītājs, pārbauda MK noteikumu Nr. 397 12. punktā noteiktās prasības tiktāl, ciktāl tas ir iespējams, izmantojot tam pieejamo informāciju, tostarp publiski pieejamas sistēmas un datu bāzes.

50. Vai minimālās kiberdrošības prasības ir obligāti jāiekļauj visos iepirkumu nolikumos, kas saistīti ar IT pakalpojumiem?

Katra iepirkuma organizēšanā, kas paredz IKT resursa vai pakalpojuma iepirkumu, ir nosakāmi nosacījumi un prasības pretendentiem atbilstoši Nacionālās kiberdrošības likuma un MK noteikumu Nr. 397 prasībām, t.sk. gadījumā, ja iepirkumu paredzēts veikt kritiskās infrastruktūras funkciju nodrošināšanai, veicot atbilstošas papildus darbības un iesniedzot attiecīgu pieteikumu par pretendenta pārbaudi SAB.

51. Vai MK noteikumu Nr. 397 94. un 108. punktā noteiktās prasības attiecībā uz IKT kritiskās infrastruktūras tehnisko resursu iegādēm un kiberdrošības prasību ievērošanu ir piemērojamas tikai tiešajiem kritiskās IKT infrastruktūras iepirkumiem, vai arī tās attiecas plašāk – uz visiem ar kritisko infrastruktūru saistītajiem tehniskajiem resursiem un informācijas sistēmām (piemēram, videonovērošanas sistēmām, elektroauto u.c.), kas var radīt kiberdrošības riskus?

Saskaņā ar MK noteikumu Nr. 397 30. punktu subjekts apzina un uzskaita visus tā īpašumā un valdījumā esošos IKT resursus un informācijas sistēmas, kas pakļauti drošības riskiem. Līdz ar to gadījumā, ja ar IKT infrastruktūru saistītie tehniskie resursi tiešā veidā ietekmē IKT tehnisko resursu un IS drošības riskus, ir vērtējama attiecīgo tehnisko resursu un IS iekļaušana IKT resursu un informācijas sistēmu katalogā, kam attiecīgi piemērojamas MK noteikumos Nr. 397 prasības par tehnisko resursu iegādēm un ar to saistītu pārbaudi veikšanu.

52. Vai iepirkumā, kurā tiek piemērots 94. punkts, uzņēmums var nepiemērot 95.2. punkta prasību, proti – vai 95.2. punktā noteiktā atzinuma saņemšana ir obligāta prasība iepirkumā, vai arī iespējams izslēgt pretendentu, ja tiek konstatēts, ka nav atbilstība 94. punktam?

Pretendentu neatbilstības gadījumā to var neizslēgt, ja saskaņā ar MK noteikumu Nr. 397 95.2. punktu, ir saņemts SAB atzinums, ka līgumu var slēgt izņēmuma kārtā.

Vienlaikus MK noteikumu Nr. 397 95.2. apakšpunktu par SAB atzinuma saņemšanu, ka līgumu var slēgt izņēmuma kārtā, var nepiemērot un drīkst izslēgt pretendentu, pamatojoties uz MK noteikumu Nr. 397 94. punkta prasībām, kas izvirza prasības tehniskā resursa ražotājam.

53. *Kādi ir veiksmīgākie soļi vai padomi iepirkumu procedūru organizēšanā, lai nodrošinātu pēc iespējas neieilgstošu iepirkuma procedūras norisi, kas saistīta ar iepirkumiem IKT kritiskajā infrastruktūrā?*

Attiecībā uz IKT KI subjekts pats nepārbauda ārpakalpojuma sniedzēju, jo saskaņā ar MK noteikumu Nr. 397 IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai atļauts slēgt tikai pēc SAB atzinuma saņemšanas un SAB veic attiecīgas pārbaudes. Līdz ar to, kā viens no raitas minētās pārbaudes nodrošināšanas apstākļiem SAB atzinuma saņemšanai varētu būt minēto noteikumu 96.1. apakšpunktā paredzētās veidlapas savlaicīga iesniegšana, norādot pēc iespējas visu iesniedzēja rīcībā esošo veidlapā paredzēto informāciju, kam varētu būt nozīme atzinuma vērtējuma izskatīšanai un saņemšanai. Vienlaikus administratīvā sloga mazināšanas nolūkos, kā arī ņemot vērā to, ka iepirkumu procedūras norit vairākās kārtās un arī pretendentu skaits mēdz būt apjomīgs, skaidrojam, ka SAB saskaņojumu sniedz tad, kad subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu un tad saņem SAB saskaņojumu, lai var virzīties tālāk ar iepirkuma procedūru.

54. *Kā būtu korektāk rīkoties – pārbaudi par ārpakalpojuma sniedzēju veicam, ja rodas šaubas vai nav pārliecības par atbilstību prasībām, bet veicot pasūtījumu EIS, uzreiz norādām to, ka nepieciešama pārbaude?*

Informējam, ka katrā konkrētajā gadījumā situācija vērtējama atbilstoši aktuāliem faktiskajiem un tiesiskajiem apstākļiem, t.sk. drošības riskiem. SAB pārbaude atzinuma saņemšanai organizējama saskaņā ar MK noteikumu Nr. 397 prasībām, t.sk. savlaicīgi informējot un nodrošinot juridiskās personas un ārpakalpojumu izpildē iesaistīto apakšuzņēmēju (ja attiecināms) piekrišanu pārbaudes veikšanai, kā arī to ārpakalpojuma izpildē iesaistīto fizisko personu piekrišanu pārbaudes veikšanai vai fiziskās personas kā ārpakalpojuma sniedzēja piekrišanu pārbaudes veikšanai, un minēto noteikumu 96.1. apakšpunktā paredzētās veidlapas savlaicīga aizpildīšana un iesniegšana norādot pēc iespējas visu iesniedzēja rīcībā esošo veidlapā paredzēto informāciju, kam varētu būt nozīme atzinuma vērtējuma izskatīšanai un saņemšanai.

55. *Kurā atklāta iepirkuma posmā notiek apakšuzņēmēja un SAB nesaskaņotā personāla nomaiņa?*

Informējam, ka katrā konkrētajā gadījumā situācija vērtējama atbilstoši aktuāliem faktiskajiem un tiesiskajiem apstākļiem, t.sk. atbilstoši drošības riskiem un SAB pārbaudē konstatētajiem apstākļiem, kas var būt konstatēti tikai pēc pārbaudes pabeigšanas un atzinuma saņemšanas. Vienlaikus vēršam uzmanību, ka administratīvā sloga mazināšanas nolūkos, kā arī ņemot vērā to, ka iepirkumu procedūras norit vairākās kārtās un arī pretendentu skaits mēdz būt apjomīgs, skaidrojam, ka SAB saskaņojumu sniedz tad, kad subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu un tad saņem SAB saskaņojumu, lai var virzīties tālāk ar iepirkuma procedūru.

56. *Vai ir pamatoti prasīt visiem iepirkuma pretendentiem pakalpojuma izpildē iesaistīto personu vārdu, uzvārdu, p.k., specialitāti, ja atlasē tie netiek nevērtēti (nepieciešams SAB pārbaudei), vai jādūdz tikai uzvarētājam?*

Skaidrojam, ka SAB saskaņojumu sniedz tad, kad subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu. Kā arī, ja tiek sniegta informācija SAB atzinuma saņemšanai, aizpildot MK noteikumu Nr. 397 8. pielikumā paredzēto veidlapu, informācija jānorāda pilnā apjomā, t.sk. par personām, kuras paredzēts iesaistīt pakalpojuma izpildē.

57. *Kādi būtu priekšlikumi piegādes ķēdes atbilstības pārbaudei?*

Atbilstoši MK noteikumiem Nr. 397 piegādes ķēdes drošības riski tiek apzināti un novērtēti pirms ārpakalpojuma iegādes, nosakot ārpakalpojuma kvalitātes, drošības un pieejamības prasības minēto risku

mazināšanai, kā arī ārpakalpojuma izbeigšanas stratēģiju. NKDC ieskatā minētie riski katrā konkrētajā gadījumā var būt atšķirīgi, bet pie vispārīgiem piegādes ķēžu atbilstības riskiem varētu būt pieskaitāmi apstākļi, kas norādīti minēto noteikumu 97. punktā, kā arī informācija par aktuāliem kiberriskiem, t.sk. attiecīgajā darbības nozarē.

58. *Vēlos saprast kā praktiski būtu jāorganizē iepirkumu procedūra. Attiecīgi kurā brīdī pretendenti IKT KI iepirkumā būtu jāizvērtē? Visi pretendenti, kas piesakās vai tikai uzvarētāju?*

Administratīvā sloga mazināšanas nolūkos, kā arī, ņemot vērā to, ka iepirkumu procedūras norit vairākās kārtās un arī pretendentu skaits mēdz būt apjomīgs, SAB saskaņojumu sniedz tad, kad subjekts ir nonācis līdz gala lēmumam par izvēlēto pretendentu un tad saņem SAB saskaņojumu, lai var virzīties tālāk ar iepirkuma procedūru.

59. *Kā rīkoties situācijās, kad, piemērojot MK noteikumu Nr. 397 86. un 94. punktu prasības, tiek konstatēts, ka EIS pasūtītām iekārtām vai to rezerves daļām ir izcelsmes marķējums "Made in China" vai cita Āzijas valsts? Piemēram: ja Lenovo serverim (vērtība 15 000 EUR) nepieciešama rezerves detaļa (ventilators par 20 EUR), kas nav pieejama ES vai draudzīgajās valstīs – kā šādu detaļu tiesiski iegādāties; vai ir pieļaujams to iegādāties, piemēram, eBay platformā? Kā pārliecināties par atbilstību prasībām?*

Nevērtējot konkrēto datortehnikas ražotāju, t.sk. apstākļus, kas saistīti ar datortehnikas vai tā daļu faktisko ražošanas vietu vai daļu komplektēšanu, informējam, ka MK noteikumi Nr. 397 86. un 94. pants paredz priekšnoteikumus attiecībā uz ārpakalpojumu sniedzēju un tehnisko ražotāju juridisko personu (reģistrācijas vietu, valdes un padomes sastāva pilsonību, juridiskās personas patiesā labuma guvējiem).

Papildus minētajam vēršam uzmanību, ka MK noteikumu 95.2. apakšpunktā atsevišķiem gadījumiem paredzēts izņēmuma gadījums, kad var nepiemērot šo noteikumu 94. punktā noteiktās prasības, kā arī katrs konkrētais gadījums ir vērtējams individuāli. Vienlaikus norādām, ka minētais izņēmums nav attiecināms uz 86. punktā noteikto ierobežojumu.