2025/295

13.2.2025.

KOMISIJAS DELEĢĒTĀ REGULA (ES) 2025/295

(2024. gada 24. oktobris),

ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par to nosacījumu saskaņošanu, kas ļauj veikt pārraudzības darbības

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 ([1]), un jo īpaši tās 41. panta 2. punkta otro daļu,

tā kā:

(1) Ar finanšu nozares digitālās darbības noturības satvaru, kas izveidots ar Regulu (ES) 2022/2554, ievieš Savienības pārraudzības satvaru attiecībā uz trešām personām, kas sniedz informācijas un komunikācijas tehnoloģiju (IKT) pakalpojumus finanšu nozarē un kas izraudzītas par kritiski svarīgām saskaņā ar minētās regulas 31. pantu.

(2) Trešai personai, kas sniedz IKT pakalpojumus un kas nolemj iesniegt brīvprātīgu pieprasījumu izraudzīšanai par kritiski svarīgu, būtu jāiesniedz saņēmējai Eiropas uzraudzības iestādei (EUI) visa nepieciešamā informācija, lai pierādītu tās kritisko svarīgumu saskaņā ar Regulā (ES) 2022/2554 noteiktajiem principiem un kritērijiem. Šā iemesla dēļ pieteikumā ar brīvprātīgu pieprasījumu iekļaujamajai informācijai vajadzētu būt pietiekami detalizētai un pilnīgai, lai varētu veikt skaidru un pilnīgu kritiskā svarīguma novērtējumu saskaņā ar minētās regulas 31. panta 11. punktu. Attiecīgajai EUI būtu jānoraida visi nepilnīgie pieteikumi un jāpieprasa trūkstošā informācija.

(3) Trešo personu, kas sniedz IKT pakalpojumus, juridiskā identifikācija šā regulatīvā tehniskā standarta darbības jomā būtu jāsaskaņo ar identifikācijas kodu, kas noteikts Komisijas īstenošanas regulā, kura pieņemta saskaņā ar Regulas (ES) 2022/2554 28. panta 9. punktu.

(4) Pēc ieteikumiem, ko galvenais pārraugs sniedzis kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, galvenajam pārraugam būtu jāuzrauga, kā kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, pilda ieteikumus. Lai nodrošinātu, ka kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, veiktās darbības vai īstenotie tiesiskās aizsardzības līdzekļi tiek efektīvi un lietderīgi uzraudzīti saistībā ar šiem ieteikumiem, galvenajam pārraugam vajadzētu būt iespējai pieprasīt Regulas (ES) 2022/2554 35. panta 1. punkta c) apakšpunktā minētos ziņojumus, kas būtu jāparedz kā starpposma progresa ziņojumi un galīgie ziņojumi.

(5) Lai veiktu Regulas (ES) 2022/2554 42. panta 1. punktā minēto novērtējumu, saskaņā ar kuru galvenajam pārraugam ir jāizvērtē, vai kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, sniegtais paskaidrojums ir pietiekams, kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, paziņojums galvenajam pārraugam par tās nodomu ievērot saņemtos ieteikumus būtu jāpapildina ar to darbību un pasākumu aprakstu, kas ir veikti, lai mazinātu ieteikumos izklāstītos riskus, kā arī to attiecīgajiem termiņiem. Šāds paskaidrojums būtu jāsniedz sanācijas plāna veidā.

(6) Tā kā ir sagaidāms, ka galvenais pārraugs novērtēs kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, apakšuzņēmuma līgumus, ir jāizstrādā veidne informācijas iesniegšanai par minētajiem līgumiem. Veidnē būtu jāņem vērā tas, ka kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, struktūras atšķiras no finanšu vienību struktūrām.

([1]) OV L 333, 27.12.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Tiklīdz galvenais pārraugs ir sniedzis ieteikumus kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, un kompetentās iestādes ir informējušas attiecīgās finanšu vienības par minētajos ieteikumos norādītajiem riskiem, galvenajam pārraugam būtu jāuzrauga un jānovērtē, kā kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, īsteno darbības un tiesiskās aizsardzības līdzekļus, lai izpildītu ieteikumus. Kompetentajām iestādēm būtu jāuzrauga un jānovērtē tas, cik lielā mērā finanšu vienības ir pakļautas šajos ieteikumos apzinātajiem riskiem. Lai saglabātu vienlīdzīgus konkurences apstākļus, veicot attiecīgos uzdevumus, jo īpaši tad, ja ieteikumos apzinātie riski ir nopietni un tie ir kopīgi lielam skaitam finanšu vienību vairākās dalībvalstīs, gan kompetentajām iestādēm, gan galvenajam pārraugam būtu savstarpēji jāapmainās ar visiem attiecīgajiem konstatējumiem, kas tiem ir vajadzīgi to attiecīgo uzdevumu veikšanai. Informācijas apmaiņas mērķis ir nodrošināt, ka galvenā pārrauga atsauksmēs kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, par darbībām un tiesiskās aizsardzības līdzekļiem, ko tā īsteno, tiek ņemta vērā ietekme uz finanšu vienību riskiem un ka kompetento iestāžu veiktās uzraudzības darbības ir balstītas uz galvenā pārrauga veikto novērtējumu.

(8) Lai nodrošinātu efektīvu un lietderīgu informācijas apmaiņu, kompetentajām iestādēm, veicot uzraudzības darbības, būtu jānovērtē, cik lielā mērā to uzraudzītās finanšu vienības ir pakļautas ieteikumos norādītajiem riskiem. Šis novērtējums būtu jāveic samērīgā un uz risku balstītā veidā. Galvenajam pārraugam būtu jāprasa kompetentajām iestādēm dalīties ar šā novērtējuma rezultātiem konkrētos gadījumos, kad ar ieteikumiem saistītie riski ir nopietni un izplatīti lielam skaitam finanšu vienību vairākās dalībvalstīs. Lai pēc iespējas labāk izmantotu kompetento iestāžu resursus, pieprasot sniegt šā novērtējuma rezultātus, galvenajam pārraugam vienmēr būtu jāņem vērā, ka šo pieprasījumu mērķis ir izvērtēt kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, darbību un tiesiskās aizsardzības līdzekļu īstenošanu.

(9) Notika apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju (EDAU) saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([2]) 42. panta 1. punktu, un EDAU 2024. gada 22. jūlijā sniedza atzinumu.

(10) Šī regula ir balstīta uz regulatīvo tehnisko standartu projektu, ko Komisijai iesniegušas EUI.

(11) EUI apvienotā komiteja veica atklātu sabiedrisko apspriešanu par regulatīvo tehnisko standartu projektu, kas ir šīs regulas pamatā, izvērtēja potenciālās saistītās izmaksas un ieguvumus un lūdza atzinumu no Banku nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 ([3]) 37. pantu, no Apdrošināšanas un pārapdrošināšanas nozares ieinteresēto personu grupas un Aroda pensiju nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1094/2010 ([4]) 37. pantu, un no Vērtspapīru un tirgu nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1095/2010 ([5]) 37. pantu,

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1094/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un aroda pensiju iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/79/EK (OV L 331, 15.12.2010., 48. lpp., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1095/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Vērtspapīru un tirgu iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/77/EK (OV L 331, 15.12.2010., 84. lpp., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Informācija, kura trešai personai, kas sniedz IKT pakalpojumus, jāiesniedz pieteikumā izraudzīšanai par kritiski svarīgu

1. Trešā persona, kas sniedz informācijas un komunikācijas tehnoloģiju (IKT) pakalpojumus, pamatotajā pieteikumā ar brīvprātīgu pieprasījumu saskaņā ar Regulas (ES) 2022/2554 31. panta 11. punktu izraudzīšanai par kritiski svarīgu saskaņā ar Regulas (ES) 2022/2554 31. panta 1. punkta a) apakšpunktu iesniedz šādu informāciju:

a) juridiskās personas nosaukums;

b) juridiskās personas identifikācijas kods;

c) kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, kontaktpersonas vārds un uzvārds un kontaktinformācija;

d) valsts, kurā juridiskajai personai ir juridiskā adrese;

e) korporatīvās struktūras apraksts, tostarp vismaz informācija par tā mātesuzņēmumu un citiem saistītiem uzņēmumiem, kas sniedz IKT pakalpojumus Savienības finanšu vienībām. Attiecīgā gadījumā minētā informācija ir šāda:

   i) juridiskās personas nosaukums;

   ii) juridiskās personas identifikācijas kods;

   iii) valsts, kurā juridiskajai personai ir juridiskā adrese;

f) trešās personas, kas sniedz IKT pakalpojumus, tirgus daļas aplēse Savienības finanšu nozarē un tirgus daļas aplēse katram finanšu vienības veidam, kā minēts Regulas (ES) 2022/2554 2. panta 1. punktā, no gada, kad iesniegts pieteikums izraudzīšanai par kritiski svarīgu, un gadu pirms minētā pieteikuma;

g) apraksts par katru Savienības finanšu vienībām sniegto IKT pakalpojumu, tostarp:

   i) apraksts par darījumdarbības veidu un finanšu vienībām sniegto IKT pakalpojumu veidu;

   ii) to finanšu vienību funkciju saraksts, kuras tiek atbalstītas ar sniegtajiem IKT pakalpojumiem, ja tāds ir pieejams;

   iii) informācija par to, vai finanšu vienībām sniegtie IKT pakalpojumi atbalsta kritiski svarīgas vai svarīgas funkcijas, ja tāda ir pieejama;

h) to finanšu vienību saraksts, kuras izmanto trešās personas, kas sniedz IKT pakalpojumus, sniegtos IKT pakalpojumus, tostarp šāda informācija par katru apkalpoto finanšu vienību, ja tāda ir pieejama:

   i) juridiskās personas nosaukums;

   ii) juridiskās personas identifikācijas kods, ja tas ir zināms trešai personai, kas sniedz IKT pakalpojumus;

   iii) finanšu vienības veids, kā noteikts Regulas (ES) 2022/2554 2. panta 1. punktā;

   iv) ģeogrāfiskā atrašanās vieta, no kuras IKT pakalpojumi tiek sniegti konkrētajai juridiskajai personai;

i) to kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, saraksts, kas iekļautas jaunākajā pieejamajā šādu pakalpojumu sniedzēju sarakstā, ko saskaņā ar Regulas (ES) 2022/2554 31. panta 9. punktu publicējušas EUI, un kas izmanto pieteikuma iesniedzēja sniegtos pakalpojumus, ja tāds ir pieejams;

j) pašnovērtējums attiecībā uz šādiem aspektiem:

   i) aizstājamības pakāpe katram pieteikuma iesniedzēja sniegtajam IKT pakalpojumam, ņemot vērā šādus aspektus:

      — trešās personas, kas sniedz IKT pakalpojumus, tirgus daļa Savienības finanšu nozarē,

— zināmo attiecīgo konkurentu skaits pa IKT pakalpojumu veidiem vai IKT pakalpojumu grupām,

— apraksts par īpatnībām saistībā ar piedāvātajiem IKT pakalpojumiem, tostarp attiecībā uz jebkuru īpašniektehnoloģiju, vai trešās personas, kas sniedz IKT pakalpojumus, organizācijas vai darbības specifiskajām iezīmēm;

ii) zināšanas par to, vai ir pieejamas alternatīvās trešās personas, kuras sniedz tādus pašus IKT pakalpojumus kā trešā persona, kas sniedz IKT pakalpojumus un iesniedz pieteikumu;

k) informācija par turpmāko uzņēmējdarbības stratēģiju attiecībā uz IKT pakalpojumu sniegšanu un infrastruktūras nodrošināšanu finanšu vienībām Savienībā, tostarp visām plānotajām izmaiņām grupā vai vadības struktūrā, ienākšanu jaunos tirgos vai jaunu darbību uzsākšanu;

l) to trešās personas, kas sniedz IKT pakalpojumus, apakšuzņēmēju identifikācija, kuri ir izraudzīti par kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus;

m) jebkādi citi iemesli, kas ir būtiski, lai trešās personas, kas sniedz IKT pakalpojumus, pieteikums tiktu izraudzīts par kritiski svarīgu.

2. Ja trešā persona, kas sniedz IKT pakalpojumus, pieder pie grupas, 1. punktā minēto informāciju iesniedz attiecībā uz IKT pakalpojumiem, ko sniedz grupa kopumā.

2. pants

Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, iesniedzamās, atklājamās vai paziņojamās informācijas saturs, struktūra un formāts

1. Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, pēc galvenā pārrauga pieprasījuma sniedz tam visu informāciju, kas galvenajam pārraugam ir vajadzīga, lai tas varētu veikt savus pārraudzības pienākumus saskaņā ar Regulas (ES) 2022/2554 prasībām.

2. Šā panta 1. punktā minētā informācija *inter alia* ir šāda:

a) informācija par līgumiem un kopijas līgumiem starp:

i) kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, un finanšu vienībām, kas minētas Regulas (ES) 2022/2554 2. panta 1. punktā;

ii) kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, un tās apakšuzņēmējiem, lai aptvertu finanšu vienībām Savienībā sniegto IKT pakalpojumu tehnoloģiskās vērtības ķēdi;

b) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, organizatorisko un grupas struktūru, tostarp visu to vienību identifikācija, kuras pieder pie tās pašas grupas un kuras tieši vai netieši sniedz IKT pakalpojumus finanšu vienībām Savienībā;

c) informācija par lielākajiem akcionāriem, tostarp to struktūra un ģeogrāfiskā izplatība, attiecībā uz jebkuru no turpmāk minētajiem:

i) vienības, kurām vienpersoniski vai kopā ar savām saistītajām vienībām pieder 25 % vai vairāk kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, kapitāla vai balsstiesību;

ii) vienības, kam ir tiesības iecelt vai atlaist kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, administratīvās, vadības vai uzraudzības struktūras locekļu vairākumu;

iii) vienības, kas saskaņā ar vienošanos kontrolē kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, akcionāru vai dalībnieku balsstiesību vairākumu;

d) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, tirgus daļu pa pakalpojumu veidiem attiecīgajos tirgos, kuros tā darbojas;

e) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, iekšējo pārvaldības kārtību, tostarp struktūra ar pārvaldības atbildības līmeņiem un pārskatatbildības noteikumiem;

f) kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, vadības struktūras un jebkuru citu attiecīgo iekšējo komiteju sanāksmju protokoli, kas jebkādā veidā attiecas uz darbībām un riskiem, kuri saistīti ar trešo personu sniegtiem IKT pakalpojumiem, kas atbalsta finanšu vienību funkcijas Savienībā;

g) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, IKT drošību, tostarp attiecīgās stratēģijas, mērķi, politika, procedūras, protokoli, procesi, kontroles pasākumi sensitīvu datu aizsardzībai, piekļuves kontrole, šifrēšanas prakse, plāni reaģēšanai uz incidentiem, un attiecīgā gadījumā informācija par atbilstību visiem attiecīgajiem noteikumiem un valsts un starptautiskajiem standartiem;

h) informācija par tehniskiem un organizatoriskiem pasākumiem, ko veic, lai nodrošinātu datu aizsardzību un datu konfidencialitāti, tostarp personas datu un nepersondatu, kontroles pasākumiem, ko īsteno, lai aizsargātu sensitīvus datus, piekļuves kontroli, šifrēšanas praksi, plānu reaģēšanai uz datu aizsardzības pārkāpumiem; ja attiecībā uz personas datu apstrādi uz trešo personu, kas sniedz IKT pakalpojumus, attiecas trešo valstu tiesību akti, tostarp trešo valstu valdības piekļuves pieprasījums, – valstu saraksts un piemērojamie tiesību akti;

i) informācija par mehānismiem, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, piedāvā Savienības finanšu vienībām attiecībā uz datu pārnesamību, lietojumprogrammu pārnesamību un sadarbspēju;

j) informāciju par to datu centru un IKT ražošanas centru atrašanās vietu, kurus izmanto, lai sniegtu pakalpojumus finanšu vienībām, tostarp saraksts ar visām attiecīgajām kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, telpām un objektiem, tostarp ārpus Savienības;

k) informācija par pakalpojumiem, ko sniedz kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus no trešām valstīm, tostarp informācija par attiecīgajām tiesību normām, kas piemērojamas personas datiem un nepersondatiem, kurus apstrādā trešā persona, kas sniedz IKT pakalpojumus;

l) informācija par pasākumiem, ko veic, lai novērstu riskus, ko rada IKT pakalpojumu sniegšana, ko veic kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, un tās apakšuzņēmēji no trešām valstīm;

m) informācija par riska pārvaldības sistēmu un incidentu pārvaldības sistēmu, tostarp kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, un tās apakšuzņēmēju politiku, procedūrām, rīkiem, mehānismiem un pārvaldības pasākumiem, tostarp tādu būtisku incidentu saraksts un apraksts, kuriem ir tieša vai netieša ietekme uz finanšu vienībām Savienībā, tostarp attiecīgā informācija, lai noteiktu incidenta nozīmīgumu finanšu vienībām un novērtētu iespējamo pārrobežu ietekmi;

n) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, un tās apakšuzņēmēju pārmaiņu pārvaldības sistēmu, tostarp politiku, procedūrām un kontroli;

o) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, vispārējo reaģēšanas un seku novēršanas sistēmu, tostarp darbības nepārtrauktības plāni un saistītie pasākumi un procedūras, programmatūras izstrādes dzīves cikla politika, reaģēšanas un seku novēršanas plāni un saistītie pasākumi un procedūras, rezerves kopiju politikas pasākumi un procedūras;

p) informācija par veiktspējas uzraudzību, drošības uzraudzību un incidentu izsekošanu, kā arī informācija par ziņošanas mehānismiem, kas saistīti ar pakalpojumu veiktspēju, incidentiem un atbilstību saskaņotajām pakalpojumu līmeņa vienošanām un pakalpojumu līmeņa mērķiem vai līdzīgiem pasākumiem starp kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, un finanšu vienībām Savienībā;

q) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, IKT trešās personas pārvaldības sistēmu, tostarp stratēģijām, politiku, procedūrām, procesiem un kontrolēm, tostarp sīka informācija par pienācīgu pārbaudi un riska novērtējumu, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, veikusi attiecībā uz saviem apakšuzņēmējiem pirms nolīguma noslēgšanas ar tiem, un lai uzraudzītu attiecības, kas aptver visus attiecīgos IKT un darījumu partnera riskus;

r) izguvumi no kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, un tās apakšuzņēmēju uzraudzības un skenēšanas sistēmām, aptverot, bet ne tikai, tīkla uzraudzību, serveru uzraudzību, lietojumprogrammu uzraudzību, drošības uzraudzību, neaizsargātības skenēšanu, reģistru pārvaldību, veiktspējas uzraudzību, incidentu pārvaldību un mērījumus attiecībā pret uzticamības mērķiem, piemēram, pakalpojumu līmeņa mērķiem;

s) izguvumi no ražošanas, pirmsražošanas un testēšanas sistēmas vai lietojumprogrammas, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, un tās apakšuzņēmēji izmanto, lai tieši vai netieši sniegtu pakalpojumus finanšu vienībām Savienībā;

t) atbilstības ziņojumi un pieejamie revīzijas ziņojumi, kā arī visi attiecīgie revīzijas konstatējumi, tostarp revīzijas, ko veikušas valsts iestādes Savienībā un ārpus Savienības, ja sadarbības nolīgumos ar attiecīgajām iestādēm ir paredzēta šāda informācijas apmaiņa, vai sertifikācijas, ko ieguvusi kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, vai tās apakšuzņēmēji, tostarp iekšējo un ārējo revidentu ziņojumi, sertifikācijas vai atbilstības novērtējumi ar nozarei specifiskiem standartiem. Tas ietver informāciju par kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, IKT sistēmu noturības jebkāda veida pieejamu neatkarīgu testēšanu, tostarp jebkāda veida draudu vadītu ielaušanās testēšanu, ko veic trešā persona, kas sniedz IKT pakalpojumus;

u) informācija par visiem novērtējumiem, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, veikusi vai kas veikti tās uzdevumā, izvērtējot to personu piemērotību un integritāti, kuras ieņem svarīgus amatus kritiski svarīgajā trešajā personā, kas sniedz IKT pakalpojumus;

v) informācija par visiem sanācijas plāniem, lai izpildītu 3. pantā minētos ieteikumus, un attiecīgā saistītā informācija, kas vajadzīga, lai apstiprinātu tiesiskās aizsardzības līdzekļu īstenošanu;

w) informācija par pieejamām darbinieku apmācības shēmām un drošības izpratnes programmām, tostarp attiecīgā gadījumā informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, investīcijām, resursiem un metodēm, lai apmācītu savus darbiniekus rīkoties ar sensitīviem finanšu datiem un saglabāt augstu drošības līmeni;

x) informācija par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, darbībām un finanšu pārskati, tostarp informācija par budžetu un resursiem, kas saistīti ar IKT un drošību.

3. pants

Informācija no kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, pēc ieteikumu sniegšanas

1. Kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, iesniedz galvenajam pārraugam ziņojumu, kurā ietverts sanācijas plāns saistībā ar ieteikumiem un tiesiskās aizsardzības līdzekļi, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, plāno īstenot, lai mazinātu riskus, kas norādīti Regulas (ES) 2022/2254 35. panta 1. punkta d) apakšpunktā minētajos ieteikumos. Ziņojums atbilst grafikam, ko katram ieteikumam noteicis galvenais pārraugs.

2. Lai būtu iespējams uzraudzīt kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, veiktās darbības vai īstenotos tiesiskās aizsardzības līdzekļus saistībā ar saņemtajiem ieteikumiem, kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, pēc pieprasījuma sniedz galvenajam pārraugam:

a) starpposma progresa ziņojumus un saistītos apliecinošos dokumentus, kuros norādīts progress to darbību un pasākumu īstenošanā, kas izklāstīti ziņojumā, kuru galvenajam pārraugam iesniegusi kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, galvenā pārrauga noteiktajā termiņā;

b) galīgos ziņojumus un saistītos apliecinošos dokumentus, kuros norādītas kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, veiktās darbības vai īstenotie tiesiskās aizsardzības līdzekļi, lai mazinātu saņemtajos ieteikumos norādītos riskus.

4. pants

Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, iesniedzamās informācijas struktūra un formāts

1. Kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, iesniedz pieprasīto informāciju galvenajam pārraugam, izmantojot īpašus drošus elektroniskos kanālus, ko galvenais pārraugs norādījis savā pieprasījumā, un galvenā pārrauga noteiktajā formātā.

2. Sniedzot informāciju galvenajam pārraugam, kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus:

a) ievēro galvenā pārrauga informācijas pieprasījumā norādīto struktūru;

b) skaidri norāda attiecīgās informācijas daļas atrašanās vietu iesniegtajos dokumentos.

3. Informācija, ko kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, iesniedz, atklāj vai paziņo galvenajam pārraugam, ir valodā, ko parasti lieto starptautisko finanšu jomā.

5. pants

Veidne informācijas iesniegšanai par apakšuzņēmuma līgumiem

Kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus un kam ir jāapmainās ar informāciju par apakšuzņēmuma līgumiem, iesniedz informāciju galvenajam pārraugam saskaņā ar pielikumā doto veidni.

6. pants

Kompetento iestāžu novērtējums par riskiem, kas aplūkoti galvenā pārrauga ieteikumos

1. Finanšu vienību uzraudzības ietvaros kompetentā iestāde novērtē kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, veikto pasākumu ietekmi uz finanšu vienībām, pamatojoties uz galvenā pārrauga ieteikumiem saskaņā ar proporcionalitātes principu.

2. Veicot 1. punktā minēto novērtējumu, kompetentā iestāde ņem vērā visu turpmāk minēto:

a) to koriģējošo un korektīvo pasākumu pietiekamību un saskaņotību, kurus finanšu vienības īsteno, lai mazinātu ieteikumos norādītos riskus;

b) galvenā pārrauga veikto novērtējumu par kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, atbilstību ziņojumā iekļautajiem pasākumiem un darbībām, ja tas ietekmē tā kompetencē esošo finanšu vienību pakļautību ieteikumos norādītajiem riskiem;

c) visu citu kompetento iestāžu viedokli, ar kurām notikusi apspriešanās saskaņā ar Regulas (ES) 2022/2554 42. panta 5. punktu;

d) vai galvenais pārraugs ir uzskatījis, ka kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, īstenotās darbības un tiesiskās aizsardzības līdzekļi ir pietiekami, lai mazinātu tā kompetencē esošo finanšu vienību pakļautību ieteikumos norādītajiem riskiem.

3. Pēc galvenā pārrauga pieprasījuma kompetentā iestāde pieņemamā laikā sniedz 1. punktā minētā novērtējuma rezultātus. Pieprasot šā novērtējuma rezultātus, galvenais pārraugs, ņem vērā proporcionalitātes principu un ar ieteikumiem saistīto risku apmēru, tostarp šo risku pārrobežu ietekmi, ja tie ietekmē finanšu vienības, kas darbojas vairāk nekā vienā dalībvalstī.

4. Attiecīgā gadījumā kompetentā iestāde pieprasa finanšu vienībām sniegt jebkādu informāciju, kas vajadzīga, lai veiktu 1. punktā minēto novērtējumu.

7. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2024. gada 24. oktobrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

PIELIKUMS

VEIDNE INFORMĀCIJAS SNIEGŠANAI PAR APAKŠUZŅĒMUMA LĪGUMIEM

Informācijas kategorija	Galvenie informācijas elementi
Vispārīga informācija	— Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, nosaukums. — Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, identifikācijas kods. — Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, kontaktpersonas vārds un uzvārds un kontaktinformācija. — Veidnes iesniegšanas datums.
Pārskats par apakšuzņēmuma līgumiem	— Apakšuzņēmuma līgumu kartēšana, tostarp īss apraksts par apakšuzņēmuma līgumattiecību mērķi un tvērumu (tostarp norāde par apakšuzņēmuma līgumu kritiskuma vai svarīguma pakāpi kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus). — To IKT pakalpojumu veidu specifikācija un apraksts, par kuriem noslēgti apakšuzņēmuma līgumi, un to nozīme finanšu vienībām sniegtajiem IKT pakalpojumiem saskaņā ar īstenošanas tehniskajiem standartiem, kas pieņemti saskaņā ar Regulas (ES) 2022/2554 28. panta 9. punktu. — Precizējot IKT pakalpojumu veidus, skatīt sarakstu IV pielikumā īstenošanas tehniskajiem standartiem, kas pieņemti saskaņā ar Regulas (ES) 2022/2554 28. panta 9. punktu.
Informācija par apakšuzņēmējiem	— Katra apakšuzņēmēja nosaukums un informācija par juridisko personu (tostarp identifikācijas kods). — To darbinieku kontaktinformācija, kuri ir atbildīgi par visām apakšuzņēmuma līgumattiecībām kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, vadības struktūrā. — Pārskats par katra apakšuzņēmēja speciālajām zināšanām, pieredzi un kvalifikāciju saistībā ar nolīgtajiem IKT pakalpojumiem.
Apraksts par apakšuzņēmēju sniegtiem pakalpojumiem	— Sīks apraksts par katra apakšuzņēmēja sniegtiem konkrētiem IKT pakalpojumiem. — Apakšuzņēmējiem piešķirto pienākumu un uzdevumu sadalījums, sīki izklāstot dažādās lomas dažādos IKT procesu posmos. — Informācija par to, cik lielā mērā apakšuzņēmējiem ir piekļuve personas datiem vai citādi sensitīviem datiem vai sistēmām attiecībā uz finanšu vienībām sniegtiem IKT pakalpojumiem. — Informācija par objektiem, no kuriem tiek sniegti apakšuzņēmēju pakalpojumi, un par pasākumiem, kas veikti, lai novērstu riskus, kurus rada ārpus Savienības sniegti pakalpojumi.
Apakšuzņēmumu pārvaldība un pārraudzība	— Apraksts par līgumisko un pārvaldības sistēmu, kas ieviesta, lai pārvaldītu apakšuzņēmuma līgumattiecības, tostarp klauzulas, kas ierobežo sensitīvu datu izmantošanu. — Skaidrojums par apakšuzņēmēju atlases, iesaistīšanas un uzraudzības procesiem. — Pārskats par snieguma rādītājiem, pakalpojumu līmeņa mērķiem un līgumiem un galvenajiem darbības rādītājiem, ko izmanto, lai novērtētu apakšuzņēmēja sniegumu un uzticamības uzraudzību.
Riska pārvaldība un atbilstība	— Novērtējums par apakšuzņēmēja riska profiliem un iespējamo ietekmi uz finanšu vienībām sniegtajiem IKT pakalpojumiem. — Skaidrojums par riska mazināšanas pasākumiem, ko īsteno, lai novērstu ar apakšuzņēmumu saistītos riskus. — Ziņas par to, kā apakšuzņēmējs ievēro attiecīgos noteikumus, tostarp par datu aizsardzību un nozares standartiem.

Informācijas kategorija	Galvenie informācijas elementi
Darbības nepārtrauktības un ārkārtas situāciju plānošana	— Pārskats par apakšuzņēmēja darbības nepārtrauktības un reaģēšanas un seku novēršanas plāniem. — Apraksts par pasākumiem, kas ieviesti, lai nodrošinātu pakalpojumu nepārtrauktību gadījumā, ja apakšuzņēmējs pārtrauc vai izbeidz darbību. — Apakšuzņēmēju veikto darbības nepārtrauktības plānu un reaģēšanas un seku novēršanas plānu testu biežums, pēdējo 3 gadu laikā veikto jaunāko testu datumi un norāde, vai minētajos testos bija iesaistīta kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus.
Ziņošana	— Apraksts par ziņošanas mehānismiem un ziņošanas biežumu starp kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, un tās apakšuzņēmējiem.
Atveseļošana un incidentu pārvaldība	— To procedūru izklāsts, ar kurām risina ar apakšuzņēmēju saistītus incidentus, pārkāpumus vai neatbilstību.
Sertifikāti un revīzijas	— Informācija par visiem sertifikātiem, neatkarīgām revīzijām vai novērtējumiem, kas veikti attiecībā uz apakšuzņēmējiem, lai validētu to drošības kontroli, kvalitātes standartus vai regulatīvo atbilstību. — Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, veikto apakšuzņēmēju revīziju datums un biežums.