Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/1773

25.6.2024.

KOMISIJAS DELEĢĒTĀ REGULA (ES) 2024/1773

(2024. gada 13. marts),

ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem, sīkāk precizējot politikas detalizēto saturu saistībā ar līgumisku vienošanos par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus

(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 28. panta 10. punkta trešo daļu,

tā kā:

(1) Ar Regulu (ES) 2022/2554 izveidotais finanšu nozares digitālās darbības noturības satvars paredz, ka finanšu vienības nosaka konkrētus pamatprincipus ar trešo personu saistītā IKT riska pārvaldībai, kuri ir īpaši svarīgi, kad finanšu vienības sadarbojas ar trešām personām, kas sniedz IKT pakalpojumus, lai atbalstītu to kritiski svarīgās vai svarīgās funkcijas.

(2) Finanšu vienībām IKT riska pārvaldības satvara ietvaros ir jāpieņem un regulāri jāpārskata ar trešo personu IKT risku saistītā stratēģija. Saskaņā ar Regulas (ES) 2022/2554 28. panta 2. punktu minētajā stratēģijā ir jāiekļauj politika par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus. Tā ir jāpiemēro individuāli un attiecīgā gadījumā subkonsolidēti un konsolidēti.

(3) Finanšu vienības ir ļoti atšķirīgas pēc apjoma, struktūras un iekšējās organizācijas, kā arī to darbību un operāciju būtības un sarežģītības. Šī daudzveidība ir jāņem vērā, vienlaikus nosakot visām finanšu vienībām piemērotas konkrētas regulatīvās pamatprasības politikas izstrādei attiecībā uz līgumiskām vienošanām par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus ("politika"), un jānodrošina, ka minētās prasības tiek piemērotas samērīgā veidā.

(4) Ja finanšu vienības pieder grupai, mātesuzņēmumam, kas ir atbildīgs par konsolidēto vai subkonsolidēto finanšu pārskatu sniegšanu attiecībā uz grupu, būtu jānodrošina, ka politiku grupas iekšienē piemēro konsekventi un saskaņoti.

(5) Piemērojot šo politiku, IKT pakalpojumu sniedzēji, kuri pieder vienai grupai, tostarp tie, kas pilnībā vai kolektīvi pieder finanšu vienībām, uz kurām attiecas tā pati institucionālā aizsardzības shēma, būtu jāuzskata par trešām personām, kas sniedz IKT pakalpojumus. Riski, ko rada IKT pakalpojumu sniedzēji, kuri pieder vienai grupai, var atšķirties, bet tiem piemēro tās pašas prasības saskaņā ar Regulu (ES) 2022/2554. Līdzīgā veidā minētā politika būtu jāpiemēro apakšuzņēmējiem, kas sniedz IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, vai to būtiskas daļas trešām personām, kas sniedz IKT pakalpojumus, ja pastāv trešo personu, kas sniedz IKT pakalpojumus, ķēde.

(6) Vadības struktūras galīgā atbildība par finanšu vienības IKT riska pārvaldību ir vispārējs princips, kas ir piemērojams arī attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, izmantošanu. Šī atbildība būtu vēl vairāk jāizpauž kā vadības struktūras pastāvīga iesaiste IKT riska pārvaldības kontrolē un uzraudzībā, tostarp vismaz reizi gadā pieņemot un pārskatot politiku.

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

(7) Lai nodrošinātu pienācīgu ziņošanu vadības struktūrai, politikā būtu skaidri jānorāda un jānosaka iekšējie pienākumi apstiprināt, pārvaldīt, kontrolēt un dokumentēt līgumiskas vienošanās par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus ("līgumiskas vienošanās"), kuri ietver IKT pakalpojumus, kas sniegti saskaņā ar Regulas (ES) 2022/2554 28. panta 1. punkta a) apakšpunktā minēto līgumisko vienošanos.

(8) Lai ņemtu vērā visus iespējamos riskus, kas var rasties, slēdzot līgumus par IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgu vai svarīgu funkciju, politikas struktūrā būtu jāievēro visi katra galvenā aprites cikla fāzes posmi attiecībā uz līgumiskām vienošanām ar trešām personām, kas sniedz pakalpojumus.

(9) Lai mazinātu konstatētos riskus, politikā būtu jāprecizē līgumisko vienošanos plānošana, tostarp riska novērtējums, pienācīga rūpība un jaunu vai būtisku izmaiņu apstiprināšanas process minētajās līgumiskajās vienošanās. Lai pārvaldītu riskus, kas var rasties pirms līgumiskas vienošanās noslēgšanas ar trešo personu, kas sniedz IKT pakalpojumus, politikā būtu jānosaka piemērots un samērīgs process, ar ko atlasa un novērtē potenciālo trešo personu, kas sniedz IKT pakalpojumus, piemērotību, un jāpieprasa, lai finanšu vienība ņemtu vērā neizsmeļošu elementu sarakstu, kam vajadzētu būt trešo personu, kas sniedz IKT pakalpojumus, rīcībā. Minētajā sarakstā būtu jāiekļauj elementi, kas saistīti ar pakalpojumu sniedzēju uzņēmējdarbības reputāciju, to finanšu resursiem, cilvēkresursiem un tehniskajiem resursiem, informācijas drošību, organizatorisko struktūru, tostarp riska pārvaldību, un iekšējo kontroli.

(10) Lai nodrošinātu pareizu riska pārvaldību tādu IKT pakalpojumu sniegšanā, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, politikā būtu jāietver informācija par līgumisko vienošanos īstenošanu, uzraudzību un pārvaldību, tostarp attiecīgā gadījumā konsolidētā un subkonsolidētā līmenī. Tas ietver prasības attiecībā uz līguma klauzulām par finanšu vienību un trešo personu, kas sniedz IKT pakalpojumus, savstarpējām saistībām, kuras būtu jāizklāsta rakstiski. Lai nodrošinātu efektīvu uzraudzību un veicinātu noturību darījumdarbības modeļa vai uzņēmējdarbības vides izmaiņu gadījumā, politikā būtu jānodrošina finanšu vienību vai iecelto trešo personu un kompetento iestāžu tiesības uz pārbaudēm un piekļuvi informācijai, kā arī būtu sīkāk jāprecizē atkāpšanās stratēģijas un izbeigšanas procesi.

(11) Ciktāl personas datus apstrādā trešās personas, kas sniedz IKT pakalpojumus, šī politika un jebkādas līgumiskas vienošanās neskar Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 ([2]) noteiktos pienākumus, kurus tām vajadzētu papildināt, piemēram, par to, ka ir jābūt noslēgtam rakstiskam līgumam, kurā aprakstīta personas datu apstrāde, par prasību nodrošināt personas datu apstrādes drošību un izklāstot visus pārējos minētajā regulā prasītos elementus.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Eiropas uzraudzības iestāžu apvienotā komiteja, kas minēta Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 ([3]) 54. pantā, Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1094/2010 ([4]) 54. pantā un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1095/2010 ([5]) 54. pantā, ir rīkojusi atklātu sabiedrisko apspriešanu par regulatīvajiem tehniskajiem standartiem, uz kuriem balstīta šī regula, analizējusi ierosināto standartu potenciālās izmaksas un radītos ieguvumus un lūgusi padomu Banku nozares ieinteresēto personu grupai, kas izveidota saskaņā ar Regulas (ES) Nr. 1093/2010 37. pantu, Apdrošināšanas un pārapdrošināšanas nozares ieinteresēto personu grupai un Aroda pensiju nozares ieinteresēto personu grupai, kas izveidotas saskaņā ar Regulas (ES) Nr. 1094/2010 37. pantu, un Vērtspapīru un tirgu nozares ieinteresēto personu grupai, kas izveidota saskaņā ar Regulas (ES) Nr. 1095/2010 37. pantu.

(13) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([6]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas sniedza atzinumu 2024. gada 24. janvārī,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Vispārējais riska profils un sarežģītība

Politikā par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, ("politika") ņem vērā finanšu vienības lielumu un vispārējo riska profilu, kā arī tās pakalpojumu, darbību un operāciju lielākas vai mazākas sarežģītības būtību, mērogu un elementus, tostarp elementus, kas attiecas uz:

a) IKT pakalpojumu veidu, kas iekļauts līgumiskajā vienošanās par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, ("līgumiskā vienošanās") starp finanšu vienību un trešo personu, kas sniedz IKT pakalpojumus;

b) trešās personas, kas sniedz IKT pakalpojumus, atrašanās vietu vai tās mātesuzņēmuma atrašanās vietu;

c) to, vai IKT pakalpojumus, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas, nodrošina trešā persona, kas sniedz IKT pakalpojumus un atrodas dalībvalstī vai trešā valstī, ņemot vērā arī vietu, no kuras tiek sniegti IKT pakalpojumi, un vietu, kur dati tiek apstrādāti un glabāti;

d) ar trešo personu, kas sniedz IKT pakalpojumus, kopīgoto datu veidu;

e) to, vai trešā persona, kas sniedz IKT pakalpojumus, ir tās pašas grupas locekle, kurā ietilpst finanšu vienība, kurai tiek sniegti pakalpojumi;

([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).

([6]) 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).

f) tādu trešo personu, kas sniedz IKT pakalpojumus, izmantošanu, kuras ir saņēmušas atļauju, ir reģistrētas vai kuras uzrauga vai pārrauga dalībvalsts kompetentā iestāde vai uz kurām attiecas Regulas (ES) 2022/2554 V nodaļas II iedaļā paredzētā pārraudzības sistēma, un tādu trešo personu, kas sniedz IKT pakalpojumus, izmantošanu, uz kurām viss iepriekšminētais neattiecas;

g) tādu trešo personu, kas sniedz IKT pakalpojumus, izmantošanu, kuras ir saņēmušas atļauju, ir reģistrētas vai uz kurām attiecas uzraudzības iestādes uzraudzība vai pārraudzība trešā valstī, un tādu trešo personu, kas sniedz IKT pakalpojumus, izmantošanu, uz kurām viss iepriekšminētais neattiecas;

h) to, vai IKT pakalpojumu sniegšana, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas, ir koncentrēta uz vienu trešo personu, kas sniedz IKT pakalpojumus, vai nelielu skaitu šādu pakalpojumu sniedzēju;

i) IKT pakalpojumu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, pārnesamību citai trešai personai, kas sniedz IKT pakalpojumus, tostarp tehnoloģiju specifikas dēļ;

j) IKT pakalpojumu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, sniegšanas traucējumu iespējamo ietekmi uz finanšu vienības darbību nepārtrauktību un tās pakalpojumu pieejamību.

2. pants

Piemērošana grupai

Ja šo regulu piemēro subkonsolidēti vai konsolidēti, mātesuzņēmums, kas ir atbildīgs par konsolidēto vai subkonsolidēto finanšu pārskatu sniegšanu grupai, nodrošina, ka politika tiek konsekventi īstenota visās finanšu vienībās, kas ir daļa no grupas, un ir atbilstīga šīs regulas efektīvai piemērošanai visos attiecīgajos grupas līmeņos.

3. pants

Pārvaldības kārtība

1. Vadības struktūra pārskata politiku vismaz reizi gadā un vajadzības gadījumā to atjaunina. Izmaiņas politikā īsteno laikus un, tiklīdz tas ir iespējams, saskaņā ar attiecīgajām līgumiskajām vienošanām. Finanšu vienība dokumentē plānoto īstenošanas grafiku.

2. Politikā nosaka metodiku vai atsaucas uz metodiku, ar ko nosaka, kuri IKT pakalpojumi atbalsta kritiski svarīgas vai svarīgas funkcijas. Politikā arī norāda, kad šis novērtējums ir jāveic un jāpārskata.

3. Politikā skaidri nosaka iekšējos pienākumus attiecībā uz attiecīgo līgumisko vienošanos apstiprināšanu, pārvaldību, kontroli un dokumentēšanu un nodrošina, ka finanšu vienībā tiek uzturētas atbilstīgas prasmes, pieredze un zināšanas, lai efektīvi pārraudzītu attiecīgās līgumiskās vienošanās, tostarp IKT pakalpojumus, ko sniedz saskaņā ar minētajām vienošanām.

4. Neskarot finanšu vienības galīgo atbildību efektīvi pārraudzīt attiecīgās līgumiskās vienošanās, politika paredz novērtēt, ka trešai personai, kas sniedz IKT pakalpojumus, ir pietiekami resursi, lai nodrošinātu, ka finanšu vienība atbilst visām tās juridiskajām un regulatīvajām prasībām attiecībā uz IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, kas tiek nodrošinātas.

5. Politikā skaidri norāda augstākās vadības funkciju vai locekli, kas ir atbildīgs par attiecīgo līgumisko vienošanos uzraudzību. Politikā precizē, kā minētā augstākās vadības funkcija vai loceklis sadarbojas ar kontroles funkcijām, ja vien tas nav daļa no tām, un nosaka kārtību, kādā jāziņo vadības struktūrai, tostarp ziņojamās informācijas veidu un iesniedzamos dokumentus. Tajā arī nosaka šādas ziņošanas biežumu.

6. Politika nodrošina, ka līgumiskās vienošanās ir saskanīgas ar:

a) IKT riska pārvaldības sistēmu, kas minēta Regulas (ES) 2022/2554 6. pantā;

b) informācijas drošības politiku, kas minēta Regulas (ES) 2022/2554 9. panta 4. punktā;

c) IKT darbības nepārtrauktības politiku, kas minēta Regulas (ES) 2022/2554 11. pantā;

d) prasībām par incidentu paziņošanu, kā izklāstīts Regulas (ES) 2022/2554 19. pantā.

7. Politika paredz, ka IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, pārbauda neatkarīgi un iekļauj revīzijas plānā.

8. Politikā skaidri norāda, ka līgumiskās vienošanās:

a) neatbrīvo finanšu vienību un tās vadības struktūru no tās regulatīvajām saistībām un pienākumiem pret klientiem;

b) nekavē finanšu vienības efektīvu uzraudzību un nav pretrunā nevienam uzraudzības ierobežojumam attiecībā uz pakalpojumiem un darbībām;

c) ir tādas, ar kurām jāpieprasa, lai trešās personas, kas sniedz IKT pakalpojumus, sadarbotos ar kompetentajām iestādēm;

d) ir tādas, ar kurām jāpieprasa, lai finanšu vienībai, tās revidentiem un kompetentajām iestādēm būtu efektīva piekļuve datiem un telpām, kas saistītas ar tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas.

4. pants

Galvenie aprites cikla posmi attiecībā uz līgumisko vienošanos pieņemšanu un izmantošanu

Politikā norāda prasības, tostarp noteikumus, pienākumus un procesus, katram līgumiskās vienošanās aprites cikla galvenajam posmam, aptverot vismaz šādus aspektus:

a) vadības struktūras pienākumi, tostarp attiecīgā gadījumā tās iesaiste lēmumu pieņemšanas procesā par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus;

b) līgumisko vienošanos, tostarp riska novērtējuma, pienācīgas rūpības, kā noteikts 5. un 6. pantā, plānošana un apstiprināšanas process attiecībā uz jaunām vai būtiskām izmaiņām līgumiskajās vienošanās, kā noteikts 8. panta 4. punktā;

c) uzņēmējdarbības vienību, iekšējās kontroles un citu attiecīgu vienību iesaiste attiecībā uz līgumiskajām vienošanām;

d) regulas 7., 8. un 9. pantā minēto līgumisko vienošanos īstenošana, uzraudzība un pārvaldība, tostarp attiecīgā gadījumā konsolidētā un subkonsolidētā līmenī;

e) dokumentācija un uzskaite, ņemot vērā Regulas (ES) 2022/2554 28. panta 3. punktā noteiktās prasības attiecībā uz informācijas reģistru;

f) atkāpšanās stratēģijas un izbeigšanas procesi, kā noteikts 10. pantā.

5. pants

Ex *ante* riska novērtējums

1. Politikā paredz, ka finanšu vienības uzņēmējdarbības vajadzības tiek noteiktas pirms līgumiskas vienošanās noslēgšanas.

2. Politikā paredz, ka riska novērtējums tiek veikts finanšu vienības līmenī un attiecīgā gadījumā konsolidētā un subkonsolidētā līmenī pirms līgumiskas vienošanās noslēgšanas.

Riska novērtējumā ņem vērā visas attiecīgās prasības, kas noteiktas Regulā (ES) 2022/2554 un piemērojamajos Savienības nozaru tiesību aktos. Tajā jo īpaši ņem vērā to IKT pakalpojumu sniegšanas ietekmi uz finanšu vienību, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, un visus riskus, ko rada tādu IKT pakalpojumu sniegšana, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, tostarp:

a) operacionālos riskus;

b) juridiskos riskus;

c) IKT riskus;

d) reputācijas riskus;

e) riskus, kas saistīti ar konfidenciālu datu vai personas datu aizsardzību;

f) riskus, kas saistīti ar datu pieejamību;

g) riskus, kas saistīti ar vietu, kur dati tiek apstrādāti un glabāti;

h) riskus, kas saistīti ar trešās personas, kas sniedz IKT pakalpojumus, atrašanās vietu;

i) IKT koncentrācijas riskus vienības līmenī.

6. pants

Pienācīga rūpība

1. Politikā precizē piemērotu un samērīgu procesu potenciālo trešo personu, kas sniedz IKT pakalpojumus, atlasei un novērtēšanai, ņemot vērā to, vai trešā persona, kas sniedz IKT pakalpojumus, ir IKT pakalpojumu sniedzējs grupas iekšienē, un pieprasa, lai finanšu vienība pirms līgumiskas vienošanās noslēgšanas novērtētu, vai trešā persona, kas sniedz IKT pakalpojumus:

a) ir tāda, kurai ir darījumdarbības reputācija, pietiekamas spējas, speciālās zināšanas un atbilstoši finanšu resursi, cilvēkresursi un tehniskie resursi, informācijas drošības standarti, atbilstoša organizatoriskā struktūra, riska pārvaldība un iekšējā kontrole un attiecīgā gadījumā nepieciešamā(-ās) atļauja(-as) vai reģistrācija(-as), lai uzticami un profesionāli sniegtu IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgo vai svarīgo funkciju;

b) spēj uzraudzīt attiecīgo tehnoloģiju attīstību un apzināt IKT drošības vadošo praksi un attiecīgā gadījumā to īstenot, lai izveidotu efektīvu un stabilu digitālās darbības noturības satvaru;

c) izmanto vai plāno izmantot IKT apakšuzņēmējus, lai sniegtu IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas vai to būtiskas daļas;

d) atrodas trešā valstī vai apstrādā vai glabā datus trešā valstī un, ja tas tā ir, vai šāda prakse ietekmē darbības vai reputācijas risku līmeni, vai risku, ka to ietekmē ierobežojoši pasākumi, tostarp embargo un sankcijas, kas var ietekmēt trešās personas, kas sniedz IKT pakalpojumus, spēju sniegt IKT pakalpojumus vai finanšu vienības spēju saņemt minētos IKT pakalpojumus;

e) piekrīt līgumiskām vienošanām, kas nodrošina, ka ir faktiski iespējams veikt trešās personas, kas sniedz IKT pakalpojumus, revīzijas, tostarp uz vietas, ko veic pati finanšu vienība, ieceltas trešās personas un kompetentās iestādes;

f) rīkojas ētiski un sociāli atbildīgi, ievēro cilvēktiesības un bērnu tiesības, tostarp bērnu darba aizliegumu, ievēro piemērojamos vides aizsardzības principus un nodrošina pienācīgus darba apstākļus.

2. Politikā precizē nepieciešamo ticamības līmeni attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, riska pārvaldības sistēmas efektivitāti attiecībā uz IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešā persona, kas sniedz IKT pakalpojumus. Ar politiku nosaka, ka pienācīgas rūpības process ietver novērtējumu par riska mazināšanas un darbības nepārtrauktības pasākumu esību un to, kā tiek nodrošināta to darbība trešās personas, kas sniedz IKT pakalpojumus, ietvaros.

3. Ar politiku nosaka pienācīgas rūpības procesu potenciālo trešo personu, kas sniedz IKT pakalpojumus, atlasei un novērtēšanai un norāda, kuri no turpmāk minētajiem elementiem jāizmanto, lai nodrošinātu vajadzīgo ticamības līmeni attiecībā uz trešās personas, kas sniedz IKT pakalpojumus, sniegumu:

a) revīzijas vai neatkarīgi novērtējumi, ko veic pati finanšu vienība vai ko veic tās vārdā;

b) neatkarīgas revīzijas ziņojumu izmantošana, kuri sagatavoti pēc trešās personas, kas sniedz IKT pakalpojumus, pieprasījuma;

c) revīzijas ziņojumu izmantošana, ko sagatavojusi trešās personas, kas sniedz IKT pakalpojumus, iekšējās revīzijas funkcija;

d) attiecīgu trešās personas sertifikātu izmantošana;

e) citas attiecīgās finanšu vienībai pieejamās informācijas vai citas informācijas, ko sniegusi trešā persona, kas sniedz IKT pakalpojumus, izmantošana.

4. Finanšu vienības nodrošina pienācīgu ticamības līmeni attiecībā uz trešās personas, kas sniedz IKT pakalpojumus, sniegumu, ņemot vērā 3. punkta a) līdz e) apakšpunktā uzskaitītos elementus. Attiecīgā gadījumā izmanto vairāk nekā vienu minētajos punktos uzskaitīto elementu.

7. pants

Interešu konflikti

1. Politikā precizē atbilstīgos pasākumus, lai identificētu, novērstu un pārvaldītu faktiskus vai potenciālus interešu konfliktus, kas rodas, izmantojot trešo personu, kas sniedz IKT pakalpojumus, un kuri jāveic pirms attiecīgu līgumisku vienošanos noslēgšanas, un paredz šādu interešu konfliktu pastāvīgu uzraudzību.

2. Ja IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, sniedz IKT pakalpojumu sniedzēji, kuri pieder vienai grupai, politikā norāda, ka lēmumi par IKT pakalpojumu nosacījumiem, tostarp finanšu nosacījumiem, ir jāpieņem objektīvi.

8. pants

Līguma klauzulas

1. Politikā norāda, ka attiecīgā līgumiskā vienošanās ir jānoslēdz rakstveidā un tajā jāiekļauj visi elementi, kas minēti Regulas (ES) 2022/2554 30. panta 2. un 3. punktā. Politikā ietver arī elementus attiecībā uz Regulas (ES) 2022/2554 1. panta 1. punkta a) apakšpunktā minētajām prasībām, kā arī attiecīgā gadījumā citiem attiecīgajiem Savienības un valsts tiesību aktiem.

2. Politikā norāda, ka attiecīgajās līgumiskajās vienošanās ietver finanšu vienības tiesības piekļūt informācijai, veikt pārbaudes un revīzijas un veikt IKT testus. Šajā nolūkā politikā pieprasa, lai finanšu vienība, neskarot finanšu vienības galīgo atbildību, izmantotu šādas metodes:

a) savu iekšējo revīziju vai revīziju, ko veic iecelta trešā persona;

b) attiecīgā gadījumā apvienotas revīzijas un apvienotu IKT testēšanu, tostarp draudu vadītu ielaušanās testēšanu, ko organizē kopīgi ar citām līgumslēdzējām finanšu vienībām vai uzņēmumiem, kuri izmanto IKT pakalpojumus, ko sniedz tā pati trešā persona, kas sniedz IKT pakalpojumus, un ko veic minētās līgumslēdzējas finanšu vienības vai uzņēmumi vai to iecelta trešā persona;

c) attiecīgā gadījumā – trešo personu izsniegtos sertifikātus;

d) attiecīgā gadījumā iekšējās revīzijas ziņojumus vai trešās personas sagatavotus revīzijas ziņojumus, ko trešā persona, kas sniedz IKT pakalpojumus, ir darījusi pieejamus.

3. Finanšu vienība laika gaitā nepaļaujas tikai uz 2. punkta c) apakšpunktā minētajiem sertifikātiem vai minētā punkta d) apakšpunktā minētajiem revīzijas ziņojumiem. Politika ļauj izmantot 2. punkta c) un d) apakšpunktā minētās metodes tikai tad, ja finanšu vienība:

a) ir apmierināta ar trešās personas, kas sniedz IKT pakalpojumus, revīzijas plānu attiecībā uz attiecīgajām līgumiskajām vienošanām;

b) nodrošina, ka sertifikātu vai revīzijas ziņojumu tvērums aptver tās identificētās sistēmas un galvenos kontroles pasākumus, kā arī atbilstību attiecīgajām normatīvajām prasībām;

c) pastāvīgi rūpīgi izvērtē sertifikātu vai revīzijas ziņojumu saturu un pārbauda, vai sertifikāti vai ziņojumi nav novecojuši;

d) nodrošina, ka galvenās sistēmas un kontroles ir ietvertas sertifikāta vai revīzijas ziņojuma turpmākajās versijās;

e) ir apmierināta ar sertificējošās vai revīzijas veicējas puses piemērotību;

f) ir apmierināta ar to, ka sertifikāti ir izsniegti un revīzijas tiek veiktas saskaņā ar plaši atzītiem attiecīgiem profesionāliem standartiem un ietver galveno ieviesto kontroļu darbības efektivitātes pārbaudi;

g) ir tāda, kurai ir līgumiskas tiesības tik bieži, cik tas ir pamatoti un likumīgi no riska pārvaldības viedokļa, pieprasīt izmaiņas sertifikātu vai revīzijas ziņojumu tvērumā, attiecinot tos uz citām attiecīgām sistēmām un kontrolēm;

h) ir tāda, kurai ir līgumiskas tiesības pēc saviem ieskatiem veikt individuālas un apvienotas revīzijas attiecībā uz līgumiskajām vienošanām un īstenot šīs tiesības saskaņā ar noteikto biežumu.

4. Politika nodrošina, ka līgumiskās vienošanās būtiskas izmaiņas ir jāformalizē rakstiskā dokumentā, ko datē un paraksta visas puses, un tajā norāda līgumisko vienošanos atjaunošanas procesu.

9. pants

Līgumisko vienošanos uzraudzība

1. Politikā paredz, ka līgumiskajās vienošanās precizē pasākumus un galvenos rādītājus, lai pastāvīgi uzraudzītu trešo personu, kas sniedz IKT pakalpojumus, sniegumu, tostarp pasākumus, lai uzraudzītu atbilstību prasībām attiecībā uz datu un informācijas konfidencialitāti, pieejamību, integritāti un autentiskumu un trešo personu, kas sniedz IKT pakalpojumus, atbilstību finanšu vienības attiecīgajai politikai un procedūrām. Politikā norāda arī pasākumus, ko piemēro, ja nav izpildītas pakalpojumu līmeņa vienošanās, tostarp attiecīgā gadījumā līgumsodus.

2. Politikā norāda, kā finanšu vienībai ir jānovērtē, vai trešās personas, kas sniedz IKT pakalpojumus, kuras izmanto IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, atbilst atbilstošiem darbības un kvalitātes standartiem saskaņā ar līgumisko vienošanos un pašas finanšu vienības politiku. Politika jo īpaši nodrošina to, ka:

a) trešās personas, kas sniedz IKT pakalpojumus, sniedz finanšu vienībai atbilstīgus ziņojumus par savām darbībām un pakalpojumiem, tostarp periodiskus ziņojumus, ziņojumus par incidentiem, pakalpojumu sniegšanas ziņojumus, ziņojumus par IKT drošību un ziņojumus par darbības nepārtrauktības pasākumiem un testēšanu;

b) trešo personu, kas sniedz IKT pakalpojumus, sniegums tiek novērtēts, izmantojot galvenos snieguma rādītājus, galvenos kontroles rādītājus, revīzijas, pašsertifikācijas un neatkarīgas pārbaudes saskaņā ar finanšu vienības IKT riska pārvaldības sistēmu;

c) finanšu vienība saņem citu būtisku informāciju no trešām personām, kas sniedz IKT pakalpojumus;

d) finanšu vienībai attiecīgā gadījumā ir paziņots par incidentiem, kas saistīti ar IKT, un par darbības vai drošības incidentiem, kas saistīti ar maksājumiem;

e) tiek veikta neatkarīga pārbaude un revīzijas, kurās pārbauda atbilstību tiesiskajām un normatīvajām prasībām un politikai.

3. Politikā norāda, ka 2. punktā minētais novērtējums ir jādokumentē un tā rezultāti jāizmanto, lai atjauninātu 6. pantā minēto finanšu vienības riska novērtējumu.

4. Politikā nosaka atbilstīgus pasākumus, kas finanšu vienībai ir jāpieņem, ja tā konstatē trūkumus, tostarp ar IKT saistītus incidentus un ar maksājumiem saistītus darbības vai drošības incidentus, trešo personu, kas sniedz IKT pakalpojumus, tādu IKT pakalpojumu sniegšanā, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, vai attiecībā uz atbilstību līgumiskām vienošanām vai juridiskajām prasībām. Tajā arī norāda, kā jāuzrauga šādu pasākumu īstenošana, lai nodrošinātu to efektīvu ievērošanu noteiktā termiņā, ņemot vērā trūkumu būtiskumu.

10. pants

Atkāpšanās no līgumiskas vienošanās un tās izbeigšana

Politikā ietver prasības par dokumentētu atkāpšanās plānu attiecībā uz katru līgumisku vienošanos un dokumentētā atkāpšanās plāna periodisku pārskatīšanu un testēšanu. Izstrādājot atkāpšanās plānu, ņem vērā turpmāk minēto:

a) neparedzētus un pastāvīgus pakalpojumu pārtraukumus;

b) neatbilstīgu vai nesekmīgu pakalpojumu sniegšanu;

c) negaidītu līgumiskās vienošanās izbeigšanu.

Atkāpšanās plāns ir reālistisks, īstenojams, balstīts uz ticamiem scenārijiem un pamatotiem pieņēmumiem, un tam ir plānots īstenošanas grafiks, kas ir saderīgs ar līgumiskās vienošanās noteikumiem par atkāpšanos no līgumiskas vienošanās un tās izbeigšanu.

11. 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 13. martā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN