Euroopa Liidu
Teataja

ET
L-seeria

2024/1773

25.6.2024

KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2024/1773,

13. märts 2024,

millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, et täpsustada põhimõtete üksikasjalikku sisu seoses lepingutega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrust (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011, ([1]) eriti selle artikli 28 lõike 10 kolmandat lõiku,

ning arvestades järgmist:

(1) Määrusega (EL) 2022/2554 kehtestatud finantssektori digitaalse tegevuskerksuse raamistiku kohaselt peavad finantssektori ettevõtjad sätestama kolmandast isikust tuleneva IKT-riski juhtimise teatavad peamised põhimõtted, mis on eriti olulised, kui finantssektori ettevõtjad kasutavad kolmandast isikust IKT-teenuste osutajaid, et toetada oma kriitilise tähtsusega või olulisi funktsioone.

(2) Finantssektori ettevõtjad peavad oma IKT-riski juhtimise raamistiku osana võtma vastu kolmandast isikust tuleneva IKT-riski strateegia ja vaatama selle korrapäraselt läbi. Kooskõlas määruse (EL) 2022/2554 artikli 28 lõikega 2 peab see strateegia hõlmama kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise põhimõtteid. Seda kohaldatakse individuaalselt ning asjakohasel juhul allkonsolideeritud ja konsolideeritud alusel.

(3) Finantssektori ettevõtjate suurus, struktuur ja sisemine korraldus ning nende tegevuse ja toimingute laad ja keerukus on väga erinevad. Seda mitmekesisust tuleb arvesse võtta, kehtestades samal ajal teatavad regulatiivsed põhinõuded, mis on asjakohased kõigi finantssektori ettevõtjate puhul, kui need töötavad välja põhimõtteid, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist (edaspidi „põhimõtted“), ning tagada, et neid nõudeid kohaldatakse proportsionaalselt.

(4) Kui finantssektori ettevõtjad kuuluvad kontserni, peaks emaettevõtja, kes vastutab kontserni konsolideeritud või allkonsolideeritud finantsaruannete esitamise eest, tagama, et põhimõtteid rakendatakse kontsernis järjepidevalt ja sidusalt.

(5) Põhimõtete kohaldamisel tuleks kontsernisiseseid IKT-teenuste osutajaid, sealhulgas neid, kes on täielikult või ühiselt samasse finantsinstitutsioonide kaitseskeemi kuuluvate finantssektori ettevõtjate omandis, käsitada kolmandast isikust IKT-teenuste osutajatena. Kontsernisisestest IKT-teenuste osutajatest tulenevad riskid võivad olla erinevad, kuid nende suhtes kohaldatavad nõuded on samad vastavalt määrusele (EL) 2022/2554. Samamoodi tuleks põhimõtteid kohaldada alltöövõtjate suhtes, kes osutavad kolmandast isikust IKT-teenuste osutajatele kriitilise tähtsusega või olulisi funktsioone või nende olulisi osi toetavaid IKT-teenuseid, kui on olemas kolmandast isikust IKT-teenuste osutajate ahel.

(6) Juhtorgani lõplik vastutus finantssektori ettevõtja IKT-riski juhtimise eest on üldpõhimõte, mida kohaldatakse ka kolmandast isikust IKT-teenuste osutajate kasutamise korral. See vastutus peaks väljenduma juhtorgani pidevas osalemises IKT-riskide juhtimise kontrollis ja jälgimises, sealhulgas põhimõtete vastuvõtmises ja vähemalt kord aastas läbivaatamises.

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

(7) Selleks et tagada asjakohane aruandlus juhtorganile, tuleks põhimõtetega selgelt kindlaks määrata kolmandast isikust IKT-teenuste osutajate osutatavaid, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste, sealhulgas määruse (EL) 2022/2554 artikli 28 lõike 1 punktis a osutatud lepingute alusel osutatavate IKT-teenuste kasutamist käsitlevate lepingute heakskiitmise, haldamise, kontrolli ja dokumenteerimisega seotud sisemised kohustused.

(8) Selleks et võtta arvesse kõiki võimalikke riske, mis võivad tekkida kriitilise tähtsusega või olulist funktsiooni toetavate IKT-teenuste lepingute sõlmimisel, peaks põhimõtete struktuur järgima kolmandast isikust teenuseosutajatega sõlmitud lepingute elutsükli iga põhietapi kõiki etappe.

(9) Tuvastatud riskide maandamiseks tuleks põhimõtetega kindlaks määrata lepingute kavandamine, sealhulgas riskihindamine, hoolsuskohustus ja kõnealuste lepingute uute või oluliste muudatuste heakskiitmise protsess. Selleks et juhtida võimalikke riske enne kolmandast isikust IKT-teenuste osutajaga lepingu sõlmimist, tuleks põhimõtetega kindlaks määrata asjakohane ja proportsionaalne protsess potentsiaalsete kolmandast isikust IKT-teenuste osutajate valimiseks ja nende sobivuse hindamiseks ning näha ette, et finantssektori ettevõtja peab võtma arvesse mitteammendavat loetelu elementidest, mis kolmandast isikust IKT-teenuste osutajatel peaksid olema. Loetelu peaks sisaldama elemente, mis on seotud teenuseosutaja mainega, finants-, inim- ja tehniliste ressurssidega, infoturbega, organisatsioonilise struktuuriga, sealhulgas riskijuhtimine, ja sisekontrolliga.

(10) Selleks et tagada usaldusväärne riskijuhtimine kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamisel kolmandast isikust IKT-teenuste osutajate poolt, peaksid põhimõtted sisaldama teavet lepingute rakendamise, jälgimise ja haldamise kohta, sealhulgas asjakohasel juhul konsolideeritud ja allkonsolideeritud tasandil. See hõlmab nõudeid finantssektori ettevõtjate ja kolmandast isikust IKT-teenuste osutajate vastastikuseid kohustusi käsitlevate lepingutingimuste kohta, mis tuleks sätestada kirjalikult. Selleks et tagada tõhus järelevalve ja edendada vastupidavust ärimudelis või ärikeskkonnas toimuvate muutuste korral, tuleks põhimõtetega tagada finantssektori ettevõtjatele või määratud kolmandatele isikutele ja pädevatele asutustele õigus teha kontrolle ja pääseda ligi teabele ning täpsustada ka väljumisstrateegiaid ja lõpetamisprotsesse.

(11) Kui isikuandmeid töötlevad kolmandast isikust IKT-teenuste osutajad, ei tohiks põhimõtted ega mis tahes leping piirata Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 ([2]) tulenevate kohustuste kohaldamist, vaid peaksid neid täiendama (nt isikuandmete töötlemist kirjeldav kirjalik leping, nõue tagada isikuandmete töötlemise turvalisus) ja neis tuleks kindlaks määrata kõik muud kõnealuse määrusega nõutavad elemendid.

([2]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016.aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Euroopa Parlamendi ja nõukogu määruse (EL) nr 1093/2010 ([3]) artiklis 54, Euroopa Parlamendi ja nõukogu määruse (EL) nr 1094/2010 ([4]) artiklis 54 ning Euroopa Parlamendi ja nõukogu määruse (EL) nr 1095/2010 ([5]) artiklis 54 osutatud Euroopa järelevalveasutuste ühiskomitee on korraldanud käesoleva määruse aluseks olevate regulatiivsete tehniliste standardite eelnõude kohta avalikud konsultatsioonid, analüüsinud kavandatud standardite võimalikke kulusid ja kasu ning küsinud nõu määruse (EL) nr 1093/2010 artikli 37 kohaselt loodud pangandussektori sidusrühmade kogult, määruse (EL) nr 1094/2010 artikli 37 kohaselt loodud kindlustuse ja edasikindlustuse sidusrühmade kogult ja tööandjapensionide sidusrühmade kogult ning määruse (EL) nr 1095/2010 artikli 37 kohaselt loodud väärtpaberituru sidusrühmade kogult,

(13) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([6]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 24. jaanuaril 2024,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Üldine riskiprofiil ja keerukus

Kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise põhimõtetes (edaspidi „põhimõtted“) tuleb võtta arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja elemente, mille tõttu keerukus suureneb või väheneb, sealhulgas elemente, mis on seotud järgmisega:

a) selliste IKT-teenuste liik, mis on sätestatud finantssektori ettevõtja ja kolmandast isikust IKT-teenuste osutaja vahel sõlmitud lepingus, mis käsitleb kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist (edaspidi „leping“);

b) kolmandast isikust IKT-teenuste osutaja või tema emaettevõtja asukoht;

c) kas kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid osutab liikmesriigis või kolmandas riigis asuv kolmandast isikust IKT-teenuste osutaja, võttes arvesse ka IKT-teenuste osutamise asukohta ning andmete töötlemise ja säilitamise asukohta;

d) kolmandast isikust IKT-teenuste osutajaga jagatud andmete laad;

e) kas kolmandast isikust IKT-teenuste osutaja kuulub samasse kontserni, kuhu kuulub ka finantssektori ettevõtja, kellele teenuseid osutatakse;

([3]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1094/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/79/EÜ (ELT L 331, 15.12.2010, lk 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1095/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ (ELT L 331, 15.12.2010, lk 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) selliste kolmandast isikust IKT-teenuste osutajate kasutamine, kellele on andnud tegevusloa või kelle on registreerinud või kelle üle teeb järelevalvet või järelevaatamist liikmesriigi pädev asutus või kelle suhtes kohaldatakse määruse (EL) 2022/2554 V peatüki II jao kohast järelevaatamisraamistikku, ning selliste kolmandast isikust IKT-teenuste osutajate kasutamine, kellele ei ole andnud tegevusluba või keda ei ole registreerinud või kelle üle ei tee järelevalvet või järelevaatamist liikmesriigi pädev asutus või kelle suhtes ei kohaldata määruse (EL) 2022/2554 V peatüki II jao kohast järelevaatamisraamistikku;

g) selliste kolmandast isikust IKT-teenuste osutajate kasutamine, kellele on andnud tegevusloa või kelle on registreerinud või kelle üle teeb järelevalvet või järelevaatamist kolmanda riigi järelevalveasutus, ning selliste kolmandast isikust IKT-teenuste osutajate kasutamine, kellele ei ole andnud tegevusluba või keda ei ole registreerinud või kelle üle ei tee järelevalvet või järelevaatamist kolmanda riigi järelevalveasutus;

h) kas kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamine on koondunud ühe kolmandast isikust IKT-teenuste osutaja või väikese arvu selliste teenuseosutajate kätte;

i) kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste ülekantavus teisele kolmandast isikust IKT-teenuste osutajale, sealhulgas tehnoloogia eripära tõttu;

j) kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamise häirete võimalik mõju finantssektori ettevõtja talitluspidevusele ja tema teenuste kättesaadavusele.

Artikkel 2

Kohaldamine kontserni tasandil

Kui käesolevat määrust kohaldatakse allkonsolideeritud või konsolideeritud alusel, tagab emaettevõtja, kes vastutab kontserni konsolideeritud või allkonsolideeritud finantsaruannete esitamise eest, et põhimõtteid rakendatakse järjepidevalt kõigis kontserni kuuluvates finantssektori ettevõtjates ja et see on piisav käesoleva määruse tulemuslikuks kohaldamiseks kontserni kõigil asjaomastel tasanditel.

Artikkel 3

Juhtimiskord

1. Juhtorgan vaatab põhimõtted läbi vähemalt kord aastas ja vajaduse korral ajakohastab neid. Põhimõtetes tehtud muudatused rakendatakse õigeaegselt ja niipea, kui see on asjaomaste lepingute raames võimalik. Finantssektori ettevõtja dokumenteerib kavandatud rakendamise ajakava.

2. Põhimõtetega kehtestatakse metoodika, mille alusel määratakse kindlaks, millised IKT-teenused toetavad kriitilise tähtsusega või olulisi funktsioone, või osutatakse sellele metoodikale. Põhimõtetega määratakse kindlaks ka, millal hindamine tuleb läbi viia ja läbi vaadata.

3. Põhimõtetega määratakse selgelt kindlaks asjaomaste lepingute heakskiitmise, haldamise, kontrolli ja dokumenteerimisega seotud sisemised kohustused ning tagatakse, et finantssektori ettevõtjal on asjakohased oskused, kogemused ja teadmised, et teha tulemuslikku järelevaatamist asjaomaste lepingute üle, sealhulgas nende lepingute alusel osutatavate IKT-teenuste üle.

4. Ilma et see piiraks finantssektori ettevõtja lõplikku vastutust asjaomaste lepingute tulemusliku järelevaatamise eest, nõutakse põhimõtetega, et kolmandast isikust IKT-teenuste osutajal oleks piisavad ressursid tagamaks, et finantssektori ettevõtja täidab kõiki oma õiguslikke ja regulatiivseid nõudeid seoses osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenustega.

5. Põhimõtetega määratakse selgelt kindlaks asjaomaste lepingute seire eest vastutava kõrgema juhtkonna roll või liige. Põhimõtetega määratakse kindlaks, kuidas see kõrgema juhtkonna roll või liige teeb koostööd kontrollifunktsioonidega, välja arvatud juhul, kui ta osaleb nendes, ning juhtorganile aruandluse esitamise ahelad, sealhulgas esitatava teabe laad ja esitatavad dokumendid. Samuti määratakse kindlaks sellise aruandluse sagedus.

6. Põhimõtetega tagatakse, et lepingud on kooskõlas järgmisega:

a) määruse (EL) 2022/2554 artiklis 6 osutatud IKT-riski juhtimise raamistik;

b) määruse (EL) 2022/2554 artikli 9 lõikes 4 osutatud infoturbekord;

c) määruse (EL) 2022/2554 artiklis 11 osutatud IKT talitluspidevuse põhimõtted;

d) määruse (EL) 2022/2554 artiklis 19 osutatud intsidentidest teavitamise nõuded.

7. Põhimõtetega nõutakse, et kolmandast isikust IKT-teenuste osutajate osutatavad kriitilise tähtsusega või olulisi funktsioone toetavad IKT-teenused vaadatakse sõltumatult läbi ja lisatakse auditikavva.

8. Põhimõtetes märgitakse selgesõnaliselt, et lepingud:

a) ei vabasta finantssektori ettevõtjat ega selle juhtorganit regulatiivsetest kohustustest ja vastutusest klientide ees;

b) ei tohi takistada tõhusat järelevalvet finantssektori ettevõtja üle ega rikkuda järelevalvepiiranguid teenuste ja toimingute suhtes;

c) peavad ette nägema, et kolmandast isikust IKT-teenuste osutajad teevad pädevate asutustega koostööd;

d) peavad ette nägema, et finantssektori ettevõtjal, tema audiitoritel ja pädevatel asutustel on tegelik juurdepääs andmetele ja ruumidele, mis on seotud kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamisega.

Artikkel 4

Lepingute sõlmimise ja kasutamise elutsükli põhietapid

Põhimõtetega määratakse kindlaks nõuded, sealhulgas eeskirjad, kohustused ja protsessid lepingu elutsükli iga põhietapi jaoks, hõlmates vähemalt järgmist:

a) juhtorgani kohustused, sealhulgas asjakohasel juhul tema osalemine otsustusprotsessis kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise üle;

b) lepingute kavandamine, sealhulgas riskihindamine, artiklites 5 ja 6 sätestatud hoolsuskohustus ning artikli 8 lõike 4 kohane lepingute uute või oluliste muudatuste heakskiitmise protsess;

c) äriüksuste, sisekontrolliüksuste ja muude asjaomaste üksuste kaasamine seoses lepingutega;

d) artiklites 7, 8 ja 9 osutatud lepingute rakendamine, jälgimine ja haldamine, sealhulgas asjakohasel juhul konsolideeritud ja allkonsolideeritud tasandil;

e) dokumenteerimine ja andmete säilitamine, võttes arvesse määruse (EL) 2022/2554 artikli 28 lõikes 3 sätestatud teaberegistriga seotud nõudeid;

f) väljumisstrateegiad ja lõpetamisprotsessid, nagu on sätestatud artiklis 10.

Artikkel 5

Riski eelhindamine

1. Põhimõtetega nõutakse, et finantssektori ettevõtja ärivajadused tuleb kindlaks määrata enne lepingute sõlmimist.

2. Põhimõtetega nõutakse, et enne lepingu sõlmimist viiakse läbi riskihindamine finantssektori ettevõtja tasandil ning vajaduse korral konsolideeritud ja allkonsolideeritud tasandil.

Riskihindamisel võetakse arvesse kõiki määruses (EL) 2022/2554 ja kohaldatavates liidu valdkondlikes õigusaktides sätestatud asjakohaseid nõudeid. Eelkõige võetakse arvesse kolmandast isikust IKT-teenuste osutajate poolt kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamise mõju finantssektori ettevõtjale ning kõiki riske, mis tulenevad kolmandast isikust IKT-teenuste osutajate poolt kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamisest, sealhulgas järgmist:

a) operatsiooniriskid;

b) õiguslikud riskid;

c) IKT-riskid;

d) maineriskid;

e) konfidentsiaalsete või isikuandmete kaitsega seotud riskid;

f) andmete kättesaadavusega seotud riskid;

g) andmete töötlemise ja säilitamise kohaga seotud riskid;

h) kolmandast isikust IKT-teenuste osutaja asukohaga seotud riskid;

i) IKT kontsentratsiooniriskid üksuse tasandil.

Artikkel 6

Hoolsuskohustus

1. Põhimõtetega määratakse kindlaks asjakohane ja proportsionaalne protsess potentsiaalsete kolmandast isikust IKT-teenuste osutajate valimiseks ja hindamiseks, võttes arvesse, kas kolmandast isikust IKT-teenuste osutaja on kontsernisisene IKT-teenuste osutaja või mitte, ning nõutakse, et finantssektori ettevõtja hindaks enne lepingu sõlmimist, kas kolmandast isikust IKT-teenuste osutaja(l):

a) on ärimaine, piisav võimekus, asjatundlikkus ja piisavad finants-, inim- ja tehnilised ressursid, infoturbestandardid, asjakohane organisatsiooniline struktuur, riskijuhtimine ja sisekontroll ning asjakohasel juhul nõutavad load või registreeringud, et osutada IKT-teenuseid, mis toetavad kriitilise tähtsusega või olulist funktsiooni usaldusväärsel ja professionaalsel viisil;

b) suudab jälgida asjakohaseid tehnoloogilisi arenguid ja teha kindlaks IKT-turbe juhtivad tavad ning vajaduse korral neid rakendada, et luua tulemuslik ja usaldusväärne digitaalse tegevuskerksuse raamistik;

c) kasutab või kavatseb kasutada IKT alltöövõtjaid kriitilise tähtsusega või olulisi funktsioone või nende olulisi osi toetavate IKT-teenuste osutamiseks;

d) asub või töötleb või säilitab andmeid kolmandas riigis ja kui see on nii, siis kas see tava mõjutab operatsiooni- või maineriski taset või ohtu, et teda mõjutavad piiravad meetmed, sealhulgas embargod ja sanktsioonid, mis võivad mõjutada kolmandast isikust IKT-teenuste osutaja suutlikkust IKT-teenuseid osutada või finantssektori ettevõtja suutlikkust neid IKT-teenuseid saada;

e) annab nõusoleku lepingutele, millega tagatakse, et finantssektori ettevõtja ise, määratud kolmandad isikud ja pädevad asutused saavad teha auditeid kolmandast isikust IKT-teenuste osutajas, sealhulgas kohapeal;

f) tegutseb eetilisel ja sotsiaalselt vastutustundlikul viisil, austab inimõigusi ja laste õigusi, sealhulgas lapstööjõu kasutamise keeldu, järgib kohaldatavaid keskkonnakaitse põhimõtteid ning tagab asjakohased töötingimused.

2. Põhimõtetega määratakse kindlaks nõutav kindlustase seoses kolmandast isikust IKT-teenuste osutajate riskijuhtimisraamistiku tulemuslikkusega tema osutatavate IKT-teenuste puhul, mis toetavad kriitilise tähtsusega või olulisi funktsioone. Põhimõtetega nõutakse, et hoolsuskohustuse protsess hõlmaks riskimaandamis- ja talitluspidevuse meetmete olemasolu hindamist ja selle hindamist, kuidas on tagatud nende meetmete toimimine kolmandast isikust IKT-teenuste osutaja puhul.

3. Põhimõtetega määratakse kindlaks hoolsuskohustuse protsess potentsiaalsete kolmandast isikust IKT-teenuste osutajate valimiseks ja hindamiseks ning märgitakse, milliseid järgmisi elemente kasutatakse nõutava kindlustaseme tagamiseks seoses kolmandast isikust IKT-teenuste osutaja tulemustega:

a) auditid või sõltumatud hindamised, mida teeb finantssektori ettevõtja ise või mida tehakse tema nimel;

b) kolmandast isikust IKT-teenuste osutaja taotlusel koostatud sõltumatute auditiaruannete kasutamine;

c) kolmandast isikust IKT-teenuste osutaja siseauditi funktsiooni koostatud auditiaruannete kasutamine;

d) asjakohaste kolmandate isikute sertifikaatide kasutamine;

e) finantssektori ettevõtjale kättesaadava muu asjakohase teabe või kolmandast isikust IKT-teenuste osutaja esitatud muu teabe kasutamine.

4. Finantssektori ettevõtjad tagavad asjakohase kindlustaseme seoses kolmandast isikust IKT-teenuste osutaja tulemustega, võttes arvesse lõike 3 punktides a–e loetletud elemente. Vajaduse korral kasutatakse rohkem kui ühte nendes punktides loetletud elementi.

Artikkel 7

Huvide konflikt

1. Põhimõtetega määratakse kindlaks sellised asjakohased meetmed kolmandast isikust IKT-teenuste osutajate kasutamisest tulenevate tegelike või võimalike huvide konfliktide kindlakstegemiseks, ennetamiseks ja haldamiseks, mis tuleb võtta enne asjakohaste lepingute sõlmimist, ning nähakse ette selliste huvide konfliktide pidev jälgimine.

2. Kui kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid osutavad kontsernisisesed IKT-teenuste osutajad, määratakse põhimõtetega kindlaks, et otsused IKT-teenuste tingimuste, sealhulgas finantstingimuste kohta tehakse objektiivselt.

Artikkel 8

Lepingutingimused

1. Põhimõtetega määratakse kindlaks, et asjaomane leping peab olema kirjalik ja sisaldama kõiki määruse (EL) 2022/2554 artikli 30 lõigetes 2 ja 3 osutatud elemente. Põhimõtted hõlmavad ka elemente, mis on seotud määruse (EL) 2022/2554 artikli 1 lõike 1 punktis a osutatud nõuetega ning asjakohasel juhul muu asjakohase liidu ja liikmesriigi õigusega.

2. Põhimõtetega määratakse kindlaks, et asjaomased lepingud peavad nägema ette, et finantssektori ettevõtjal on õigus pääseda ligi teabele ning teha kontrolle, auditeid ja IKT teste. Selleks nähakse põhimõtetega ette, et ilma et see piiraks finantssektori ettevõtja lõplikku vastutust, kasutab finantssektori ettevõtja järgmisi meetodeid:

a) oma siseaudit või määratud kolmanda isiku audit;

b) asjakohasel juhul ühisauditid ja IKT ühistestimine, sealhulgas ohuteabel põhinev läbistustestimine, mis korraldatakse ühiselt teiste alltöövõttu kasutavate finantssektori ettevõtjatega või ettevõtetega, kes kasutavad sama kolmandast isikust IKT-teenuste osutaja IKT-teenuseid, ning mille viivad läbi kõnealused alltöövõttu kasutavad finantssektori ettevõtjad või ettevõtted või nende määratud kolmas isik;

c) asjakohasel juhul kolmanda isiku sertifikaadid;

d) asjakohasel juhul sise- või välisauditi aruanded, mille kolmandast isikust IKT-teenuste osutaja on kättesaadavaks teinud.

3. Finantssektori ettevõtja ei tohi aja jooksul tugineda üksnes lõike 2 punktis c osutatud sertifikaatidele või kõnealuse lõike punktis d osutatud auditiaruannetele. Põhimõtetega lubatakse kasutada lõike 2 punktides c ja d osutatud meetodeid üksnes juhul, kui finantssektori ettevõtja(l):

a) on rahul kolmandast isikust IKT-teenuste osutaja auditikavaga asjaomaste lepingute kohta;

b) tagab, et sertifikaatide või auditiaruannete ulatus hõlmab selles kindlaks määratud süsteeme ja põhikontrolle ning tagab vastavuse asjakohastele regulatiivsetele nõuetele;

c) hindab pidevalt põhjalikult sertifikaatide või auditiaruannete sisu ja kontrollib, et aruanded või sertifikaadid ei ole aegunud;

d) tagab, et sertifikaadi või auditiaruande tulevased versioonid hõlmavad põhisüsteeme ja -kontrolle;

e) on veendunud, et sertifitseeriv või auditeeriv isik on sobiv;

f) on veendunud, et sertifikaadid on välja antud ja auditid on tehtud laialdaselt tunnustatud asjakohaste kutsestandardite alusel ning need hõlmavad kehtestatud põhikontrollide toimimise tulemuslikkuse testi;

g) on lepinguline õigus nõuda riskijuhtimise seisukohast mõistliku ja õiguspärase sagedusega sertifikaatide või auditiaruannete ulatuse muutmist nii, et need hõlmaks muid asjakohaseid süsteeme ja kontrolle;

h) on lepinguline õigus teha seoses lepingutega oma äranägemisel individuaalseid ja ühisauditeid ning kasutada seda õigust kokkulepitud sagedusega.

4. Põhimõtetega tagatakse, et lepingu olulised muudatused vormistatakse kirjalikus dokumendis, millel on kuupäev ja millele on alla kirjutanud kõik pooled, ning määratakse kindlaks lepingute uuendamise protsess.

Artikkel 9

Lepingute jälgimine

1. Põhimõtetega nõutakse, et lepingutes määratakse kindlaks meetmed ja põhinäitajad, mille abil pidevalt jälgida kolmandast isikust IKT-teenuste osutajate tegevust, sealhulgas meetmed, millega jälgitakse andmete ja teabe konfidentsiaalsuse, kättesaadavuse, usaldusväärsuse ja autentsusega seotud nõuete täitmist ning kolmandast isikust IKT-teenuste osutajate vastavust finantssektori ettevõtja asjakohastele põhimõtetele ja menetlustele. Põhimõtetega määratakse ka kindlaks meetmed, mida kohaldatakse juhul, kui teenustaseme kokkuleppeid ei täideta, sealhulgas vajaduse korral leppetrahvid.

2. Põhimõtetega määratakse kindlaks, kuidas finantssektori ettevõtja peab hindama, kas kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamiseks kasutatavad kolmandast isikust IKT-teenuste osutajad vastavad asjakohastele tulemus- ja kvaliteedistandarditele kooskõlas lepingu ja finantssektori ettevõtja enda põhimõtetega. Põhimõtetega tagatakse eelkõige järgmine:

a) kolmandast isikust IKT-teenuste osutajad esitavad finantssektori ettevõtjale asjakohaseid aruandeid oma tegevuse ja teenuste kohta, sealhulgas perioodilisi aruandeid ning aruandeid intsidentide, teenuse osutamise, IKT-turbe ning talitluspidevuse meetmete ja testimise kohta;

b) kolmandast isikust IKT-teenuste osutajate tulemusi hinnatakse peamiste tulemusnäitajate, peamiste kontrollinäitajate, auditite, enesesertifitseerimise ja sõltumatu läbivaatamise abil kooskõlas finantssektori ettevõtja IKT-riskide juhtimise raamistikuga;

c) finantssektori ettevõtja saab kolmandast isikust IKT-teenuste osutajatelt muud asjakohast teavet;

d) finantssektori ettevõtjat teavitatakse vajaduse korral IKTga seotud intsidentidest ning tegevust või turvalisust mõjutavatest maksetega seotud intsidentidest;

e) tehakse sõltumatu läbivaatus ja auditid, et kontrollida vastavust õiguslikele ja regulatiivsetele nõuetele ja põhimõtetele.

3. Põhimõtetega määratakse kindlaks, et lõikes 2 osutatud hindamine dokumenteeritakse ja selle tulemusi kasutatakse artiklis 6 osutatud finantssektori ettevõtja riskihindamise ajakohastamiseks.

4. Põhimõtetega kehtestatakse asjakohased meetmed, mida finantssektori ettevõtja peab võtma, kui ta teeb kindlaks kolmandast isikust IKT-teenuste osutajate puudused, sealhulgas IKTga seotud intsidendid ning tegevust või turvalisust mõjutavad maksetega seotud intsidendid, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamisel või lepingute või õiguslike nõuete täitmisel. Samuti määratakse kindlaks, kuidas tuleb jälgida selliste meetmete rakendamist, et tagada nende tulemuslik järgimine kindlaksmääratud aja jooksul, võttes arvesse puuduste olulisust.

Artikkel 10

Lepingust väljumine ja selle lõpetamine

Põhimõtted peavad sisaldama nõudeid, mis käsitlevad iga lepingu puhul dokumenteeritud väljumiskava ning selle perioodilist läbivaatamist ja testimist. Väljumiskava koostamisel võetakse arvesse järgmist:

a) ettenägematud ja püsivad teenusekatkestused;

b) ebasobiv või ebaõnnestunud teenuse osutamine;

c) lepingu ootamatu lõpetamine.

Väljumiskava peab olema realistlik, teostatav, põhinema usutavatel stsenaariumidel ja mõistlikel eeldustel ning sisaldama kavandatud rakendamise ajakava, mis on kooskõlas lepingus sätestatud väljumis- ja lõpetamistingimustega.

Artikkel 11

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 13. märts 2024

Komisjoni nimel
president
Ursula VON DER LEYEN