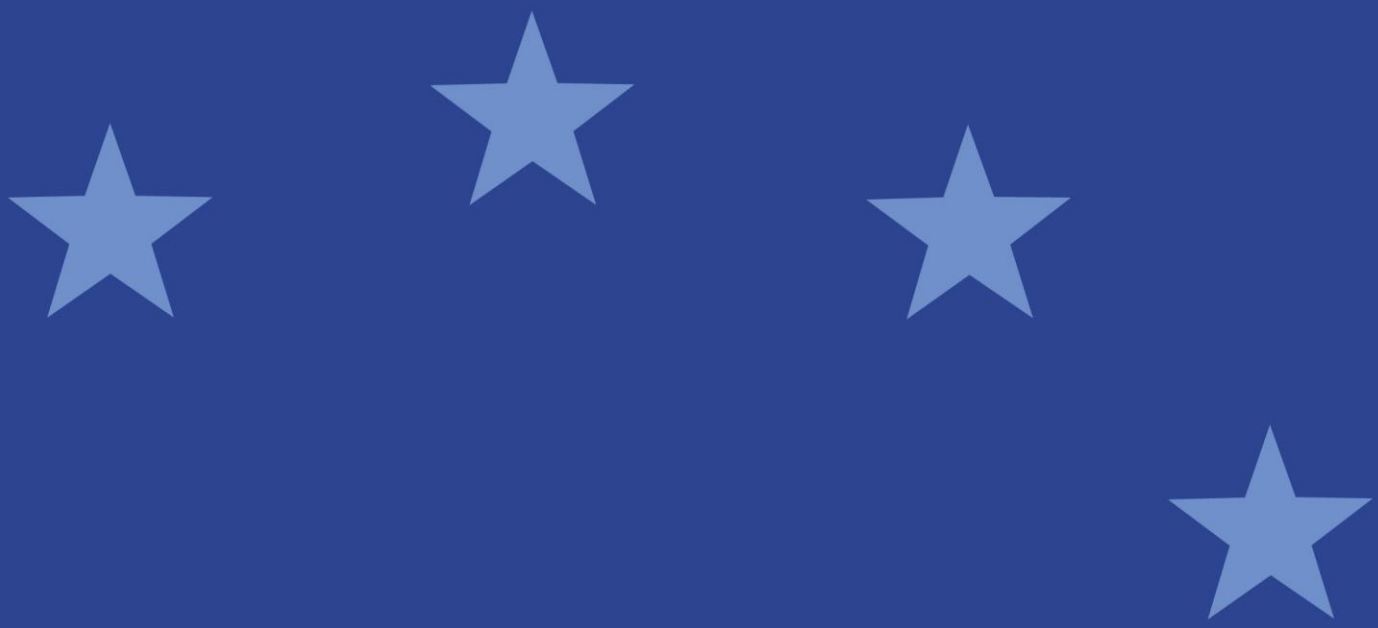
esma European Securities and Markets Authority

# Ohjeet

## ulkoistamisesta pilvipalvelujen tarjoajille



10/05/2021 | ESMA50-164-4285 FI

# Sisällysluettelo

# I. Soveltamisala

**Kenelle?**

1. Ohjeita sovelletaan toimivaltaisiin viranomaisiin sekä (i) vaihtoehtoisten sijoitusrahastojen hoitajiin ja vaihtoehtoisten sijoitusrahastojen säilytysyhteisöihin, (ii) siirtokelpoisiin arvopapereihin kohdistuvaa yhteistä sijoitustoimintaa harjoittaviin yrityksiin (yhteissijoitusyritys), yhteissijoitusyritysten rahastoyhtiöihin ja säilytysyhteisöihin sekä sijoitusrahastoihin, jotka eivät ole nimittäneet yhteissijoitusyrityksiä koskevan direktiivin nojalla valtuutettua rahastoyhtiötä, (iii) keskusvastapuoliin, mukaan luettuina kolmansiin maihin sijoittautuneet toisen tason keskusvastapuolet, jotka noudattavat asiaankuuluvia Euroopan markkinarakenneasetuksen (EMIR) vaatimuksia, (iv) kauppatietorekistereihin, (v) sijoituspalveluyrityksiin ja luottolaitoksiin sijoituspalveluiden ja -toimien suorittamisen yhteydessä, raportointipalvelujen tarjoajiin ja kauppapaikoissa toimiviin markkinoiden ylläpitäjiin, (vi) arvopaperikeskuksiin, (vii) luottoluokituslaitoksiin, (viii) arvopaperistamisrekistereihin ja (ix) kriittisten vertailuarvojen hallinnoijiin.

2. Lisäksi ESMA ottaa nämä ohjeet huomioon arvioidessaan, missä määrin kolmanteen maahan sijoittautunut toisen tason keskusvastapuoli noudattaa asianmukaisia EMIR-vaatimuksia, kun se noudattaa vastaavia kolmannessa maassa sovellettavia vaatimuksia EMIR-asetuksen 25 artiklan 2b kohdan a alakohdan nojalla.

**Mitä?**

3. Näitä ohjeita sovelletaan seuraavien säännösten osalta:

   a) vaihtoehtoisten sijoitusrahastojen hoitajia koskevan direktiivin 15, 18 ja 20 artikla ja 21 artiklan 8 kohta; komission delegoidun asetuksen (EU) N:o 2013/231 13, 22, 38, 39, 40, 44 ja 45 artikla, 57 artiklan 1 kohdan d alakohta, 57 artiklan 2 ja 3 kohta sekä 58, 75, 76, 77, 79, 81, 82 ja 98 artikla;
   b) yhteissijoitusyrityksistä annetun direktiivin 12 artiklan 1 kohdan a alakohta, 13 artikla, 14 artiklan 1 kohdan c alakohta, 22 ja 22a artikla, 23 artiklan 2 kohta sekä 30 ja 31 artikla; komission direktiivin 2010/43/EU 4 artiklan 1–3 kohta, 4 artiklan 5 kohta, 5 artiklan 2 kohta, 7 ja 9 artikla, 23 artiklan 4 kohta sekä 32, 38, 39 ja 40 artikla; komission delegoidun asetuksen (EU) 2016/438 2 artiklan 2 kohdan j alakohta, 3 artiklan 1 kohta, 13 artiklan 2 kohta sekä 15, 16 ja 22 artikla;
   c) EMIR-asetuksen 25 artikla, 26 artiklan 1, 3 ja 6 kohta sekä 34, 35 ja 78–81 artikla; SFTR-asetuksen 5 ja 12 artikla; komission delegoidun asetuksen (EU) N:o 153/2013 3 artiklan 1 kohdan f alakohta, 3 artiklan 2 kohta, 4 artikla, 7 artiklan 2 kohdan d ja f alakohta sekä 9 ja 17 artikla; komission delegoidun asetuksen (EU) N:o 150/2013 16 ja 21 artikla; komission delegoidun asetuksen (EU) 2019/359 16 ja 21 artikla;
   d) MiFID II -asetuksen 16 artiklan 2, 4 ja 5 kohta, 18 artiklan 1 kohta, 19 artiklan 3 kohdan a alakohta, 47 artiklan 1 kohdan b ja c alakohta, 48 artiklan 1 kohta,

64 artiklan 4 kohta, 65 artiklan 5 kohta ja 66 artiklan 3 kohta [1]; komission delegoidun asetuksen (EU) 2017/565 21 artiklan 1–3 kohta, 23 artikla, 29 artiklan 5 kohta sekä 30, 31 ja 32 artikla; komission delegoidun asetuksen (EU) 2017/584 6 ja 15 artikla ja 16 artiklan 6 kohta; komission delegoidun asetuksen (EU) 2017/571 6, 7, 8 ja 9 artikla;

e) CSDR-asetuksen 22, 26, 30, 42, 44 ja 45 artikla ja komission delegoidun asetuksen (EU) 2017/392 33 ja 47 artikla, 50 artiklan 1 kohta, 57 artiklan 2 kohdan i alakohta sekä, 66, 68, 75, 76, 78 ja 80 artikla;
f) luottoluokituslaitosasetuksen 9 artikla ja liitteessä I olevan A jakson 4 ja 8 kohta ja liitteessä II oleva 17 kohta sekä komission delegoidun asetuksen (EU) N:o 2012/449 11 ja 25 artikla;
g) SECR-asetuksen 10 artiklan 2 kohta;
h) vertailuarvoasetuksen 6 artiklan 3 kohta ja 10 artikla sekä komission delegoidun asetuksen (EU) 2018/1646 liitteessä I oleva 7 kohta.

**Milloin?**

4. Näitä ohjeita sovelletaan 31. heinäkuuta 2021 alkaen kaikkiin pilvipalvelujen ulkoistamisjärjestelyihin, jotka on tehty tai joita on jatkettu tai muutettu kyseisenä päivänä tai sen jälkeen. Yritysten on arvioitava ja muutettava nykyiset pilvipalvelujen ulkoistamisjärjestelyt vastaavasti sen varmistamiseksi, että nämä ohjeet otetaan niissä huomioon 31. joulukuuta 2022 mennessä. Jos kriittisiä tai tärkeitä toimintoja koskevia pilvipalvelujen ulkoistamisjärjestelyjä ei ole arvioitu 31. joulukuuta 2022 mennessä, yritysten on ilmoitettava tästä toimivaltaiselle viranomaiselle ja sisällytettävä ilmoitukseen suunnitellut toimenpiteet, joilla arviointi saatetaan päätökseen, tai mahdollinen irtautumisstrategia.

# II. Lainsäädäntöviittaukset, lyhenteet ja määritelmät

**Lainsäädäntöviittaukset**

| | |
|---|---|
| ESMA-asetus | Euroopan parlamentin ja neuvoston asetus (EU) N:o 1095/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan arvopaperimarkkinaviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/77/EY kumoamisesta[2] |
| AIFMD-direktiivi | Euroopan parlamentin ja neuvoston direktiivi 2011/61/EU, annettu 8 päivänä kesäkuuta 2011, vaihtoehtoisten sijoitusrahastojen hoitajista ja direktiivin 2003/41/EY ja |

[1] Tammikuun 1. päivästä 2022 alkaen viittaukset MiFID II -asetuksen 64 artiklan 4 kohtaan, 65 artiklan 5 kohtaan ja 66 artiklan 3 kohtaan on katsottava viittauksiksi MiFIR -asetuksen 27g artiklan 4 kohtaan, 27h artiklan 5 kohtaan ja 27i artiklan 3 kohtaan.
[2] EUVL L 331, 15.12.2010, s. 84.

| | |
|---|---|
| | 2009/65/EY sekä asetuksen (EY) N:o 1060/2009 ja (EU) N:o 1095/2010 muuttamisesta[3] |
| Komission delegoitu asetus (EU) N:o 2013/231 | Komission delegoitu asetus (EU) N:o 2013/231, annettu 19 päivänä joulukuuta 2012, Euroopan parlamentin ja neuvoston direktiivin 2011/61/EY täydentämisestä poikkeuksien, yleisten toimintaedellytysten, säilytysyhteisöjen, vivutuksen, avoimuuden ja valvonnan osalta[4] |
| Yhteissijoitusyrityksistä annettu direktiivi | Euroopan parlamentin ja neuvoston direktiivi 2009/65/EY, annettu 13 päivänä heinäkuuta 2009, siirtokelpoisiin arvopapereihin kohdistuvaa yhteistä sijoitustoimintaa harjoittavia yrityksiä (yhteissijoitusyritykset) koskevien lakien, asetusten ja hallinnollisten määräysten yhteensovittamisesta[5] |
| Komission direktiivi 2010/43/EU | Komission direktiivi 2010/43/EU, annettu 1 päivänä heinäkuuta 2010, Euroopan parlamentin ja neuvoston direktiivin 2009/65/EY täytäntöönpanosta organisaatiovaatimusten, eturistiriitojen, liiketoiminnan harjoittamisen, riskienhallinnan sekä säilytysyhteisön ja rahastoyhtiön välisen sopimuksen sisällön osalta[6] |
| Komission delegoitu asetus (EU) 2016/438 | Komission delegoitu asetus (EU) 2016/438, annettu 17 päivänä joulukuuta 2015, Euroopan parlamentin ja neuvoston direktiivin 2009/65/EY täydentämisestä säilytysyhteisöjen velvollisuuksien osalta[7] |
| EMIR-asetus | Euroopan parlamentin ja neuvoston asetus (EU) N:o 648/2012, annettu 4 päivänä heinäkuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä[8] |
| SFTR-asetus | Euroopan parlamentin ja neuvoston asetus (EU) 2015/2365, annettu 25 päivänä marraskuuta 2015, arvopapereilla toteutettavien rahoitustoimien ja uudelleenkäytön raportoinnista ja läpinäkyvyydestä sekä asetuksen (EU) N:o 648/2012 muuttamisesta[9] |
| Komission delegoitu asetus (EU) N:o 153/2013 | Komission delegoitu asetus (EU) N:o 153/2013, annettu 19 päivänä joulukuuta 2012, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 täydentämisestä |

[3] EUVL L 174, 1.7.2011, s. 1.
[4] EUVL L 83, 22.3.2013, s. 1.
[5] EUVL L 302, 17.11.2009, s. 32.
[6] EUVL L 176, 10.7.2010, s. 42.
[7] EUVL L 78, 24.3.2016, s. 11.
[8] EUVL L 201, 27.7.2012, s. 1.
[9] EUVL L 337, 23.12.2015, s. 1.

| | |
|---|---|
| | keskusvastapuoliin liittyviä vaatimuksia koskevien teknisten sääntelystandardien osalta[10] |
| Komission delegoitu asetus (EU) N:o 150/2013 | Komission delegoitu asetus (EU) N:o 150/2013, annettu 19 päivänä joulukuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 täydentämisestä kauppatietorekistereihin ilmoitettavien tietojen vähimmäisyksityiskohtia koskevien teknisten sääntelystandardien osalta[11] |
| Komission delegoitu asetus (EU) 2019/359 | Komission delegoitu asetus (EU) 2019/359, annettu 13 päivänä joulukuuta 2018, Euroopan parlamentin ja neuvoston asetuksen (EU) 2015/2365 täydentämisestä kauppatietorekistereihin ilmoitettavia arvopapereilla toteutettavien rahoitustoimien tietoja koskevilla teknisillä sääntelystandardeilla[12] |
| MiFID II -direktiivi | Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta[13] |
| Rahoitusmarkkina-asetus (MiFIR) | Euroopan parlamentin ja neuvoston asetus (EU) N:o 600/2014, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä asetuksen (EU) N:o 648/2012 muuttamisesta ([14]) |
| Komission delegoitu asetus (EU) 2017/565 | Komission delegoitu asetus (EU) 2017/565, annettu 25 päivänä huhtikuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä sijoituspalveluyritysten toiminnan järjestämistä koskevien vaatimusten, toiminnan harjoittamisen edellytysten ja kyseisessä direktiivissä määriteltyjen käsitteiden osalta[15] |
| Komission delegoitu asetus (EU) 2017/584 | Komission delegoitu asetus (EU) 2017/584, annettu 14 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä kauppapaikkojen toiminnan järjestämistä koskevia vaatimuksia täsmentävillä teknisillä sääntelystandardeilla[16] |
| Komission delegoitu asetus (EU) 2017/571 | Komission delegoitu asetus (EU) 2017/571, annettu 2 päivänä kesäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä |

[10] EUVL L 52, 23.2.2013, s. 41.
[11] EUVL L 52, 23.2.2013, s. 25.
[12] EUVL L 81, 22.3.2019, s. 45.
[13] EUVL L 173, 12.6.2014, s. 349.
[14] EUVL L 173, 12.6.2014, s. 84.
[15] EUVL L 87, 31.3.2017, s. 1.
[16] EUVL L 87, 31.3.2017, s. 350.

| | |
|---|---|
| | raportointipalvelujen tarjoajiin sovellettavilla toimiluvan myöntämistä, toiminnan järjestämistä koskevia vaatimuksia sekä liiketoimien julkistamista koskevilla teknisillä sääntelystandardeilla[17] |
| CSDR-asetus | Euroopan parlamentin ja neuvoston asetus (EU) N:o 909/2014, annettu 23 päivänä heinäkuuta 2014, arvopaperitoimituksen parantamisesta Euroopan unionissa sekä arvopaperikeskuksista ja direktiivien 98/26/EY ja 2014/65/EU sekä asetuksen (EU) N:o 236/2012 muuttamisesta[18] |
| Komission delegoitu asetus (EU) 2017/392 | Komission delegoitu asetus (EU) 2017/392, annettu 11 päivänä marraskuuta 2016, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 909/2014 täydentämisestä arvopaperikeskusten toimilupiin, valvontaan ja toimintaan liittyviä vaatimuksia koskevilla teknisillä sääntelystandardeilla[19] |
| Luottoluokituslaitosasetus | Euroopan parlamentin ja neuvoston asetus (EY) N:o 1060/2009, annettu 16 päivänä syyskuuta 2009, luottoluokituslaitoksista[20] |
| Komission delegoitu asetus (EU) N:o 2012/449 | Komission delegoitu asetus (EU) N:o 449/2012, annettu 21 päivänä maaliskuuta 2012, Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1060/2009 täydentämisestä luottoluokituslaitosten rekisteröintiä ja sertifiointia varten toimitettaviin tietoihin sovellettavien teknisten sääntelystandardien osalta[21] |
| SECR-asetus | Euroopan parlamentin ja neuvoston asetus (EU) 2017/2402, annettu 12 päivänä joulukuuta 2017, yleisestä arvopaperistamista koskevasta kehyksestä ja erityisestä kehyksestä yksinkertaiselle, läpinäkyvälle ja standardoidulle arvopaperistamiselle sekä direktiivien 2009/65/EY, 2009/138/EY ja 2011/61/EU ja asetusten (EY) N:o 1060/2009 ja (EU) N:o 648/2012 muuttamisesta[22] |
| Vertailuarvoasetus | Euroopan parlamentin ja neuvoston asetus (EU) 2016/1011, annettu 8 päivänä kesäkuuta 2016, rahoitusvälineissä ja rahoitussopimuksissa vertailuarvoina tai sijoitusrahastojen arvonkehityksen mittaamisessa käytettävistä indekseistä ja |

[17] EUVL L 87, 31.3.2017, s. 126.
[18] EUVL L 257, 28.8.2014, s. 1.
[19] EUVL L 65, 10.3.2017, s. 48.
[20] EUVL L 302, 17.11.2009, s. 1.
[21] EUVL L 140, 30.5.2012, s. 32.
[22] EUVL L 347, 28.12.2017, s. 35.

| | |
|---|---|
| | direktiivien 2008/48/EY ja 2014/17/EU sekä asetuksen (EU) N:o 596/2014 muuttamisesta[23] |
| Komission delegoitu asetus (EU) 2018/1646 | Komission delegoitu asetus (EU) 2018/1646, annettu 13 päivänä heinäkuuta 2018, Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/1011 täydentämisestä toimilupahakemuksessa ja rekisteröintihakemuksessa ilmoitettavia tietoja koskevilla teknisillä sääntelystandardeilla[24] |
| Yleinen tietosuoja-asetus | Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta[25] |

**Lyhenteet**

| | |
|---|---|
| *CSP* | Pilvipalvelun tarjoaja |
| *ESMA* | Euroopan arvopaperimarkkinaviranomainen |
| *EU* | Euroopan unioni |

**Määritelmät**

| | |
|---|---|
| *Toiminto* | tarkoittaa prosesseja, palveluja ja toimia; |
| *Kriittinen tai tärkeä toiminto* | tarkoittaa toimintoa, jossa ilmenevä toimintahäiriö tai sen toteuttamatta jääminen heikentäisi oleellisesti seuraavia:<br>a) yrityksen sovellettavan lainsäädännön mukaisten velvoitteiden noudattaminen;<br>b) yrityksen taloudellinen tulos; tai<br>c) yrityksen keskeisten palveluiden ja toimien vakaus tai jatkuvuus; |
| *Pilvipalvelut* | tarkoittavat etäresurssien avulla toimitettavia palveluja; |
| *Etäresurssipalvelut tai pilvi*[26] | tarkoittavat lähestymistapaa, jolla mahdollistetaan pääsy verkkoon skaalautuvalle ja mukautuvalle joukolle jaettavissa olevia fyysisiä tai virtuaalisia resursseja (esimerkiksi palvelimet, käyttöjärjestelmät, verkostot, ohjelmistot, sovellukset ja tallennusvälineet), joille tarjotaan itsepalvelu sekä pyynnöstä hallinnointi; |

[23] EUVL L 171, 29.6.2016, s. 1.
[24] EUVL L 274, 5.11.2018, s. 43.
[25] EUVL L 119, 4.5.2016, s. 1–88.
[26] Etäresurssipalveluista käytetään usein lyhyempää käsitettä ”pilvi”. Tässä asiakirjassa käytetään käsitettä ”pilvi” viittaamisen sujuvoittamiseksi.

| | |
|---|---|
| *Pilvipalvelun tarjoaja* | tarkoittaa kolmatta osapuolta, joka tarjoaa pilvipalveluja pilvipalvelujen ulkoistamisjärjestelyn perusteella; |
| *Pilvipalvelujen ulkoistamisjärjestely* | tarkoittaa minkä tahansa muotoista järjestelyä, valtuutusjärjestelyt mukaan luettuina, seuraavien tahojen välillä:<br>(i) yritys ja pilvipalvelun tarjoaja, siten, että pilvipalvelun tarjoaja suorittaa toiminnon, jonka yritys muutoin suorittaisi itse; tai<br>(ii) yritys ja kolmas osapuoli, joka ei ole pilvipalvelun tarjoaja, kuitenkin siten, että järjestely perustuu merkittävästi pilvipalvelun tarjoajaan, joka suorittaa toiminnon, jonka yritys muutoin suorittaisi itse. Tässä tapauksessa kaikki näissä ohjeissa olevat viittaukset pilvipalvelun tarjoajaan olisi katsottava viittauksiksi kyseiseen kolmanteen osapuoleen. |
| *Edelleen ulkoistaminen* | tarkoittaa tilannetta, jossa pilvipalvelun tarjoaja siirtää ulkoistetun toiminnan (tai sen osan) edelleen muulle palveluntarjoajalle ulkoistamisjärjestelyn mukaisesti. |
| *Pilven käyttöönottomalli* | tarkoittaa tapaa, jolla pilvi voidaan järjestää fyysisten tai virtuaalisten resurssien hallinnan ja jakamisen perusteella. Pilven käyttöönottomalleja ovat yhteisöpilvi[27], hybridipilvi[28], yksityinen pilvi[29] ja julkinen[30] pilvi; |
| *Yritykset* | a) vaihtoehtoisten sijoitusrahastojen hoitajat, sellaisina kuin ne määritellään AIFMD-direktiivin 4 artiklan 1 kohdan b alakohdassa, sekä säilytysyhteisöt sellaisina, kuin ne määritellään AIFMD-direktiivin 21 artiklan 3 kohdassa (”vaihtoehtoisten sijoitusrahastojen säilytysyhteisöt”);<br>b) rahastoyhtiöt, sellaisina kuin ne määritellään yhteissijoitusyrityksistä |

[27] Pilven käyttöönottomalli, jossa pilvipalveluilla tuetaan ainoastaan tiettyä pilvipalvelun asiakkaiden joukkoa, jotka jakavat pilvipalvelut ja joilla on jaetut vaatimukset ja keskinäinen suhde, ja jossa vähintään yksi kyseisen joukon jäsen hallitsee resursseja;
[28] Pilven käyttöönottomalli, jossa käytetään vähintään kahta erilaista pilven käyttöönottomallia
[29] Pilven käyttöönottomalli, jossa ainoastaan yksi pilvipalvelun asiakas käyttää pilvipalveluja ja hallitsee resursseja
[30] Pilven käyttöönottomalli, jossa pilvipalvelut ovat mahdollisesti kenen tahansa pilvipalvelun asiakkaan käytettävissä ja pilvipalvelujen tarjoaja hallitsee resursseja

annetun direktiivin 2 artiklan 1 kohdan b alakohdassa (”yhteissijoitusyritysten rahastoyhtiöt”), ja säilytysyhteisöt, sellaisina kuin ne määritellään yhteissijoitusyrityksistä annetun direktiivin 2 artiklan 1 kohdan a alakohdassa (”yhteissijoitusyritysten säilytysyhteisöt”);

c) keskusvastapuolet, sellaisina kuin ne määritellään EMIR-asetuksen 2 artiklan 1 kohdassa, ja EMIR-asetuksen 25 artiklan 2a kohdassa tarkoitetut kolmanteen maahan sijoittautuneet toisen tason vastapuolet, jotka noudattavat asiaankuuluvia EMIR-vaatimuksia EMIR-asetuksen 25 artiklan 2b kohdan a alakohdan nojalla;

d) kauppatietorekisterit, sellaisina kuin ne määritellään EMIR-asetuksen 2 artiklan 2 kohdassa ja SFTR-asetuksen 3 artiklan 1 kohdassa;

e) sijoituspalveluyritykset, sellaisina kuin ne määritellään MiFID II -direktiivin 4 artiklan 1 kohdan 1 alakohdassa, sekä MiFID I -direktiivin 4 artiklan 1 kohdan 27 alakohdassa määritellyt luottolaitokset, jotka suorittavat MiFID -direktiivin 4 artiklan 1 kohdan 2 alakohdassa tarkoitettuja sijoituspalveluja ja -toimia;

f) raportointipalvelujen tarjoajat, sellaisina kuin ne määritellään MiFID II -direktiivin 4 artiklan 1 kohdan 63 alakohdassa[31];

g) kauppapaikoissa toimivat markkinoiden ylläpitäjät, joita tarkoitetaan MiFID II -direktiivin 4 artiklan 1 kohdan 24 alakohdassa;

h) arvopaperikeskukset, sellaisina kuin ne määritellään CSDR-asetuksen 2 artiklan 1 kohdan 1 alakohdassa;

[31] Tammikuun 1. päivästä 2022 alkaen viittaus tähän säännökseen on katsottava viittaukseksi MiFIR -asetuksen 2 artiklan 1 kohdan 36 alakohdan a alakohtaan.

i) luottoluokituslaitokset, sellaisina kuin ne määritellään luottoluokituslaitosasetuksen 3 artiklan 1 kohdan b alakohdassa;

j) arvopaperistamisrekisterit, sellaisina kuin ne määritellään SECR-asetuksen 2 artiklan 23 kohdassa;

k) kriittisten vertailuarvojen hallinnoijat, sellaisina kuin ne määritellään vertailuarvoasetuksen 3 artiklan 1 kohdan 25 alakohdassa.

# III. Tarkoitus

5. Nämä ohjeet perustuvat ESMA-asetuksen 16 artiklan 1 kohtaan. Ohjeiden tarkoituksena on saada aikaan johdonmukaiset, tehokkaat ja vaikuttavat valvontakäytännöt Euroopan finanssivalvojien järjestelmässä ja varmistaa kohdassa 1.1 (otsikko ”Mitä?”) tarkoitettujen vaatimusten yhteinen, yhtenäinen ja yhdenmukainen soveltaminen, kun yritykset ulkoistavat toimintoja pilvipalvelun tarjoajille. Ohjeilla pyritään erityisesti auttamaan yrityksiä ja toimivaltaisia viranomaisia yksilöimään, käsittelemään ja seuraamaan pilvipalvelujen ulkoistamisjärjestelyistä aiheutuvia riskejä ja haasteita, jotka vaihtelevat ulkoistamispäätöksen tekemisestä, pilvipalvelujen tarjoajan valinnasta ja ulkoistettujen toimien seurannasta aina irtautumisstrategioiden määrittämiseen.

# IV. Noudattamista ja ilmoittamista koskevat vaatimukset

**Ohjeiden asema**

6. ESMA-asetuksen 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten ja yritysten on pyrittävä kaikin tavoin noudattamaan näitä ohjeita.

7. Toimivaltaisten viranomaisten, joihin ohjeita sovelletaan, on noudatettava niitä saattamalla ne soveltuvin osin osaksi kansallista lainsäädäntö- ja/tai valvontakehystä myös silloin, kun tietyt ohjeet on suunnattu ensisijaisesti yrityksille. Tässä tapauksessa toimivaltaisten viranomaisten on valvottava, että yritykset noudattavat ohjeita.

8. ESMA arvioi jatkuvan suoran valvontansa kautta sitä, kuinka luottoluokituslaitokset, kauppatietorekisterit, arvopaperistamisrekisterit, kolmansiin maihin sijoittautuneet toissijaiset keskusvastapuolet sekä 1. tammikuuta 2022 alkaen raportointipalvelujen tarjoajat ja EU:n kriittisten vertailuarvojen hallinnoijat soveltavat näitä ohjeita.

**Ilmoittamista koskevat vaatimukset**

9. Kahden kuukauden kuluessa siitä päivästä, kun ohjeet on julkaistu ESMAn verkkosivustolla EU:n kaikilla virallisilla kielillä, toimivaltaisten viranomaisten, joihin näitä ohjeita sovelletaan, on ilmoitettava ESMAlle, että ne i) noudattavat, ii) eivät noudata mutta aikovat noudattaa, iii) eivät noudata eivätkä aio noudattaa näitä ohjeita.

10. Noudattamatta jättämisen tapauksessa toimivaltaisten viranomaisten on lisäksi ilmoitettava ESMAlle syynsä näiden ohjeiden noudattamatta jättämiselle kahden kuukauden kuluessa siitä päivästä, kun ohjeet on julkaistu ESMAn verkkosivustolla EU:n kaikilla virallisilla kielillä. ESMAn verkkosivustolla on mallipohja ilmoituksia varten. Kun mallipohja on täytetty, se lähetetään ESMAlle.

11. Yritysten ei edellytetä raportoivan, noudattavatko ne näitä ohjeita.

# V. Ohjeet ulkoistamisesta pilvipalvelujen tarjoajille

## Suuntaviiva 1. Hallinta, valvonta ja dokumentointi

12. Yrityksellä on oltava määritelty ja ajantasainen pilven ulkoistamisstrategia, joka on yhdenmukainen yrityksen asiaankuuluvien strategioiden ja sisäisten toimintatapojen ja menettelyiden kanssa myös tieto- ja viestintäteknologian, tietoturvan ja operatiivisten riskien hallinnan osalta.

13. Yrityksen on

    a) määriteltävä selkeästi vastuu pilvipalvelujen ulkoistamisjärjestelyjen dokumentoinnista, hallinnasta ja valvonnasta omassa organisaatiossaan;
    b) kohdennettava riittävät resurssit näiden ohjeiden ja kaikkien yrityksen pilvipalvelujen ulkoistamisjärjestelyihin sovellettavien lakisääteisten vaatimusten noudattamisen varmistamista varten;
    c) perustettava pilvipalvelujen ulkoistamisjärjestelyn valvontatoimi tai nimettävä johtoasemassa olevat työntekijät, jotka ovat suoraan vastuuvelvollisia ylimmälle hallintoelimelle ja vastuussa pilvipalvelujen ulkoistamisjärjestelyjä koskevien riskien hallinnoinnista ja valvonnasta. Yritysten on tätä ohjetta noudattaessaan otettava huomioon liiketoimintansa luonne, laajuus ja monimutkaisuus myös taloushallinnon järjestelmään kohdistuvien riskien sekä ulkoistettaville toiminnoille ominaisten riskien kannalta ja varmistettava, että ylimmällä hallintoelimellä on asiaankuuluvat tekniset taidot, jotta se voi ymmärtää pilvipalvelujen ulkoistamisjärjestelyihin liittyvät riskit[32]. Pienten ja yksinkertaisempien yritysten on vähintään varmistettava selkeä

[32] Sijoituspalveluyritysten ja luottolaitosten osalta ks. EAMV:n ja EPV:n yhteiset ohjeet direktiivin 2013/36/EU ja direktiivin 2014/65/EU mukaisten ylimmän hallintoelimen ja keskeisistä tehtävistä vastaavien henkilöiden sopivuuden arviointia varten (EBA/GL/2017/12).

tehtävä- ja vastuujako pilvipalvelujen ulkoistamisjärjestelyjen hallinnoinnissa ja valvonnassa.

14. Yrityksen on valvottava pilvipalvelun tarjoajiensa toimien suorittamista, turvatoimia ja sovittujen palvelujen tason noudattamista. Valvonnan on oltava riskiperusteista ja siinä on painotettava ensisijaisesti ulkoistettuja kriittisiä tai tärkeitä toimintoja.

15. Yrityksen on arvioitava säännöllisin väliajoin, koskevatko sen pilvipalvelujen ulkoistamisjärjestelyt kriittistä tai tärkeää toimintoa. Arviointi on tehtävä myös aina silloin, kun ulkoistetun toiminnon luonne tai laajuus tai siihen liittyvä riski on muuttunut olennaisesti.

16. Yrityksen on pidettävä yllä ajantasaista rekisteriä kaikkia sen pilvipalvelujen ulkoistamisjärjestelyjä koskevista tiedoista ja eroteltava kriittisten tai tärkeiden toimintojen ulkoistaminen muista ulkoistamisjärjestelyistä. Erotellessaan kriittisten tai tärkeiden toimintojen ulkoistamisen muista ulkoistamisjärjestelyistä yrityksen on laadittava lyhyt tiivistelmä syistä, joiden vuoksi ulkoistettu toiminto on tai ei ole kriittinen tai tärkeä. Huomioon ottaen kansallinen lainsäädäntö, yrityksen on säilytettävä tietoja päättyneistä pilvipalvelujen ulkoistamisjärjestelyistä asianmukaisen ajanjakson ajan.

17. Kriittisiä tai tärkeitä toimintoja koskevien pilvipalvelujen ulkoistamisjärjestelyjen osalta rekisteriin on lisättävä vähintään seuraavat tiedot kustakin pilvipalvelujen ulkoistamisjärjestelystä:

    a) viitenumero;
    b) alkamispäivä ja tarvittaessa sopimuksen seuraava uusimispäivä, päättymispäivä ja/tai pilvipalvelujen tarjoajaa ja yritystä koskevat irtisanomisajat;
    c) lyhyt kuvaus ulkoistetusta toiminnosta, mukaan luettuina ulkoistetut tiedot ja maininta siitä, sisältyykö kyseisiin tietoihin henkilötietoja (esimerkiksi merkitsemällä ”kyllä” tai ”ei” erilliseen tietokenttään);
    d) yrityksen määrittämä luokka, joka kuvaa ulkoistetun toiminnon luonnetta (esimerkiksi tietotekninen toiminto, valvontatoiminto), mikä helpottaa erilaisten pilvipalvelujen ulkoistamisjärjestelytyyppien tunnistamista;
    e) tieto siitä, tukeeko ulkoistettu toiminto aikakriittistä liiketoimintaa;
    f) pilvipalvelun tarjoajan nimi ja (mahdollinen) tuotenimi, rekisteröintimaa, yrityksen rekisterinumero, oikeushenkilötunnus (jos saatavissa), rekisteröity osoite ja muut oleelliset yhteystiedot sekä mahdollisen emoyhtiön nimi;
    g) pilvipalvelujen ulkoistamisjärjestelyä sääntelevä lainsäädäntö sekä mahdollinen lainkäyttövallan valinta;
    h) pilvipalvelujen ja käyttöönottomallien tyyppi ja säilytettävien tietojen erityisluonne sekä sijainnit (alueet tai maat), joissa kyseisiä tietoja voidaan säilyttää;
    i) kriittisen tai tärkeän ulkoistetun toiminnon viimeisimmän arvioinnin päivämäärä sekä seuraavan suunnitellun arvioinnin päivämäärä;
    j) pilvipalvelun tarjoajan viimeisimmän riskinarvioinnin/tarkastuksen päivämäärä ja lyhyt tiivistelmä tärkeimmistä tuloksista sekä seuraavan suunnitellun riskinarvioinnin/tarkastuksen päivämäärä;
    k) yrityksessä henkilö tai päätöksentekoelin, joka on hyväksynyt pilvipalvelujen ulkoistamisjärjestelyn;

l) tarvittaessa niiden alihankkijoiden nimet, joille kriittinen tai tärkeä toiminto (tai sen olennaisia osia) on edelleen ulkoistettu, sekä maat, joissa alihankkijat ovat rekisteröityneet, joissa edelleen ulkoistettu palvelu suoritetaan, ja sijainnit (alueet tai maat), joissa tietoja säilytetään;
m) pilvipalvelujen ulkoistamisjärjestelyn arvioidut vuosittaiset budjettikustannukset.

18. Muita kuin kriittisiä tai tärkeitä toimintoja koskevien pilvipalvelujen ulkoistamisjärjestelyjen osalta yrityksen on määriteltävä rekisteriin sisällytettävä tiedot ulkoistetulle toiminnolle olennaisten riskien luonteen, laajuuden ja monimutkaisuuden perusteella.

## Suuntaviiva 2. Ulkoistamista edeltävä analyysi ja huolellisuusvelvollisuus (due diligence)

19. Ennen pilvipalvelujen ulkoistamisjärjestelyn tekemistä yrityksen on

a) arvioitava, koskeeko pilvipalvelujen ulkoistamisjärjestely kriittistä tai tärkeää toimintoa;
b) tunnistettava ja arvioitava kaikki pilvipalvelujen ulkoistamisjärjestelyyn liittyvät oleelliset riskit;
c) suoritettava aiottua pilvipalvelun tarjoajaa koskeva huolellisuusvelvollisuuden tarkastus;
d) tunnistettava ja arvioitava mahdolliset eturistiriidat, joita ulkoistamisesta voi aiheutua.

20. Aiottua pilvipalvelun tarjoajaa koskevien ulkoistamista edeltävän analyysin ja huolellisuusvelvollisuuden tarkastuksen on oltava suhteellisia sen toiminnon luonteen, laajuuden ja monimutkaisuuden kannalta, jonka yritys aikoo ulkoistaa, sekä kyseiselle toiminnolle ominaisten riskien kannalta. Tähän on sisällyttävä vähintään arviointi pilvipalvelujen ulkoistamisjärjestelyn mahdollisista vaikutuksista yrityksen operatiivisiin ja oikeudellisiin riskeihin sekä vaatimustenmukaisuuteen ja maineeseen liittyviin riskeihin.

21. Mikäli pilvipalvelujen ulkoistamisjärjestely koskee kriittisiä tai tärkeitä toimintoja, yrityksen on myös

a) arvioitava kaikki oleelliset riskit, joita voi syntyä pilvipalvelujen ulkoistamisjärjestelyn tuloksena (mukaan luettuina tieto- ja viestintäteknologiaan, tietoturvaan ja liiketoiminnan jatkuvuuteen liittyvät riskit, oikeudelliset ja vaatimustenmukaisuuteen liittyvät riskit, maineeseen liittyvät riskit, operatiiviset riskit sekä mahdolliset yritystä koskevat valvontarajoitukset) seuraavien seikkoihin liittyen:
    i. valittu pilvipalvelu ja ehdotetut käyttöönottomallit;
    ii. toimintojen siirtämiseen ja/tai implementointiin liittyvät menettelyt;
    iii. ulkoistettaviksi harkittavien toimintojen ja niihin liittyvien tietojen arkaluonteisuus sekä tarvittavat turvatoimet;

iv. yrityksen ja pilvipalvelun tarjoajan järjestelmien ja sovellusten yhteentoimivuus, nimenomaisesti niiden kyky vaihtaa tietoja ja käyttää vaihdettuja tietoja molemminpuolisesti;

v. yrityksen tietojen siirrettävyys, nimenomaisesti kyky siirtää yrityksen tiedot helposti yhdeltä pilvipalvelun tarjoajalta toiselle tai takaisin yritykselle;

vi. niiden EU:n jäsenvaltioiden tai EU:n ulkopuolisten maiden, joissa ulkoistetut toiminnot tarjotaan ja joissa ulkoistettuja tietoja säilytettäisiin, poliittinen vakaus, turvallisuustilanne ja oikeusjärjestelmä (mukaan luettuina voimassa olevat lainvalvontasäännökset, pilvipalvelun tarjoajan konkurssiin sovellettavat maksukyvyttömyyslainsäädännön säännökset, voimassa olevat tietosuojalait sekä se, täyttyvätkö yleisen tietosuoja-asetuksen mukaiset henkilötietojen siirtämistä kolmanteen maahan koskevat ehdot); jos kyseessä on edelleen ulkoistaminen, mahdolliset lisäriskit, joita voi aiheutua, jos alihankkija on sijoittautunut kolmanteen maahan tai eri maahan kuin pilvipalvelun tarjoaja, sekä, jos kyseessä on edelleen ulkoistamista koskeva ketju, mahdolliset lisäriskit, joita voi aiheutua muun muassa siitä, että yrityksen ja alihankkijan välillä ei ole suoraa sopimusta;

vii. yrityksen sisällä mahdollinen keskittäminen (tarvittaessa myös yrityksen konsernin tasolla), joka johtuu saman pilvipalvelun tarjoajan kanssa tehdyistä useista pilvipalvelujen ulkoistamisjärjestelyistä, sekä mahdollinen keskittäminen rahoitusalalla EU:ssa, joka johtuu siitä, että useat yritykset käyttävät samaa pilvipalvelun tarjoajaa tai pientä joukkoa pilvipalvelun tarjoajia. Keskittämisriskiä arvioidessaan yrityksen on otettava huomioon kaikki pilvipalvelujen ulkoistamisjärjestelynsä (sekä tarvittaessa konsernin tasoiset pilvipalvelujen ulkoistamisjärjestelyt) kyseisen pilvipalvelun tarjoajan kanssa;

b) huomioitava pilvipalvelujen ulkoistamisjärjestelyn odotettavissa olevat hyödyt ja kustannukset sekä verrattava merkittäviä riskejä, joita järjestely voi pienentää tai joiden hallintaa se voi helpottaa, niihin merkittäviin riskeihin, joita ehdotettu pilvipalvelujen ulkoistamisjärjestely voi aiheuttaa.

22. Jos ulkoistetaan kriittisiä tai tärkeitä toimintoja, huolellisuusvelvollisuuden tarkastukseen on sisällyttävä pilvipalvelun tarjoajan soveltuvuuden arviointi. Pilvipalvelun tarjoajan soveltuvuutta arvioidessaan yrityksen on varmistettava, että pilvipalvelun tarjoajalla on tarvittava maine, valmiudet, resurssit (esim. henkilö-, IT- ja rahoitusresurssit), organisaatiorakenne sekä tarvittaessa toimilupa, toimiluvat tai rekisteröinti tai rekisteröinnit, jotka vaaditaan kriittisen tai tärkeän toiminnon luotettavaan ja ammattitaitoiseen tarjoamiseen sekä velvoitteiden täyttämiseen pilvipalvelujen ulkoistamisjärjestelyn aikana. Pilvipalvelun tarjoajan huolellisuusvelvollisuuden tarkastuksessa on huomioitava esimerkiksi seuraavat muut seikat:

a) tietoturvan hallinnointi ja erityisesti henkilötietojen, luottamuksellisten tietojen tai muutoin arkaluonteisten tietojen suojaus;
b) palvelun tuki, mukaan luettuina tukisuunnitelmat ja yhteyspisteet, sekä häiriötilanteiden hallintamenettelyt;

c) liiketoiminnan jatkuvuutta ja vakavasta virhetilanteesta palautumista koskevat suunnitelmat.

23. Tarvittaessa ja suoritettavan huolellisuusvelvollisuuden tarkastuksen tukemiseksi yritys voi käyttää kansainvälisiin standardeihin perustuvia sertifiointeja sekä ulkoisia tai sisäisiä tarkastuksia koskevia kertomuksia.

24. Jos yrityksen tietoon tulee merkittäviä puutteita ja/tai muutoksia tarjotuissa palveluissa tai pilvipalvelun tarjoajan tilanteessa, pilvipalvelun tarjoajaa koskevat ulkoistamista edeltävä analyysi ja huolellisuusvelvollisuuden tarkastus on arvioitava viipymättä ja tehtävä tarvittaessa uudelleen.

25. Jos yritys tekee uuden järjestelyn tai uusii olemassa olevan sopimuksen sellaisen pilvipalvelun tarjoajan kanssa, joka on jo arvioitu, yrityksen on määritettävä riskien perusteella, onko uusi huolellisuusvelvollisuuden tarkastus tarpeen.

## Suuntaviiva 3. Keskeiset sopimuksen osat

26. Yrityksen ja pilvipalvelujen tarjoajan oikeudet ja velvoitteet on määritettävä selkeästi kirjallisella sopimuksella.

27. Kirjallisessa sopimuksessa on nimenomaisesti määritettävä, että yritys voi tarvittaessa päättää sopimuksen.

28. Jos ulkoistetaan kriittisiä tai tärkeitä toimintoja, kirjalliseen sopimukseen on sisällyttävä vähintään

a) ulkoistettavan toiminnon selkeä kuvaus;

b) sopimuksen alkamispäivä ja tarvittaessa päättymispäivä sekä pilvipalvelun tarjoajaa ja yritystä koskevat irtisanomisajat;

c) sopimusta sääntelevä lainsäädäntö sekä mahdollinen lainkäyttövallan valinta;

d) yrityksen ja pilvipalvelun tarjoajan taloudelliset velvoitteet;

e) sallitaanko edelleen ulkoistaminen ja, jos sallitaan, millaisin ehdoin (ottaen huomioon suuntaviivan 7);

f) sijainti tai sijainnit (alueet tai maat), joissa ulkoistettu toiminto suoritetaan ja joissa tietoja säilytetään ja käsitellään, sekä noudatettavat ehdot, myös velvollisuus ilmoittaa yritykselle, jos pilvipalvelun tarjoaja ehdottaa kyseisen sijainnin tai kyseisten sijaintien muuttamista;

g) tietoturvaa ja henkilötietojen suojausta koskevat säännöt (ottaen huomioon suuntaviivan 4);

h) yrityksen oikeus seurata pilvipalvelun tarjoajan suoritusta pilvipalvelujen ulkoistamisjärjestelyn puitteissa säännöllisin väliajoin (ottaen huomioon suuntaviivan 6);

i) sovitut palvelutasot sekä määrälliset ja laadulliset suoritustavoitteet oikea-aikaista seurantaa varten, jotta korjaaviin toimenpiteisiin voidaan ryhtyä viipymättä, jos sovittua palvelutasoa ei saavuteta;

j) pilvipalvelun tarjoajan raportointivelvollisuudet yritykselle sekä tarvittaessa velvoite toimittaa yrityksen turvallisuustoimintojen ja keskeisten toimintojen kannalta oleellisia kertomuksia, kuten pilvipalvelun tarjoajan sisäisen tarkastustoiminnon laatimia kertomuksia;

k) pilvipalvelun tarjoajan häiriötilanteiden hallintaa koskevat säännökset, mukaan luettuna pilvipalvelun tarjoajan velvollisuus ilmoittaa yritykselle ilman aiheetonta viivytystä häiriötilanteista, jotka ovat vaikuttaneet yrityksen sopimusperusteisen palvelun toimintaan;

l) tieto siitä, onko pilvipalvelun tarjoajan otettava pakollinen vakuutus tiettyjä riskejä vastaan ja vaadittu vakuutusturva tarvittaessa;

m) vaatimukset, joiden mukaan pilvipalvelun tarjoajan on toteutettava ja testattava liiketoiminnan jatkuvuutta ja vakavasta virhetilanteesta palautumista koskevat suunnitelmat;

n) vaatimus, jonka mukaan pilvipalvelun tarjoajan on annettava yritykselle, sen toimivaltaisille viranomaisille tai kenelle tahansa yrityksen tai toimivaltaisten viranomaisten nimittämälle henkilölle oikeus käyttää (”käyttöoikeudet”) ja tarkastaa (”tarkastusoikeudet”) pilvipalvelun tarjoajan oleellisia tietoja, tiloja, järjestelmiä ja laitteita siinä laajuudessa kuin on tarpeen, jotta voidaan seurata pilvipalvelujen ulkoistamisjärjestelyä koskevan sopimuksen alaista pilvipalvelun tarjoajan suoritusta ja sitä, että pilvipalvelun tarjoaja noudattaa sovellettavia sääntelyllisiä ja sopimusperusteisia vaatimuksia (ottaen huomioon suuntaviivan 6);

o) säännökset, joilla varmistetaan, että pilvipalvelun tarjoajan yrityksen puolesta käsittelemiä tai säilyttämiä tietoja voidaan käsitellä ja ne voidaan palauttaa ja toimittaa takaisin yritykselle tarvittaessa (ottaen huomioon suuntaviivan 5).

## Suuntaviiva 4. Tietoturva

29. Yrityksen on määritettävä tietoturvavaatimukset sisäisissä toimintatavoissaan ja menettelyissään sekä pilven ulkoistamista koskevassa kirjallisessa sopimuksessa ja seurattava näiden vaatimusten noudattamista jatkuvasti myös luottamuksellisten tietojen, henkilötietojen tai muutoin arkaluonteisten tietojen suojaamiseksi. Näiden vaatimusten on oltava suhteellisia sen toiminnon luonteen, laajuuden ja monimutkaisuuden kannalta, jonka yritys ulkoistaa pilvipalvelun tarjoajalle, sekä kyseiselle toiminnolle ominaisten riskien kannalta.

30. Tätä tarkoitusta varten kriittisten tai tärkeiden toimintojen ulkoistamisen yhteydessä, sanotun kuitenkaan rajoittamatta yleisen tietosuoja-asetuksen mukaisesti sovellettavia vaatimuksia, riskiperusteista lähestymistapaa käyttävän yrityksen on vähintään huolehdittava seuraavista:

a) *tietoturvajärjestelyt:* varmistettava, että tietoturvaa koskevat tehtävät ja vastuut on jaettu selkeästi yrityksen ja pilvipalvelun tarjoajan kesken myös uhkien havaitsemisen, häiriötilanteiden hallinnan ja ohjelmistokorjausten hallinnan osalta, ja varmistettava, että pilvipalvelun tarjoaja kykenee tosiasiallisesti täyttämään tehtävänsä ja vastuunsa;
b) *henkilöllisyyden ja käyttöoikeuksien hallinta*: varmistettava, että käytössä on vahvat tunnistusmekanismit (esimerkiksi kaksivaiheinen tunnistus) ja käyttöoikeuksien hallinta, joilla estetään luvaton pääsy yrityksen tietoihin ja taustaohjelmien pilviresursseihin;
c) *salaus ja avaintenhallinta*: varmistettava, että tarvittaessa käytetään oleellisia salausteknologioita siirrettävien tietojen, muistissa olevien tietojen, varastoitujen tietojen ja tietojen varmuuskopioiden suojaamiseksi yhdessä asianmukaisten avaintenhallintaratkaisujen kanssa, jotta voidaan rajoittaa salausavainten luvattoman käytön riskiä; yrityksen on erityisesti otettava huomioon viimeisin teknologia ja prosessit valitessaan avaintenhallintaratkaisuaan;
d) *toiminta ja verkkoturvallisuus*: otettava huomioon asianmukaiset verkon saatavuuden asteet, verkkojen eristäminen (esimerkiksi vuokraajien eristäminen jaetussa pilviympäristössä, verkkoa koskeva toiminnan eristäminen, sovellusten logiikka, käyttöjärjestelmä, verkko, tietokannan hallintajärjestelmä ja tallennuskerrokset) sekä käsittely-ympäristöt (esimerkiksi testaus, hyväksymistestaus, kehitys, tuotanto)
e) *ohjelmointirajapinnat (API)*: otettava huomioon pilvipalvelujen integrointiin yrityksen järjestelmiin käytettävät mekanismit, joilla varmistetaan ohjelmointirajapintojen turvallisuus (esimerkiksi tietoturvapolitiikkojen ja -menettelyjen perustaminen ja ylläpitäminen ohjelmointirajapintoja varten useissa järjestelmärajapinnoissa, lainkäyttöalueilla ja liiketoimintaa koskevissa toiminnoissa tietojen luvattoman paljastamisen, muokkauksen tai tuhoamisen estämiseksi);
f) *liiketoiminnan jatkuvuus ja vakavasta virhetilanteesta palautuminen*: varmistettava, että käytössä on liiketoiminnan jatkuvuutta ja vakavasta virhetilanteesta palautumista koskevat tehokkaat hallintakeinot (esimerkiksi säätämällä vähimmäiskapasiteettia koskevat vaatimukset, valitsemalla maantieteellisesti hajautetut isännöintivaihtoehdot, joita voidaan vaihdella keskenään, tai pyytämällä ja arvioimalla asiakirjat, joista ilmenee yrityksen tietojen siirtoreitti pilvipalvelun tarjoajan järjestelmissä, sekä ottamalla huomioon mahdollisuus siirtää sama virtuaalikoneen kuvatiedosto toiseen, riippumattomaan säilytyspaikkaan, joka on riittävän eristyksissä verkosta tai jonka verkkoyhteys on katkaistu);
g) *tietojen sijainti*: käytettävä riskiperusteista lähestymistapaa tietojen säilytys- ja käsittelypaikkojen sijainnin tai sijaintien (alueet tai maat) osalta;
h) *vaatimustenmukaisuus ja seuranta*: todennettava, että pilvipalvelun tarjoaja noudattaa kansainvälisesti tunnustettuja tietoturvastandardeja ja on toteuttanut asianmukaiset tietoturvan valvontatoimet (esimerkiksi pyytämällä pilvipalvelun tarjoajaa toimittamaan todisteet siitä, että se suorittaa asianmukaiset tietoturvatarkistukset, ja suorittamalla säännöllisesti pilvipalvelun tarjoajan tietoturvajärjestelyjä koskevat arvioinnit ja testit).

## Suuntaviiva 5. Irtautumisstrategiat

31. Jos kyseessä on kriittisten tai tärkeiden toimintojen ulkoistaminen, yrityksen on varmistettava, että se voi irtautua pilvipalvelujen ulkoistamisjärjestelystä ilman, että sen liiketoiminnassa tai asiakkailleen toimittamissa palveluissa esiintyy kohtuuttomia häiriöitä, ja siten, että irtautuminen ei vaaranna yrityksen sovellettavan lainsäädännön mukaisten velvoitteiden noudattamista tai sen tietojen luottamuksellisuutta, eheyttä ja saatavuutta.

    Tätä varten yrityksen on:

    a) laadittava irtautumissuunnitelmat, jotka ovat kattavia, dokumentoituja ja riittävästi testattuja. Näitä suunnitelmia on päivitettävä tarpeen mukaan, myös silloin, kun ulkoistettuun toimintoon tehdään muutoksia;
    b) tunnistettava vaihtoehtoiset ratkaisut ja kehitettävä siirtymäsuunnitelmat ulkoistetun toiminnon ja tietojen poistamiseksi pilvipalvelun tarjoajan ja soveltuvissa tapauksissa alihankkijan hallinnasta ja siirrettävä ne yrityksen ilmoittamalla vaihtoehtoiselle pilvipalvelun tarjoajalle tai suoraan takaisin yritykselle. Näissä ratkaisuissa on huomioitava haasteet, joita tietojen sijainti voi aiheuttaa, ja tarvittavat toimet, joilla voidaan varmistaa liiketoiminnan jatkuvuus siirtymävaiheessa;
    c) varmistettava, että pilven ulkoistamista koskevassa kirjallisessa sopimuksessa velvoitetaan pilvipalvelun tarjoaja tukemaan ulkoistetun toiminnon asianmukaista siirtämistä (sekä tähän liittyvää tietojen käsittelyä) pilvipalvelun tarjoajalta ja mahdolliselta alihankkijalta yrityksen ilmoittamalle muulle pilvipalvelun tarjoajalle tai suoraan yritykselle, mikäli yritys käynnistää irtautumisstrategian. Ulkoistetun toiminnon asianmukaisen siirtämisen ja asiaan liittyvän tietojen käsittelyn tukemista koskevaan velvoitteeseen on tarvittaessa sisällyttävä tietojen turvallinen poistaminen pilvipalvelun tarjoajan ja mahdollisen alihankkijan järjestelmistä.

32. Laatiessaan edellä kohdissa a) ja b) tarkoitettuja irtautumissuunnitelmia ja -ratkaisuja (”irtautumisstrategia”) yrityksen on otettava huomioon seuraavat seikat:

    a) määritettävä irtautumisstrategian tavoitteet;
    b) määritettävä laukaisevat tapahtumat, joiden perusteella irtautumisstrategia voidaan käynnistää. Näihin on sisällyttävä vähintään pilvipalvelujen ulkoistamisjärjestelyä koskevan sopimuksen päättäminen yrityksen tai pilvipalvelun tarjoajan aloitteesta sekä pilvipalvelun tarjoajan liiketoiminnan päättyminen tai muu vakava keskeytys;
    c) laadittava vaikutusanalyysi, joka on oikeassa suhteessa ulkoistettuun toimintoon ja jossa määritetään, mitä henkilö- ja muita resursseja irtautumissuunnitelman toteuttamiseksi tarvitaan;
    d) osoitettava tehtävät ja vastuut irtautumisstrategian hallinnointia varten;
    e) testattava irtautumisstrategian soveltuvuus riskiperusteisen lähestymistavan avulla (esimerkiksi analysoimalla mahdolliset kustannukset, vaikutukset, resurssit ja ajalliset seuraamukset, jotka koituvat ulkoistetun palvelun siirtämisestä vaihtoehtoiselle palveluntarjoajalle);
    f) määritettävä siirtymän onnistumista koskevat kriteerit.

33. Yrityksen on sisällytettävä irtautumisstrategian laukaisevia tapahtumia koskevat indikaattorit omaan jatkuvaan seurantaansa ja valvontaansa, joiden kohteena ovat pilvipalvelun tarjoajan pilvipalvelujen ulkoistamisjärjestelyä koskevan sopimuksen mukaisesti suorittamat palvelut.

## Suuntaviiva 6. Käyttö- ja tarkastusoikeudet

34. Yrityksen on varmistettava, että pilvipalvelujen ulkoistamisjärjestelyä koskevalla kirjallisella sopimuksella ei rajoiteta toimivaltaisen viranomaisen mahdollisuutta käyttää tehokkaasti pilvipalvelun tarjoajaa koskevia käyttö- ja tarkastusoikeuksia ja valvontavaihtoehtoja.

35. Yrityksen on varmistettava, että käyttö- ja tarkastusoikeuksien käyttämisessä (esimerkiksi tarkastusten tiheys ja tarkastuksen kohteena olevat alueet ja palvelut) otetaan huomioon se, onko kyseessä kriittisen tai tärkeän toiminnon ulkoistaminen, sekä yritykselle pilvipalvelujen ulkoistamisjärjestelystä aiheutuvien riskien ja vaikutusten luonne ja laajuus.

36. Mikäli käyttö- ja tarkastusoikeuksien tai tiettyjen tarkastustekniikoiden käyttö muodostaa riskin pilvipalvelun tarjoajan ympäristölle ja/tai toisen pilvipalvelun tarjoajan asiakkaalle (esimerkiksi vaikuttamalla palvelutasoihin tai tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen), pilvipalvelun tarjoajan on esitettävä yritykselle selkeät perustelut siitä, miksi tällainen riski muodostuu, ja sovittava yrityksen kanssa vaihtoehtoisista tavoista saavuttaa vastaava tulos (esimerkiksi erityisten testattavien valvontakeinojen sisällyttäminen pilvipalvelun tarjoajan toimittamaan erityiseen kertomukseen/sertifikaattiin).

37. Yritykset voivat tehostaa tarkastusresurssien käyttöä ja pienentää pilvipalvelujen tarjoajan ja asiakkaiden organisatorista taakkaa seuraavin tavoin ilman, että yritysten lopullista vastuuta pilvipalvelujen ulkoistamisjärjestelyistä rajoitetaan:

    a) pilvipalvelun tarjoaja antaa saataville kolmannen osapuolen sertifioinnit ja ulkoiset tai sisäiset tarkastuskertomukset;
    b) käytetään yhteisiä tarkastuksia, jotka suoritetaan yhdessä saman pilvipalvelun tarjoajan muiden asiakkaiden kanssa tai jotka suorittaa kolmantena osapuolena toimiva tarkastaja, jonka nimittävät useat saman pilvipalvelun tarjoajan asiakkaat.

38. Jos ulkoistetaan kriittisiä tai tärkeitä toimintoja, yrityksen on arvioitava, ovatko kohdan 37 alakohdassa a) tarkoitetut kolmannen osapuolen sertifikaatit ja ulkoiset tai sisäiset tarkastuskertomukset asianmukaisia ja riittäviä sen sovellettavan lainsäädännön mukaisten velvoitteiden täyttämiseksi, ja pidemmällä aikavälillä yrityksen on pyrittävä olemaan turvautumatta ainoastaan kyseisiin sertifikaatteihin ja kertomuksiin.

39. Jos kriittisiä tai tärkeitä toimintoja ulkoistetaan, yrityksen olisi käytettävä kohdan 37 alakohdassa a) tarkoitettuja kolmannen osapuolen sertifikaatteja ja ulkoisia tai sisäisiä tarkastuskertomuksia vain, jos

    a) yritys luottaa siihen, että sertifioinnin tai tarkastuskertomuksen laajuus kattaa pilvipalvelun tarjoajan keskeiset järjestelmät (esimerkiksi prosessit, sovellukset, infrastruktuurin, tietokeskukset), yrityksen tunnistamat keskeiset valvontatoimet sekä asiaankuuluvan sovellettavan lainsäädännön noudattamisen;
    b) yritys arvioi säännöllisesti sertifiointien tai tarkastuskertomusten sisällön perusteellisesti ja todentaa, että sertifioinnit tai kertomukset eivät ole vanhentuneet;
    c) yritys varmistaa, että sertifioinnin tai tarkastuskertomusten tulevat versiot kattavat pilvipalvelun tarjoajan keskeiset järjestelmät ja valvontakeinot;
    d) yritys on varmistunut sertifioinnin tai tarkastuksen suorittavan tahon luotettavuudesta (esimerkiksi sen pätevyyden ja kelpoisuuden, asiantuntemuksen ja perusteena olevan tarkastushavaintojen näytön uudelleen hankkimisen/todentamisen sekä sertifioinnin tai tarkastuksen suorittavan yrityksen rotaation osalta);
    e) yritys luottaa siihen, että sertifioinnit annetaan ja tarkastukset tehdään asianmukaisten normien mukaisesti ja niihin sisältyy käytössä olevien keskeisten valvontakeinojen tehokkuuden testaaminen;
    f) yrityksellä on sopimukseen perustuva oikeus pyytää laajentamaan sertifiointia tai tarkastuskertomusta koskemaan muita pilvipalvelun tarjoajan oleellisia järjestelmiä tai valvontakeinoja edellyttäen, että laajuuden muutosta koskevien pyyntöjen määrä ja toistuvuus on kohtuullinen ja perusteltu riskinhallinnan näkökulmasta;
    g) yrityksellä säilyy sopimusperusteinen oikeus tehdä halutessaan paikalla yksittäisiä tarkastuksia, jotka koskevat ulkoistettua toimintoa.

40. Yrityksen on varmistettava, että ennen kuin paikalla käydään, myös silloin kun kyseessä on yrityksen nimittämän kolmannen osapuolen (esimerkiksi tarkastajan) käynti, pilvipalvelun tarjoajalle annetaan asiasta ennakkoilmoitus kohtuullisessa ajassa, paitsi jos varhainen ennakkoilmoitus ei ole mahdollinen hätätilan tai kriisitilanteen vuoksi tai jos sen antaminen johtaisi tilanteeseen, jossa tarkastus ei olisi enää tehokas. Ilmoituksessa on eriteltävä käyntikohde, käynnin tarkoitus ja käynnille osallistuva henkilöstö.

41. Ottaen huomioon, että pilvipalvelut ovat teknisesti erittäin monimutkaisia ja niihin liittyy erityisiä lainkäyttövaltaa koskevia haasteita, tarkastuksen suorittavilla työntekijöillä – jotka ovat joko yrityksen tarkastajia tai yrityksen puolesta toimivia tarkastajia – on oltava oikeat taidot ja tietämys oleellisten pilvipalvelujen asianmukaista arviointia ja tehokkaan ja asiaankuuluvan tarkastuksen suorittamista varten. Tätä on sovellettava myös silloin, kun yrityksen työntekijät tarkistavat palvelun tarjoajan toimittamat sertifikaatit tai tarkastuskertomukset.

## Suuntaviiva 7. Edelleen ulkoistaminen

42. Jos kriittisten tai tärkeiden toimintojen (tai niiden olennaisten osien) ulkoistaminen edelleen on sallittua, yrityksen ja pilvipalvelujen tarjoajan tekemässä pilvipalvelujen ulkoistamisjärjestelyä koskevassa kirjallisessa sopimuksessa on

    a) täsmennettävä ulkoistettavan toiminnon kaikki osat tai näkökohdat, jotka suljetaan mahdollisen edelleen ulkoistamisen ulkopuolelle;
    b) määritettävä ehdot, joita on noudatettava edelleen ulkoistamisessa;
    c) täsmennettävä, että pilvipalvelun tarjoaja pysyy vastuuvelvollisena ja on velvollinen valvomaan edelleen ulkoistamiaan palveluita ja varmistamaan, että pilvipalvelun tarjoajan ja yrityksen välisiä kaikkia sopimusvelvoitteita noudatetaan jatkuvasti;
    d) määritettävä pilvipalvelun tarjoajan velvoite ilmoittaa yritykselle kaikesta aiotusta edelleen ulkoistamisesta tai siihen tehtävistä olennaisista muutoksista, erityisesti mikäli tämä voi vaikuttaa pilvipalvelun tarjoajan kykyyn täyttää yrityksen kanssa tehdyn pilvipalvelujen ulkoistamisjärjestelyn mukaiset velvoitteensa. Kirjallisessa sopimuksessa asetetun ilmoitusajan on oltava sellainen, että yrityksellä on riittävästi aikaa suorittaa vähintään ehdotettua edelleen ulkoistamista tai siihen tehtäviä olennaisia muutoksia koskeva riskinarviointi ja joko vastustaa tai nimenomaisesti hyväksyä edelleen ulkoistaminen tai muutokset, kuten jäljempänä alakohdassa e) todetaan;
    e) varmistettava, että yrityksellä on oikeus vastustaa aiottua edelleen ulkoistamista tai siihen tehtäviä olennaisia muutoksia tai että nimenomaista hyväksyntää edellytetään ennen kuin ehdotettu edelleen ulkoistaminen tai olennaiset muutokset tulevat voimaan;
    f) varmistettava, että yrityksellä on sopimusperusteinen oikeus päättää pilvipalvelun tarjoajan kanssa tehty pilvipalvelujen ulkoistamisjärjestely, jos yritys vastustaa aiottua edelleen ulkoistamista tai siihen tehtäviä olennaisia muutoksia tai jos edelleen ulkoistaminen on perusteeton (esimerkiksi tapauksessa, jossa pilvipalvelun tarjoaja aloittaa edelleen ulkoistamisen ilmoittamatta yritykselle tai edelleen ulkoistaminen rikkoo vakavasti ulkoistamissopimuksessa määritettyjä edelleen ulkoistamista koskevia ehtoja).

43. Yrityksen on varmistettava, että pilvipalvelun tarjoaja valvoo alihankkijaa asianmukaisesti.

## Suuntaviiva 8. Kirjallinen ilmoitus toimivaltaisille viranomaisille

44. Yrityksen on ilmoitettava toimivaltaiselle viranomaiselleen kirjallisesti ja ajoissa suunnitteilla olevista pilvipalvelujen ulkoistamisjärjestelyistä, jotka koskevat kriittistä tai tärkeää toimintoa. Lisäksi yrityksen on ilmoitettava toimivaltaiselle viranomaiselleen kirjallisesti ja ajoissa sellaisista pilvipalvelujen ulkoistamisjärjestelyistä, jotka koskevat aiemmin muuksi kuin kriittiseksi tai tärkeäksi luokiteltua toimintoa, josta on sittemmin tullut kriittinen tai tärkeä.

45. Yrityksen kirjallisessa ilmoituksessa on annettava suhteellisuusperiaatteen mukaisesti vähintään seuraavat tiedot:

    a) pilvipalvelujen ulkoistamisjärjestelyä koskevan sopimuksen alkamispäivä ja tarvittaessa sopimuksen seuraava uusimispäivä, päättymispäivä ja/tai pilvipalvelun tarjoajaa ja yritystä koskevat irtisanomisajat;
    b) ulkoistettavan toiminnon lyhyt kuvaus;
    c) lyhyt tiivistelmä syistä, joiden vuoksi ulkoistettu toiminta katsotaan kriittiseksi tai tärkeäksi;
    d) pilvipalvelun tarjoajan nimi ja (mahdollinen) tuotenimi, rekisteröintimaa, yrityksen rekisterinumero, oikeushenkilötunnus (jos saatavissa), rekisteröity osoite ja muut oleelliset yhteystiedot sekä mahdollisen emoyhtiön nimi;
    e) pilven ulkoistamista koskevaa sopimusta säätelevä lainsäädäntö sekä mahdollinen lainkäyttövallan valinta;
    f) pilvipalvelun käyttöönottomallit ja pilvipalvelun tarjoajan säilyttämien tietojen erityisluonne sekä sijainnit (alueet tai maat), joissa kyseisiä tietoja säilytetään;
    g) kriittisen tai tärkeän ulkoistetun toiminnon viimeisimmän arvioinnin päivämäärä.
    h) pilvipalvelun tarjoajan viimeisimmän riskinarvioinnin/tarkastuksen päivämäärä ja lyhyt tiivistelmä tärkeimmistä tuloksista sekä seuraavan suunnitellun riskinarvioinnin tai tarkastuksen päivämäärä;
    i) yrityksessä henkilö tai päätöksentekoelin, joka on hyväksynyt pilvipalvelujen ulkoistamisjärjestelyn;
    j) mahdollisten sellaisten alihankkijoiden nimet, joille kriittisten tai tärkeiden toimintojen oleelliset osat on ulkoistettu edelleen, mukaan lukien maa, tai alue, jossa alihankkijat ovat rekisteröityneet ja jossa edelleen ulkoistettu palvelu toteutetaan sekä tarvittaessa sijainti, jossa tietoja säilytetään.

## Suuntaviiva 9. Pilvipalvelujen ulkoistamisjärjestelyjen valvonta

46. Toimivaltaisten viranomaisten on arvioitava yrityksen pilvipalvelujen ulkoistamisjärjestelyistä aiheutuvat riskit osana valvontamenettelyään. Arvioinnissa on erityisesti keskityttävä järjestelyihin, jotka liittyvät kriittisten tai tärkeiden toimintojen ulkoistamiseen.

47. Toimivaltaisten viranomaisten on varmistettava, että ne pystyvät valvomaan yrityksiä tehokkaasti erityisesti silloin, kun nämä ulkoistavat kriittisiä tai tärkeitä toimintoja, jotka toteutetaan EU:n ulkopuolella.

48. Toimivaltaisten viranomaisten on arvioitava riskiperusteisen lähestymistavan perusteella

    a) onko yrityksillä käytössä oleelliset hallinnolliset, resursseja koskevat ja toiminnalliset menettelyt, jotta ne voivat asianmukaisesti ja tehokkaasti tehdä, toteuttaa ja valvoa pilvipalvelujen ulkoistamisjärjestelyjä;
    b) tunnistavatko ja arvioivatko yritykset kaikki pilvipalvelujen ulkoistamisjärjestelyyn liittyvät oleelliset riskit.

49. Mikäli havaitaan keskittämistä koskevia riskejä, toimivaltaisten viranomaisten on seurattava kyseisten riskien kehittymistä ja arvioitava niiden mahdollista vaikutusta muihin valvomiinsa yrityksiin ja rahoitusmarkkinoiden vakauteen.