

Ohjeet



Suuntaviivat 06/2020 toisen maksupalveludirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta

Versio 2.0

Hyväksytty 15. joulukuuta 2020

Versioyhteenveto

Versio 2.0	15.12.2020	Suuntaviivojen hyväksyminen julkisen kuulemisen jälkeen
Versio 1.0	17.7.2020	Suuntaviivojen hyväksyminen julkista kuulemista varten

Sisällysluettelo

1.	Johdanto.....	5
1.1	Määritelmät.....	6
1.2	Toisen maksupalveludirektiivin mukaiset palvelut	7
2	Toisen maksupalveludirektiivin mukaiset lailliset perusteet ja jatkokäsittely	10
2.1	Käsittelyn lailliset perusteet	10
2.2	Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta (käsittely on tarpeen sopimuksen täytäntöön panemiseksi)	10
2.3	Petostentorjunta	12
2.4	Jatkokäsittely (tilitietopalvelun tarjoajat ja maksutoimeksiantopalvelun tarjoajat)	12
2.5	Tiliin pääsyn oikeudellinen peruste (tiliä ylläpitävät maksupalveluntarjoajat).....	13
3	Nimenomainen suostumus	15
3.1	Yleisen tietosuoja-asetuksen mukainen suostumus	15
3.2	Toisen maksupalveludirektiivin mukainen suostumus	15
3.2.1	Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukainen nimenomainen hyväksyntä.....	16
3.3	Päätelmät	18
4	Hiljaisen osapuolen tietojen käsittely	19
4.1	Hiljaisen osapuolen tiedot.....	19
4.2	Rekisterinpitäjän oikeutettu etu	19
4.3	Hiljaisen osapuolen henkilötietojen jatkokäsittely	19
5	Toisen maksupalveludirektiivin mukainen erityisiä henkilötietoryhmiä koskeva käsittely	21
5.1	Eryiset henkilötietoryhmät	21
5.2	Mahdolliset poikkeukset	22
5.3	Tärkeä yleinen etu	22
5.4	Nimenomainen suostumus	22
5.5	Ei soveltuvaa poikkeusta	23
6	Tietojen minimointi, turvallisuus, läpinäkyvyys, tilivelvollisuus ja profilointi	24
6.1	Tietojen minimointi ja sisäänrakennettu ja oletusarvoinen tietosuoja	24
6.2	Tietojen minimointia koskevat toimenpiteet.....	24
6.3	Turvallisuus.....	26
6.4	Läpinäkyvyys ja tilivelvollisuus	26
6.5	Profilointi	28

Euroopan tietosuojaneuvosto

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annettun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018¹,

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

sekä katsoo seuraavaa:

(1) Yleisessä tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista yhdenmukaisista säännöistä kaikkialla EU:ssa.

(2) Toisella maksupalveludirektiivillä (23 päivänä joulukuuta 2015 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366) kumotaan direktiivi 2007/64/EY, ja siinä säädetään uusista säännöistä, joilla varmistetaan kuluttajien, kauppiaiden ja yritysten oikeusvarmuus maksuketjussa ja nykyaikaistetaan maksupalvelumarkkinoiden oikeudellista kehystä². Jäsenvaltioiden oli saatettava toinen maksupalveludirektiivi osaksi kansallista lainsäädäntöään 13. tammikuuta 2018 mennessä.

(3) Toisen maksupalveludirektiivin tärkeä piirre on uusia maksutoimeksiantopalveluja ja tilitietopalveluja koskevan oikeudellisen kehysten käyttöönotto. Toisella maksupalveludirektiivillä annetaan uusille maksupalveluntarjoajille pääsy rekisteröityjen maksutileille kyseisten palvelujen tarjoamista varten.

(4) Toisen maksupalveludirektiivin 94 artiklan 1 kohdan mukaisesti tietosuojan osalta kaikessa henkilötietojen käsittelyssä, mukaan lukien käsittelyä koskevien tietojen antaminen toista maksupalveludirektiiviä sovellettaessa, on noudatettava yleistä tietosuoja-asetusta³ ja asetusta (EU) 2018/1725.

(5) Toisen maksupalveludirektiivin johdanto-osan 89 kappaleessa todetaan, että kun henkilötietoja käsitellään toisen maksupalveludirektiivin soveltamiseksi, olisi erityisesti mainittava käsittelyn täsmällinen tarkoitus, viitattava asiaankuuluvaan oikeusperustaan ja noudatettava asiaankuuluvia yleisessä tietosuoja-asetuksessa säädettyjä turvallisuusvaatimuksia sekä kunnioitettava tarpeellisuuden, oikeasuhteisuuden, käyttötarkoituksen rajoittamisen ja tietojen säilyttämisen oikeasuhteisen enimmäisajan periaatteita. Kaikkiin toisen maksupalveludirektiivin puitteissa kehitettäviin ja sovellettaviin tietojenkäsittelyjärjestelmiin olisi myös sisällyttävä sisäänrakennettu tietosuoja ja oletusarvoinen tietosuoja.⁴

(6) Toisen maksupalveludirektiivin johdanto-osan 93 kappaleessa todetaan, että yhtäältä maksutoimeksiantopalvelun tarjoajien ja tilitietopalvelun tarjoajien sekä toisaalta tiliä ylläpitävien

¹ Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETAn jäsenvaltioita.

² Toisen maksupalveludirektiivin johdanto-osan 6 kappale.

³ Koska toinen maksupalveludirektiivi on annettu ennen yleistä tietosuoja-asetusta, siinä viitataan edelleen direktiiviin 95/46. Yleisen tietosuoja-asetuksen 94 artiklassa säädetään, että viittauksia kumottuun direktiiviin 95/46/EY pidetään viittauksina yleiseen tietosuoja-asetukseen.

⁴ Toisen maksupalveludirektiivin johdanto-osan 89 kappale.

maksupalveluntarjoajien olisi noudatettava tässä direktiivissä säädettyjä tai tarkoitettuja tai teknisiin sääntelystandardeihin sisältyviä tarvittavia tietosuoja- ja turvallisuusvaatimuksia.

ON HYVÄKSYNYT SEURAAVAT SUUNTAVIIVAT:

1. JOHDANTO

1. Toisella maksupalveludirektiivillä on otettu käyttöön useita maksupalvelualan uudistuksia. Vaikka toisen maksupalveludirektiivin soveltaminen luo uusia mahdollisuuksia kuluttajille ja lisää läpinäkyvyyttä tällä alalla, sen soveltaminen nostaa esille tiettyjä kysymyksiä ja huolenaiheita, jotka liittyvät siihen, että rekisteröityjen tulisi edelleen pystyä valvomaan henkilötietojaan täysimääräisesti. Yleistä tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, mukaan lukien toisessa maksupalveludirektiivissä määriteltyjen maksupalvelujen yhteydessä suoritettaviin käsittelytoimiin.⁵ Näin ollen toisen maksupalveludirektiivin soveltamisalaan kuuluvilla aloilla toimivien rekisterinpitäjien on aina varmistettava, että yleisen tietosuoja-asetuksen vaatimuksia, muun muassa sen 5 artiklassa säädettyjä tietosuojaperiaatteita, ja sovellettavia sähköisen viestinnän tietosuojadirektiivin⁶ säännöksiä noudatetaan. Vaikka toinen maksupalveludirektiivi⁷ ja asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevat tekniset sääntelystandardit, jäljempänä 'tekniset sääntelystandardit'⁸, sisältävät tiettyjä tietosuojaa ja tietoturva koskevia säännöksiä, näiden säännösten tulkinnasta ja yleisen tietosuojakehyksen ja toisen maksupalveludirektiivin välisestä vuorovaikutuksesta on syntynyt epävarmuutta.
2. Euroopan tietosuojaneuvosto julkaisi 5. heinäkuuta 2018 toista maksupalveludirektiiviä koskevan kirjeen, jossa se selvensi henkilötietojen suojaan liittyviä kysymyksiä toisen maksupalveludirektiivin näkökulmasta, erityisesti tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien suorittamaa muiden kuin sopimuspuolten henkilötietojen (ns. silent party -datan eli hiljaisen osapuolen tietojen) käsittelyä, suostumuksen antamiseen ja peruuttamiseen liittyviä menettelyjä, teknisiä sääntelystandardeja sekä tiliä ylläpitävien maksupalveluntarjoajien välistä turvatoimia koskevaa yhteistyötä. Näiden suuntaviivojen valmistelutyöhön kuului palautteen kerääminen sidosryhmiltä sekä kirjallisesti että sidosryhmätapahtumassa kiireellisimpien haasteiden tunnistamiseksi.
3. Näillä suuntaviivoilla on tarkoitus antaa lisäohjeita tietosuojanäkökohdista toisen maksupalveludirektiivin kannalta ja erityisesti yleisen tietosuoja-asetuksen ja toisen maksupalveludirektiivin asiaa koskevien säännösten välisestä suhteesta. Näissä suuntaviivoissa keskitytään pääasiassa siihen, miten tilitietopalvelun tarjoajat ja maksutoimeksiantopalvelun

⁵ Yleisen tietosuoja-asetuksen 1 artiklan 1 kohta.

⁶ Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37–47).

⁷ Muun muassa maksupalveludirektiivin 94 artikla.

⁸ Komission delegoitu asetus (EU) 2018/389, annettu 27 päivänä marraskuuta 2017, Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (ETA:n kannalta merkityksellinen teksti); C/2017/7782 (EUVL L 69, 13.3.2018, s. 23–43), saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32018R0389&from=EN>

tarjoajat käsittelevät henkilötietoja. Tässä asiakirjassa käsitellään näin ollen tiliä ylläpitävien maksupalveluntarjoajien antamaa pääsyä maksutilitetoihin koskevia ehtoja ja maksutoimeksiantopalvelun tarjoajien ja tilitietopalvelun tarjoajien suorittamaa henkilötietojen käsittelyä, mukaan lukien vaatimukset ja suoja-toimet, jotka koskevat maksutoimeksiantopalvelun tarjoajien ja tilitietopalvelun tarjoajien suorittamaa henkilötietojen käsittelyä muihin tarkoituksiin kuin siihen alkuperäiseen tarkoitukseen, jota varten tiedot on kerätty, erityisesti silloin, kun ne on kerätty tilitietopalvelun⁹ tarjoamisen yhteydessä. Tässä asiakirjassa käsitellään myös toisen maksupalveludirektiivin ja yleisen tietosuoja-asetuksen mukaisia nimenomaisen suostumuksen eri käsitteitä, ”hiljaisen osapuolen tietojen” käsittelyä, maksutoimeksiantopalvelun tarjoajien ja tilitietopalvelun tarjoajien suorittamaa erityisten henkilötietoryhmien käsittelyä ja yleisessä tietosuoja-asetuksessa vahvistettujen keskeisten tietosuojaperiaatteiden soveltamista, mukaan lukien tietojen minimointi, läpinäkyvyys, osoitusvelvollisuus ja turvatoimet. Toinen maksupalveludirektiivi sisältää muun muassa kuluttajansuojaa ja kilpailuoikeutta koskevia monialaisia vastuita. Näitä oikeudenaloja koskevat näkökohdat eivät kuulu näiden suuntaviivojen soveltamisalaan.

4. Lukemisen helpottamiseksi tässä asiakirjassa käytetyt keskeiset määritelmät esitetään jäljempänä.

1.1 Määritelmät

’Tilitietopalvelun tarjoajalla’ tarkoitetaan sellaisen verkkopalvelun tarjoajaa, jonka kautta annetaan koottua tietoa yhdestä tai useammasta maksutilistä, jotka maksupalvelunkäyttäjällä on joko toisen maksupalveluntarjoajan tai useamman kuin yhden maksupalveluntarjoajan hallinnassa;

’Tiliä ylläpitävällä maksupalveluntarjoajalla’ tarkoitetaan sellaista maksupalveluntarjoajaa, joka tarjoaa maksajalle maksutilejä ja hoitaa niitä;

’Tietojen minimointi’ on tietosuojaperiaate, jonka mukaan henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettava siihen, mikä on välttämätöntä niiden käsittelyn tarkoitusten kannalta;

’Maksajalla’ tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka on maksutilin haltija ja joka antaa luvan maksutoimeksiantoon kyseiseltä maksutililtä tai, jos maksutiliä ei ole, luonnollista henkilöä tai oikeushenkilöä, joka antaa maksutapahtumaa koskevan toimeksiannon;

’Maksunsaajalla’ tarkoitetaan luonnollista tai oikeushenkilöä, joka on tarkoitettu maksutapahtuman kohteena olevien varojen vastaanottajaksi;

’Maksutilillä’ tarkoitetaan yhden tai useamman maksupalvelunkäyttäjän nimissä olevaa tiliä, jota käytetään maksutapahtumien toteuttamiseen;

’Maksutoimeksiantopalvelun tarjoajalla’ tarkoitetaan sellaisen palvelun tarjoajaa, jossa maksutoimeksiannon käynnistämiseksi maksupalvelunkäyttäjän pyynnöstä toteutetaan palvelu toisen maksupalveluntarjoajan hallussa olevan maksutilin osalta;

⁹ Tilitietopalvelu on verkkopalvelu, jonka kautta annetaan koottua tietoa yhdestä tai useammasta maksutilistä, jotka maksupalvelunkäyttäjällä on joko toisen maksupalveluntarjoajan tai useamman kuin yhden maksupalveluntarjoajan hallussa.

'Maksupalveluntarjoajalla' tarkoitetaan toisen maksupalveludirektiivin 1 artiklan 1 kohdassa¹⁰ tarkoitettua laitosta tai luonnollista henkilöä tai oikeushenkilöä, joka kuuluu soveltamatta jättämisen piiriin toisen maksupalveludirektiivin 32 tai 33 artiklan nojalla;

'Maksupalvelunkäyttäjällä' luonnollista tai oikeushenkilöä, joka käyttää maksupalvelua joko maksajan tai maksunsaajan tai molempien ominaisuudessa;

'Henkilötiedoilla' tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä *'rekisteröity'*, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella;

'Sisäänrakennetulla tietosuojalla' tarkoitetaan tuotteeseen tai palveluun sisällytettyjä teknisiä ja organisatorisia toimenpiteitä, joilla on tarkoitus panna tehokkaasti täytäntöön tietosuojaperiaatteet ja sisällyttää tarvittavat suoja-toimet käsittelyn osaksi, jotta käsittely vastaisi yleisen tietosuoja-asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin;

'Oletusarvoisella tietosuojalla' tarkoitetaan tuotetta tai palvelua koskevia asianmukaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja;

'Teknisillä sääntelystandardeilla' tarkoitetaan 27 päivänä marraskuuta 2017 annettua komission delegeoitua asetusta (EU) 2018/389 Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla;

'Kolmansilla palveluntarjoajilla' tarkoitetaan sekä maksutoimeksiantopalvelun tarjoajia että tilitietopalvelun tarjoajia.

1.2 Toisen maksupalveludirektiivin mukaiset palvelut

5. Toisella maksupalveludirektiivillä otetaan käyttöön kaksi uudentyyppistä maksupalvelua (maksupalvelujen palveluntarjoajaa) eli maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat. Toisen maksupalveludirektiivin liite I sisältää kahdeksan toisen maksupalveludirektiivin soveltamisalaan kuuluvaa maksupalvelua.

¹⁰ Toisen maksupalveludirektiivin 1 artiklan 1 kohdassa säädetään, että toisessa maksupalveludirektiivissä vahvistetaan säännöt, joiden mukaisesti jäsenvaltioiden on jaettava *maksupalveluntarjoajat* seuraaviin ryhmiin:

- a) Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 1 alakohdassa määritellyt luottolaitokset, mukaan lukien niiden mainitun kohdan 17 alakohdassa tarkoitettut sivuliikkeet, jos tällaiset sivuliikkeet sijaitsevat unionissa, siitä riippumatta, sijaitsevatko niiden päätoimipaikat unionissa tai direktiivin 2013/36/EU 47 artiklan ja kansallisen lainsäädännön mukaisesti unionin ulkopuolella;
- b) direktiivin 2009/110/EY 2 artiklan 1 kohdassa tarkoitettut sähköisen rahan liikkeeseenlaskijalaitokset, mukaan lukien – mainitun direktiivin 8 artiklan ja kansallisen lainsäädännön mukaisesti – niiden sivukonttorit, jos tällaiset sivukonttorit sijaitsevat unionissa ja niiden päätoimipaikat sijaitsevat unionin ulkopuolella, siltä osin kuin näiden sivukonttoreiden maksupalvelut liittyvät sähköisen rahan liikkeeseen laskemiseen;
- c) postisiirtoa hoitavat laitokset, joilla on kansallisen lainsäädännön nojalla oikeus tarjota maksupalveluja;
- d) maksulaitokset;
- e) EKP ja kansalliset keskuspankit, kun ne eivät toimi raha- tai muina viranomaisina;
- f) jäsenvaltiot tai niiden alueelliset tai paikalliset viranomaiset, kun ne eivät toimi viranomaisina.

6. Maksutoimeksiantopalvelun tarjoajat tarjoavat maksutoimeksiantojen käynnistämiseksi maksupalvelunkäyttäjän pyynnöstä toteutettavia palveluja toisen maksupalveluntarjoajan hallussa olevan maksutilin osalta.¹¹ Maksutoimeksiantopalvelun tarjoaja voi pyytää tiliä ylläpitävää maksupalveluntarjoajaa (tavallisesti pankkia) käynnistämään tapahtuman maksupalvelunkäyttäjän puolesta. Käyttäjä (maksupalvelunkäyttäjä) voi olla luonnollinen henkilö (eli rekisteröity) tai oikeushenkilö.
7. Tilitietopalvelun tarjoajat tarjoavat verkkopalveluja, joiden kautta annetaan koottua tietoa yhdestä tai useammasta maksutilistä, jotka maksupalvelunkäyttäjällä on joko toisen maksupalveluntarjoajan tai useamman kuin yhden maksupalveluntarjoajan hallussa.¹² Maksupalvelunkäyttäjä voi toisen maksupalveludirektiivin johdanto-osan 28 kappaleen mukaisesti saada kokonaiskuvan rahoitustilanteestaan välittömästi minä hyvänsä ajankohtana.
8. Tilitietopalvelut voivat sisältää useita erityyppisiä palveluja, joissa painotetaan erilaisia ominaisuuksia ja käyttötarkoituksia. Jotkin palveluntarjoajat voivat esimerkiksi tarjota käyttäjille talousarvion suunnittelun ja menojen seurannan kaltaisia palveluja. Näiden palvelujen yhteydessä suoritettava henkilötietojen käsittely kuuluu toisen maksupalveludirektiivin soveltamisalaan. Palvelut, joihin sisältyy maksupalvelunkäyttäjän luottokelpoisuuden arviointia, tai tilintarkastuspalvelut, jotka perustuvat tilitietopalvelun kautta tapahtuvaan tiedonkeruuseen, eivät kuulu toisen maksupalveludirektiivin soveltamisalaan, joten ne kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan. Lisäksi sellaiset tilit, jotka eivät ole maksutilejä (esimerkiksi säästötilit ja sijoitustilit), eivät myöskään kuulu toisen maksupalveludirektiivin soveltamisalaan. Yleinen tietosuoja-asetus on joka tapauksessa henkilötietojen käsittelyyn sovellettava oikeudellinen kehys.

Esimerkki 1:

HappyPayments on yritys, joka ylläpitää verkkopalvelua, joka koostuu yhden tai useamman maksutilin tietojen toimittamisesta mobiilisovelluksen kautta taloudellisen valvonnan (tilitietopalvelu) tarjoamiseksi. Tämän palvelun avulla maksupalvelunkäyttäjä näkee nopeasti kahdessa tai useammassa eri pankissa olevien maksutilien saldot ja viimeaikaiset tapahtumat. Lisäksi maksupalvelunkäyttäjä voi halutessaan luokitella menot ja tulot eri luokkien (muun muassa palkka, vapaa-aika, energia ja asuntolaina) mukaan, mikä auttaa maksupalvelunkäyttäjää suunnittelemaan talouttaan. HappyPayments tarjoaa tämän sovelluksen kautta myös palvelua, jonka avulla käyttäjät voivat käynnistää maksuja suoraan määritellyiltä maksutileiltä (maksutoimeksiantopalvelu).

9. Toisessa maksupalveludirektiivissä säädetään näiden palvelujen tarjoamisen osalta oikeudellisista edellytyksistä, joiden mukaisesti maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat voivat käyttää maksutilejä tarjotakseen maksupalvelunkäyttäjälle palvelua.
10. Toisen maksupalveludirektiivin 66 artiklan 1 kohdassa ja 67 artiklan 1 kohdassa säädetään, että maksu- ja tilitietopalvelujen saaminen ja käyttö ovat maksupalvelunkäyttäjän oikeuksia. Tämä tarkoittaa sitä, että maksupalvelunkäyttäjän olisi pystyttävä käyttämään kyseistä oikeutta täysin vapaasti ja että maksupalvelunkäyttäjää ei voida pakottaa käyttämään tätä oikeutta.
11. Pääsyä maksutileihin ja maksutilitietojen käyttöä säännellään osittain toisen maksupalveludirektiivin 66 ja 67 artiklassa, jotka sisältävät tietojen (henkilötietojen) suoja

¹¹ Toisen maksupalveludirektiivin 4 artiklan 15 kohta.

¹² Toisen maksupalveludirektiivin 4 artiklan 16 kohta.

koskevia suojatoimia. Toisen maksupalveludirektiivin 66 artiklan 3 kohdan f alakohdassa säädetään, että maksutoimeksiantopalvelun tarjoaja ei saa pyytää maksupalvelunkäyttäjältä mitään muita tietoja kuin ne, jotka tarvitaan maksutoimeksiantopalvelua varten, ja toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohdassa säädetään, että maksutoimeksiantopalvelun tarjoajat eivät saa käyttää, hankkia eivätkä säilyttää mitään tietoja muussa tarkoituksessa kuin maksajan nimenomaisesti pyytämän maksutoimeksiantopalvelun suorittamiseksi. Lisäksi maksupalveludirektiivin 67 artiklan 2 kohdan d alakohdassa rajoitetaan tilitietopalvelun tarjoajien pääsy ainoastaan nimettyjen maksutilien tietoihin ja niihin liittyviin maksutapahtumiin, kun taas toisen maksupalveludirektiivin 67 artiklan 2 kohdan f alakohdassa säädetään, että tilitietopalvelun tarjoajat eivät saa käyttää, hankkia eivätkä säilyttää mitään tietoja muussa tarkoituksessa kuin maksupalvelunkäyttäjän nimenomaisesti pyytämän tilitietopalvelun suorittamiseksi tietosuojasääntöjen mukaisesti. Viimeksi mainitussa korostetaan sitä, että tilitietopalvelujen yhteydessä henkilötietoja voidaan kerätä vain tiettyä nimenomaista ja laillista tarkoitusta varten. Sen vuoksi tilitietopalvelun tarjoajan on ilmoitettava sopimuksessa selkeästi, mihin erityisiin tarkoituksiin henkilökohtaisia tilitietoja käsitellään sen tarjoaman tilitietopalvelun yhteydessä. Sopimuksen on oltava lainmukainen, kohtuullinen ja läpinäkyvä yleisen tietosuojasetuksen 5 artiklan mukaisesti, ja siinä on myös noudatettava muuta kuluttajansuojalainsäädäntöä.

12. Erityisistä olosuhteista riippuen maksupalveluntarjoajat voivat olla yleisen tietosuojasetuksen mukaisia rekisterinpitäjiä tai henkilötietojen käsittelijöitä. Näissä suuntaviivoissa 'rekisterinpitäjillä' tarkoitetaan niitä maksupalveluntarjoajia, jotka yksin tai yhdessä toisten kanssa määrittävät henkilötietojen käsittelyn tarkoitukset ja keinot. Lisätietoja tästä on tietosuojaneuvoston yleisen tietosuojasetuksen mukaisia rekisterinpitäjän ja henkilötietojen käsittelijän käsitteitä koskevissa suuntaviivoissa 07/2020.

2 TOISEN MAKSUPALVELUDIREKTIIVIN MUKAISET LAILLISET PERUSTEET JA JATKOKÄSITTELY

2.1 Käsitteilyn lailliset perusteet

13. Yleisen tietosuoja-asetuksen mukaisesti rekisterinpitäjillä on oltava oikeusperuste henkilötietojen käsittelylle. Yleisen tietosuoja-asetuksen 6 artiklan 1 kohta sisältää tyhjentävän ja rajoittavan luettelon kuudesta oikeusperusteesta, joita sovelletaan yleisen tietosuoja-asetuksen mukaiseen henkilötietojen käsittelyyn.¹³ Rekisterinpitäjän tehtävänä on määrittää asianmukainen oikeusperuste ja varmistaa, että kaikki tämän oikeusperusteen edellytykset täyttyvät. Pätevän ja tarkoituksenmukaisimman perusteen määrittäminen tietyssä tilanteessa riippuu olosuhteista, joissa käsittely tapahtuu, mukaan lukien käsittelyn tarkoitus ja rekisterinpitäjän ja rekisteröidyn välinen suhde.

2.2 Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta (käsitteily on tarpeen sopimuksen täytäntöön panemiseksi)

14. Maksupalveluja tarjotaan maksupalvelunkäyttäjän ja maksupalveluntarjoajan välillä sopimusperusteisesti. Kuten toisen maksupalveludirektiivin johdanto-osan 87 kappaleessa todetaan, "[t]ässä direktiivissä olisi käsiteltävä ainoastaan maksupalvelunkäyttäjän ja -tarjoajan välisiä sopimusvelvoitteita ja -vastuita." Yleisen tietosuoja-asetuksen osalta henkilötietojen käsittelyn tärkein oikeusperuste maksupalvelujen tarjoamiseksi on tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta, mikä tarkoittaa sitä, että käsittely on tarpeen joko sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

15. Toisen maksupalveludirektiivin mukaiset maksupalvelut määritellään toisen maksupalveludirektiivin liitteessä I. Näiden toisessa maksupalveludirektiivissä määriteltyjen palvelujen tarjoaminen on edellytys sellaisen sopimuksen tekemiselle, jossa osapuolilla on pääsy maksupalvelunkäyttäjän maksutilitietoihin. Näiden maksupalveluntarjoajien on myös oltava toimiluvan saaneita toimijoita. Toisen maksupalveludirektiivin mukaisten maksutoimeksiantopalvelujen ja tilitietopalvelujen osalta sopimukseen voi sisältyä ehtoja, joilla asetetaan ehtoja myös lisäpalveluille, joita ei säännellä toisella maksupalveludirektiivillä. Tietosuojaneuvoston suuntaviivoissa 2/2019 yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b

¹³ Käsitteily on 6 artiklan mukaisesti lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

- (a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
- (b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
- (c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
- (d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
- (e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
- (f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suoja edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä tehdään selväksi, että rekisterinpitäjien on arvioitava, mikä henkilötietojen käsittely on objektiivisesti tarpeen sopimuksen täytäntöön panemiseksi. Näissä suuntaviivoissa todetaan, että välttämättömyyden perusteleva riippuu palvelun luonteesta, sopimuspuolten keskinäisistä näkökulmista ja odotuksista, sopimuksen perusteluista ja sopimuksen oleellisista osista.

16. Tietosuojaneuvoston suuntaviivoissa 2/2019 tehdään myös selväksi, että yleisen tietosuojasetuksen 7 artiklan 4 kohdan perusteella erotellaan toisistaan sopimuksen täytäntöön panemiseksi tarpeelliset käsittelytoimet ja lausekkeet, joilla palvelun ehdoksi asetetaan tiettyjä käsittelytoimia, jotka eivät itse asiassa ole tarpeen sopimuksen täytäntöön panemiseksi. Välttämättömyys sopimuksen täytäntöön panemiseksi vaatii perusteeksi selvästi muutakin kuin sopimulausekkeen.¹⁴ Rekisterinpitäjän olisi voitava osoittaa, kuinka rekisteröidyn kanssa tehdyn kyseisen sopimuksen pääsisältöä ei voida tosiasiallisesti panna täytäntöön, ellei kyseessä olevia henkilötietoja käsitellä. Pelkkä sopimuksessa oleva viittaus tietojen käsittelyyn tai maininta siitä ei riitä siihen, että kyseinen käsittely kuuluu yleisen tietosuojasetuksen 6 artiklan 1 kohdan b alakohdan soveltamisalaan.
17. Yleisen tietosuojasetuksen 5 artiklan 1 kohdan b alakohdassa säädetään käyttötarkoitussidonnaisuutta koskevasta periaatteesta, jonka perusteella henkilötiedot on kerättävä tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Kun arvioidaan, onko 6 artiklan 1 kohdan b alakohta asianmukainen oikeusperuste verkkopalvelun (maksupalvelun) yhteydessä tapahtuvaa käsittelyä varten, on tarkasteltava palvelun erityistä päämäärää, tarkoitusta tai tavoitetta.¹⁵ Käsittelyn tarkoitukset on määritettävä ja ilmoitettava selkeästi rekisteröidyille rekisterinpitäjän käyttötarkoitussidonnaisuutta ja läpinäkyvyyttä koskevien velvoitteiden mukaisesti. Tarpeellisuuden arviointiin sisältyy yhdistetty, tosiasioihin perustuva arviointi käsittelystä ”määritetyn tavoitteen kannalta sekä sen osalta, onko käsittely vähemmän tunkeileva verrattuna muihin saman tavoitteen saavuttamiseksi käytettävissä oleviin vaihtoehtoihin”. Asetuksen 6 artiklan 1 kohdan b alakohtaan ei sisälly käsittely, joka on hyödyllistä mutta ei objektiivisesti tarpeen sopimuksen kohteena olevan palvelun suorittamiseksi tai asiaankuuluvien sopimusta edeltävien toimien toteuttamiseksi rekisteröidyn pyynnöstä, vaikka se olisi tarpeen rekisterinpitäjän muun liiketoiminnan kannalta.¹⁶
18. Tietosuojaneuvoston suuntaviivoissa 2/2019 tehdään selväksi, että sopimuksilla ei voida keinotekoisesti laajentaa henkilötietojen luokkia tai sellaisten käsittelytoimien tyyppejä, jotka rekisterinpitäjän täytyy suorittaa sopimuksen täytäntöön panemiseksi 6 artiklan 1 kohdan b alakohdan mukaisesti.¹⁷ Näissä suuntaviivoissa käsitellään myös tapauksia, joissa rekisteröidyille, jotka ovat kiinnostuneita vain yhdestä palvelusta, saatetaan luoda ”ota tai jätä” -tilanteita. Näin voi tapahtua, jos rekisterinpitäjä haluaa niputtaa yhteen sopimukseen useita erillisiä palveluita tai palvelun osia, joiden perustarkoitukset, ominaisuudet tai perusteet eroavat toisistaan. Mikäli sopimus koostuu useista erillisistä palveluista tai palvelun osista, jotka voidaan kohtuudella

¹⁴ Suuntaviivat 2/2019 yleisen tietosuojasetuksen 6 artiklan 1 kohdan b alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä, Euroopan tietosuojaneuvosto, s. 8.

¹⁵ Ks. edellinen alaviite.

¹⁶ Samoin kuin edellä, s. 7.

¹⁷ Samoin kuin edellä, s. 10.

suorittaa toisistaan riippumatta, asetuksen 6 artiklan 1 kohdan b alakohdan soveltaminen on arvioitava kunkin kyseessä olevan palvelun osalta erikseen siten, että tarkastellaan, mikä on objektiivisesti tarpeen kunkin sellaisen yksittäisen palvelun suorittamiseksi, joita rekisteröity on aktiivisesti pyytänyt tai jotka tämä on tilannut.¹⁸

19. Edellä mainittujen suuntaviivojen mukaisesti rekisterinpitäjien on arvioitava, mikä on objektiivisesti tarpeen sopimuksen täytäntöön panemiseksi. Jos rekisterinpitäjät eivät pysty osoittamaan, että henkilökohtaisten maksutilitietojen käsittely on objektiivisesti tarpeen kunkin palvelun tarjoamiseksi erikseen, yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta ei ole pätevä oikeudellinen peruste tietojen käsittelylle. Tällaisissa tapauksissa rekisterinpitäjän olisi harkittava käsittelylle muuta oikeusperustetta.

2.3 Petostentorjunta

20. Toisen maksupalveludirektiivin 94 artiklan 1 kohdassa säädetään, että jäsenvaltioiden on sallittava, että maksujärjestelmät ja maksupalveluntarjoajat käsittelevät henkilötietoja, kun se on välttämätöntä maksupetoksiin liittyvien rikosten torjunnan, tutkinnan ja selvittämisen turvaamiseksi. Ehdottoman välttämätön henkilötietojen käsittely petosten estämistarkoituksissa voi olla myös maksupalveluntarjoajan oikeutetun edun mukaista edellyttäen, että rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä näitä etuja.¹⁹ Petostentorjuntaan liittyvien käsittelytoimien olisi perustuttava osoitusvelvollisuusperiaatteen mukaiseen rekisterinpitäjän huolellisesti suorittamaan tapauskohtaiseen arviointiin. Petosten torjumiseksi rekisterinpitäjiin voidaan lisäksi soveltaa erityisiä lakisääteisiä velvoitteita, joiden toteuttaminen edellyttää henkilötietojen käsittelyä.

2.4 Jatkokäsittely (tilitietopalvelun tarjoajat ja maksutoimeksiantopalvelun tarjoajat)

21. Yleisen tietosuoja-asetuksen 6 artiklan 4 kohdassa määritetään edellytykset henkilötietojen käsittelylle, jos käsittely tapahtuu muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty. Tarkemmin sanottuna tällainen jatkokäsittely voidaan suorittaa, jos se perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhtaisen toimenpiteen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden takaamiseksi, jos rekisteröity on antanut suostumuksensa tai jos käsittely muuhun tarkoitukseen kuin siihen, jota varten henkilötiedot kerättiin, on yhteensopiva alkuperäisen tarkoituksen kanssa.
22. Toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohta ja 67 artiklan 2 kohdan f alakohta on otettava huolellisesti huomioon. Kuten edellä mainitaan, toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohdassa säädetään, että maksutoimeksiantopalvelun tarjoaja ei saa käyttää, hankkia eikä säilyttää mitään tietoja muussa tarkoituksessa kuin maksajan nimenomaisesti pyytämän maksutoimeksiantopalvelun suorittamiseksi; Toisen maksupalveludirektiivin 67 artiklan 2 kohdan f alakohdassa säädetään, että tilitietopalvelun tarjoaja ei saa käyttää, hankkia eikä säilyttää mitään tietoja muussa tarkoituksessa kuin maksupalvelunkäyttäjän nimenomaisesti pyytämän tilitietopalvelun suorittamiseksi tietosuoja sääntöjen mukaisesti.
23. Näin ollen toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohdassa ja 67 artiklan 2 kohdan f alakohdassa rajoitetaan huomattavasti mahdollisuuksia käsitellä tietoja muita tarkoituksia varten, mikä tarkoittaa sitä, että muuhun tarkoitukseen tapahtuva käsittely ei ole

¹⁸ Samoin kuin edellä, s. 11.

¹⁹ Yleisen tietosuoja-asetuksen johdanto-osan 47 kappale.

sallittua, paitsi jos rekisteröity on antanut suostumuksensa yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohdan mukaisesti tai jos käsittelyä säädetään rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä yleisen tietosuoja-asetuksen 6 artiklan 4 kohdan mukaisesti. Jos käsittely tapahtuu muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty, eikä käsittely perustu rekisteröidyn suostumukseen eikä unionin oikeuteen tai jäsenvaltion lainsäädäntöön, toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohdassa ja 67 artiklan 2 kohdan f alakohdassa säädetyissä rajoituksissa tehdään selväksi, että mikään muu tarkoitus ei ole yhteensopiva sen tarkoituksen kanssa, jota varten henkilötiedot alun perin kerättiin. Yleisen tietosuoja-asetuksen 6 artiklan 4 kohdassa tarkoitettu tasapainotesti ei voi johtaa käsittelyn oikeusperustaan.

24. Yleisen tietosuoja-asetuksen 6 artiklan 4 kohdassa sallitaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuva myöhempi käsittely. Esimerkiksi kaikki maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat ovat 20 päivänä toukokuuta 2015 rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/849 3 artiklan 2 kohdan a alakohdassa tarkoitettuja ilmoitusvelvollisia. Näiden ilmoitusvelvollisten on sen vuoksi sovellettava direktiivissä määritettyjä asiakkaan tuntemisvelvollisuutta koskevia toimenpiteitä. Toisen maksupalveludirektiivin mukaisen palvelun yhteydessä käsiteltäviä henkilötietoja käsitellään sen vuoksi myöhemmin vähintään yhden palveluntarjoajalle kuuluvan lakisääteisen veloitteen perusteella.²⁰
25. Kuten 20 kohdassa mainitaan, yleisen tietosuoja-asetuksen 6 artiklan 4 kohdassa säädetään, että jos käsittely tapahtuu muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty, käsittely voisi perustua rekisteröidyn suostumukseen, jos kaikki yleisen tietosuoja-asetuksen mukaiset suostumuksen edellytykset täyttyvät. Kuten edellä todetaan, rekisterinpitäjän on osoitettava, että suostumuksen antamisesta voidaan kieltäytyä tai että suostumus voidaan peruuttaa ilman, että siitä aiheutuu rekisteröidylle haittaa (yleisen tietosuoja-asetuksen johdanto-osan 42 kappale).

2.5 Tiliin pääsyn oikeudellinen peruste (tiliä ylläpitävät maksupalveluntarjoajat)

26. Kuten 10 kohdassa todetaan, maksupalvelunkäyttäjät voivat käyttää oikeuttaan käyttää maksutoimeksianto- ja tilitietopalveluja. Toisen maksupalveludirektiivin 66 artiklan 1 kohdassa ja 67 artiklan 1 kohdassa jäsenvaltioille asetetut veloitteet olisi saatettava osaksi kansallista lainsäädäntöä, jotta voidaan käytännössä taata maksupalvelunkäyttäjän oikeus hyötyä edellä mainituista maksupalveluista. Tällaisten oikeuksien tehokas soveltaminen ei olisi mahdollista ilman, että tiliä ylläpitävällä maksupalveluntarjoajalla, tavallisesti pankilla, on vastaava velvollisuus myöntää maksupalveluntarjoajalle pääsy tilille sillä edellytyksellä, että se on täyttänyt kaikki maksupalvelunkäyttäjän tilille pääsyä koskevat vaatimukset. Lisäksi toisen maksupalveludirektiivin 66 artiklan 5 kohdassa ja 67 artiklan 4 kohdassa todetaan selkeästi, että maksutoimeksianto- ja tilitietopalvelujen tarjoaminen ei saa riippua siitä, onko maksutoimeksianto- tai tilitietopalvelun tarjoajien ja tiliä ylläpitävien maksupalveluntarjoajien välillä olemassa tätä varten sopimussuhde.
27. Tiliä ylläpitävän maksupalveluntarjoajan suorittama henkilötietojen käsittely, jossa maksutoimeksiantopalvelun tarjoajan ja tilitietopalvelun tarjoajan pyytämiin henkilötietoihin myönnetään pääsy, jotta ne voivat suorittaa maksupalvelunsa maksupalvelunkäyttäjälle, perustuu lakisääteiseen veloitteeseen. Toisen maksupalveludirektiivin tavoitteiden saavuttamiseksi tiliä ylläpitävien maksupalveluntarjoajien on annettava pääsy maksutoimeksiantopalvelun tarjoajien ja tilitietopalvelun tarjoajien palvelujen tarvitsemiin henkilötietoihin, mikä on välttämätön edellytys

²⁰ On huomattava, että tämän asiakirjan soveltamisalan ulkopuolelle jää perusteellinen tarkastelu siitä, täyttääkö rahanpesunvastainen direktiivi yleisen tietosuoja-asetuksen 6 artiklan 4 kohdan vaatimukset.

sille, että maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat voivat tarjota palvelujaan ja että näin voidaan varmistaa toisen maksupalveludirektiivin 66 artiklan 1 kohdassa ja 67 artiklan 1 kohdassa säädettyjen oikeuksien toteutuminen. Sen vuoksi tässä tapauksessa sovellettava oikeudellinen peruste on yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta.

28. Koska yleisessä tietosuoja-asetuksessa täsmennetään, että lakisääteiseen veloitteeseen perustuvasta käsittelystä olisi säädettävä selkeästi unionin oikeudessa tai jäsenvaltion lainsäädännössä (ks. yleisen tietosuoja-asetuksen 6 artiklan 3 kohta), tiliä ylläpitävien maksupalveluntarjoajien veloitteesta antaa pääsy tietoihin olisi säädettävä toisen maksupalveludirektiivin täytäntöön panevassa kansallisessa lainsäädännössä.

3 NIMENOMAINEN SUOSTUMUS

3.1 Yleisen tietosuojasetuksen mukainen suostumus

29. Yleisen tietosuojasetuksen nojalla suostumus on yksi kuudesta henkilötietojen käsittelyn lainmukaisesta oikeusperusteesta. Yleisen tietosuojasetuksen 4 artiklan 11 kohdan mukaisesti suostumuksella tarkoitetaan ”mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen”. Nämä neljä vapaaehtoisuutta, yksilöimistä, tietoisuutta ja yksiselitteisyyttä koskevaa ehtoa ovat suostumuksen pätevyyden kannalta olennaisen tärkeitä. Euroopan tietosuojaneuvoston asetuksen 2016/679 mukaista suostumusta koskevien suuntaviivojen 05/2020 mukaisesti suostumus voi olla asianmukainen laillinen peruste vain, jos rekisteröidylle tarjotaan mahdollisuus valvoa tietojensa käyttöä sekä aito tilaisuus valita vapaasti hyväksyykö hän tarjotut ehdot vai hylkääkö hän ne, eikä hylkäämisestä aiheudu hänelle haittaa. Pyytäessään suostumusta rekisterinpitäjän on arvioitava, täyttääkö pyyntö kaikki pätevän suostumuksen hankkimista koskevat edellytykset. Jos suostumus hankitaan täysin yleisen tietosuojasetuksen mukaisesti, kyseessä on väline, jonka avulla rekisteröidyt voivat valvoa, käsitelläänkö heidän henkilötietojaan vai ei. Muussa tapauksessa rekisteröity voi valvoa tietojensa käsittelyä vain näennäisesti ja suostumus on epäpätevä käsittelyperuste, minkä vuoksi käsittelytoimet ovat laittomia.²¹
30. Yleisen tietosuojasetuksen 7 artiklaan sisältyy myös muita suoja-toimia, joiden mukaisesti rekisterinpitäjän on voitava osoittaa, että suostumus oli käsittelyhetkellä pätevä. Suostumuksen antamista koskeva pyyntö myös on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Lisäksi rekisteröidylle on ilmoitettava oikeudesta peruuttaa suostumus milloin tahansa yhtä yksinkertaisella tavalla kuin suostumuksen antamisen yhteydessä.
31. Yleisen tietosuojasetuksen 9 artiklan mukaisesti suostumus on yksi poikkeuksista erityisten henkilötietojen ryhmien käsittelyä koskevaan yleiseen kieltoon. Tällaisessa tapauksessa rekisteröidyn suostumuksen on kuitenkin oltava ”nimenomainen suostumus”.²²
32. Asetuksen 2016/679 mukaista suostumusta koskevien tietosuojaneuvoston suuntaviivojen 05/2020 mukaan yleisen tietosuojasetuksen mukaisella nimenomaisella suostumuksella viitataan tapaan, jolla rekisteröity ilmaisee suostumuksen. Se tarkoittaa, että rekisteröidyn on annettava yksiselitteinen tiettyjä käsittelytarkoituksia koskeva suostumusta ilmaiseva lausuma. Selvä tapa varmistaa nimenomainen suostumus olisi suostumuksen nimenomainen vahvistaminen kirjallisessa lausumassa. Rekisterinpitäjä voisi tarvittaessa varmistaa, että rekisteröity on allekirjoittanut kirjallisen lausuman, jotta myöhemmin ei ole mitään epäilystä eikä näytön puutetta.
33. Suostumusta ei voida missään tapauksessa johtaa mahdollisesti moniselitteisistä lausunnoista tai toimista. Rekisterinpitäjän on myös otettava huomioon, ettei suostumusta voida hankkia samalla teolla, jolla sopimus tai palvelun yleiset ehdot hyväksytään.

3.2 Toisen maksupalveludirektiivin mukainen suostumus

²¹ Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat 05/2020, Euroopan tietosuojaneuvosto, 3 kohta.

²² Ks. myös lausunto 15/2011 suostumuksen määritelmästä (WP 187), s. 6–8, ja/tai lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä (WP 217), s. 9, 10, 13 ja 14.

34. Tietosuojaneuvosto toteaa, että nimenomaista suostumusta koskeva oikeudellinen kehys on monimutkainen, sillä nimenomaisen suostumuksen käsite sisältyy sekä toiseen maksupalveludirektiiviin että yleiseen tietosuojasetukseen. Tämä johtaa kysymykseen siitä, olisiko toisen maksupalveludirektiivin 94 artiklan 2 kohdassa tarkoitettua nimenomaista hyväksyntää tulkittava samalla tavalla kuin yleisen tietosuojasetuksen mukaista nimenomaista suostumusta.

3.2.1 Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukainen nimenomainen hyväksyntä

35. Toinen maksupalveludirektiivi sisältää useita henkilötietojen käsittelyä koskevia erityisiä sääntöjä: Sen 94 artiklan 1 kohdassa säädetään, että asianomaisessa direktiivissä tarkoitettussa henkilötietojen käsittelyssä on noudatettava EU:n tietosuojalainsäädäntöä. Lisäksi sen 94 artiklan 2 kohdassa säädetään, että maksupalveluntarjoajat voivat vain maksupalvelunkäyttäjän nimenomaisella hyväksynnällä saada, käsitellä ja säilyttää sellaisia henkilötietoja, jotka ovat tarpeen niiden maksupalvelujen tarjoamiseksi. Toisen maksupalveludirektiivin 33 artiklan 2 kohdan mukaisesti tätä vaatimusta maksupalvelunkäyttäjän nimenomaisesta hyväksymisestä ei sovelleta tilitietopalvelun tarjoajiin. Toisen maksupalveludirektiivin 67 artiklan 2 kohdan a alakohdassa säädetään kuitenkin edelleen, että tilitietopalvelun tarjoajat saavat tarjota vain palveluja, jotka perustuvat maksupalvelunkäyttäjän nimenomaiseen hyväksymiseen.

36. Kuten edellä mainitaan, yleisen tietosuojasetuksen mukaisen käsittelyn laillisia perusteita koskeva luettelo on tyhjentävä. Kuten 14 kohdassa mainitaan, henkilötietojen käsittelyn oikeusperusta maksupalvelujen tarjoamiseksi on lähtökohtaisesti tietosuojasetuksen 6 artiklan 1 kohdan b alakohta, mikä tarkoittaa sitä, että käsittely on tarpeen joko sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Tästä seuraa, että toisen maksupalveludirektiivin 94 artiklan 2 kohtaa ei voida pitää henkilötietojen käsittelyn lisäoikeusperustana. Tietosuojaneuvosto katsoo, että edellä esitetyn perusteella tätä kohtaa olisi tulkittava yhtäältä sovellettavan tietosuojaa koskevan oikeudellisen kehysten mukaisesti ja toisaalta siten, että sen hyödyllinen vaikutus säilyy. Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukaista nimenomaista hyväksyntää olisi sen vuoksi pidettävä sopimusperusteisena lisävaatimuksena²³, joka koskee pääsyä henkilötietoihin ja niiden myöhempää käsittelyä ja tallentamista maksupalvelujen tarjoamista varten, eikä se sen vuoksi ole sama kuin yleisen tietosuojasetuksen mukainen (nimenomainen) suostumus.

37. Toisen maksupalveludirektiivin 94 artiklan 2 kohdassa tarkoitettu nimenomainen hyväksyntä on sopimukseen perustuva suostumus. Tämä tarkoittaa sitä, että toisen maksupalveludirektiivin 94 artiklan 2 kohtaa olisi tulkittava siten, että kun rekisteröidyt tekevät sopimuksen maksupalveluntarjoajan kanssa toisen maksupalveludirektiivin mukaisesti, rekisteröityjen on oltava täysin tietoisia käsiteltävien henkilötietojen tietyistä tietoryhmistä. Lisäksi rekisteröidyille on ilmoitettava erityisesti (maksupalvelun) tarkoituksesta, jota varten heidän henkilötietojaan käsitellään, ja heidän on nimenomaisesti hyväksyttävä nämä lausekkeet. Tällaisten lausekkeiden olisi oltava selvästi erotettavissa muista sopimuksessa käsitellyistä asioista, ja rekisteröidyn olisi nimenomaisesti hyväksyttävä ne.

38. Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukaisen nimenomaisen hyväksynnän käsitteen keskiössä on pääsy henkilötietoihin näiden tietojen myöhemmäksi käsittelemiseksi ja

²³ 5. heinäkuuta 2018 päivätty toista maksupalveludirektiiviä koskeva Euroopan tietosuojaneuvoston kirje, s. 4.

säilyttämiseksi maksupalvelujen tarjoamista varten. Tämä tarkoittaa sitä, että maksupalveluntarjoaja²⁴ ei vielä käsittele henkilötietoja, vaan sen on saatava pääsy henkilötietoihin, joiden käsittelemisestä on vastannut jokin muu rekisterinpitäjä. Jos maksupalvelunkäyttäjä tekee sopimuksen esimerkiksi maksutoimeksiantopalvelun tarjoajan kanssa, tämän tarjoajan on saatava pääsy maksupalvelunkäyttäjän henkilötietoihin, joiden käsittelemisestä vastaa tiliä ylläpitävä maksupalveluntarjoaja. Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukaisen nimenomaisen hyväksynnän tarkoituksena on saada pääsy kyseisiin henkilötietoihin ja käsitellä ja säilyttää näitä henkilötietoja, jotka ovat tarpeen maksupalvelun tarjoamiseksi. Jos rekisteröity antaa nimenomaisen suostumuksensa, tiliä ylläpitävän maksupalveluntarjoajan on annettava pääsy ilmoitettuihin henkilötietoihin.

39. Vaikka toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukainen hyväksyntä ei ole oikeudellinen peruste henkilötietojen käsittelylle, se liittyy erityisesti henkilötietoihin ja tietosuojaan ja sillä varmistetaan maksupalvelunkäyttäjälle läpinäkyvyys ja valvonta.²⁵ Vaikka toisessa maksupalveludirektiivissä ei täsmennetä sen 94 artiklan 2 kohdan mukaisen hyväksynnän aineellisia edellytyksiä, se olisi, kuten edellä todetaan, ymmärrettävä sovellettavan tietosuoja koskevan oikeudellisen kehityksen mukaisesti ja siten, että sen hyödyllinen vaikutus säilyy.
40. Rekisterinpitäjien antamien tietojen ja läpinäkyvyysvaatimuksen osalta tietosuojatyöryhmän läpinäkyvyyttä koskeissa suuntaviivoissa täsmennetään, että "[l]äpinäkyvyyden periaatteessa on näiden säännösten perusteella tärkeää se, että rekisteröity saa etukäteen tiedon käsittelyn laajuudesta ja seurauksista ja että henkilötietojen käyttötavat eivät tule rekisteröidylle myöhemmin yllätyksenä".²⁶
41. Lisäksi käyttötarkoitussidonnaisuutta koskevan periaatteen mukaisesti henkilötietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohta). Jos henkilötietoja kerätään useampaa kuin yhtä tarkoitusta varten, rekisterinpitäjien olisi vältettävä yksilöimästä vain yhtä laajaa tarkoitusta, joilla perusteltaisiin erilaisia jatkokäsittelytoimia, jotka itse asiassa liittyisivät vain etäältä varsinaiseen alkuperäiseen tarkoitukseen.²⁷ Tietosuojaneuvosto on viimeksi verkkopalveluja koskevien sopimusten yhteydessä korostanut riskiä siitä, että sopimukseen pyritään sisällyttämään yleisiä käsittelyä koskevia ehtoja ja todennut, että keräämisen tarkoitus on määritettävä selkeästi ja nimenomaisesti: tarkoituksen olisi oltava kyllin yksityiskohtainen sen määrittämiseksi, millainen käsittely sisältyy tai ei sisälly määritettyyn käyttötarkoitukseen, ja sen perusteella on voitava arvioida lainmukaisuus ja soveltaa tietosuojatoimia.²⁸
42. Kun tätä tarkastellaan toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukaisen nimenomaista hyväksyntää koskevan lisävaatimuksen yhteydessä, rekisterinpitäjien on annettava rekisteröidyille erityisiä ja nimenomaisia tietoja rekisterinpitäjän yksilöimistä erityisistä tarkoituksista, joita varten rekisteröityjen henkilötietoja käsitellään ja säilytetään. Toisen

²⁴ Tämä koskee toisen maksupalveludirektiivin liitteessä I tarkoitettuja maksupalveluja 1–7.

²⁵ Toisen maksupalveludirektiivin 94 artiklan 2 kohta sisältyy 4 lukuun, jonka otsikkona on "Tietosuoja".

²⁶ Euroopan tietosuojaneuvoston hyväksymät tietosuojatyöryhmän asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat (hyväksytty 11. huhtikuuta 2018), 10 kohta.

²⁷ Tietosuojatyöryhmän käyttötarkoituksen rajoittamista koskeva lausunto 03/2013 (WP 203), s. 16.

²⁸ Suuntaviivat 2/2019 yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä, 16 kohta (julkinen kuuleminen) ja tietosuojatyöryhmän käyttötarkoituksen rajoittamista koskeva lausunto 03/2013 (WP 203), s. 15–16.

maksupalveludirektiivin 94 artiklan 2 kohdan mukaisesti rekisteröityjen on nimenomaisesti hyväksyttävä nämä erityiset tarkoitukset.

43. Kuten edellä 10 kohdassa todetaan, tietosuojaneuvosto korostaa lisäksi, että maksupalvelunkäyttäjän on voitava valita, käyttääkö se palvelua, eikä maksupalvelunkäyttäjää voida pakottaa käyttämään sitä. Siksi toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukaisen suostumuksen on oltava myös vapaaehtoinen suostumus.

3.3 Päätelmät

44. Toisen maksupalveludirektiivin mukainen nimenomainen hyväksyntä eroaa yleisen tietosuojasetuksen mukaisesta (nimenomaisesta) suostumuksesta. Toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukainen nimenomainen hyväksyntä on sopimukseen perustuva lisävaatimus. Kun maksupalveluntarjoaja tarvitsee pääsyn henkilötietoihin voidakseen tarjota maksupalvelua, siihen tarvitaan maksupalvelunkäyttäjän toisen maksupalveludirektiivin 94 artiklan 2 kohdan mukainen nimenomainen hyväksyntä.

4 HILJAISEN OSAPUOLEN TIETOJEN KÄSITTELY

4.1 Hiljaisen osapuolen tiedot

45. Tietosuojakysymys, jota on tarkasteltava huolellisesti, on niin kutsuttujen ”hiljaisen osapuolen tietojen” eli silent party -datan käsittely. Tässä asiakirjassa hiljaisen osapuolen tiedoilla tarkoitetaan sellaisen rekisteröidyn henkilötietoja, joka ei ole tietyn maksupalveluntarjoajan käyttäjä, mutta jonka henkilötietoja kyseinen maksupalveluntarjoaja käsittelee palveluntarjoajan ja maksupalvelunkäyttäjän välisen sopimuksen täyttämiseksi. Tämä koskee esimerkiksi tapausta, jossa maksupalvelunkäyttäjä eli rekisteröity A käyttää tilitietopalvelun tarjoajan palveluja ja rekisteröity B on suorittanut useita maksutapahtumia rekisteröidyn A maksutilille. Tässä tapauksessa rekisteröityä B pidetään hiljaisena osapuolena, ja rekisteröidyn B henkilötietoja (kuten rekisteröidyn B tilinumero ja näihin maksutapahtumiin liittyvä rahamäärä) pidetään hiljaisen osapuolen tietoina.

4.2 Rekisterinpitäjän oikeutettu etu

46. Yleisen tietosuojasetuksen 5 artiklan 1 kohdan b alakohdassa edellytetään, että henkilötietoja kerätään ainoastaan tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Lisäksi yleisessä tietosuojasetuksessa edellytetään, että kaiken henkilötietojen käsittelyn on oltava sekä tarpeellista että oikeasuhteista ja tietosuojaperiaatteiden, kuten käyttötarkoitussidonnaisuuden ja tietojen minimoinnin, mukaista.

47. Yleisellä tietosuojasetuksella voidaan sallia hiljaisen osapuolen tietojen käsittely, jos käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi (yleisen tietosuojasetuksen 6 artiklan 1 kohdan f alakohta). Tällainen käsittely ei kuitenkaan ole mahdollista, jos ”henkilötietojen suoja edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät” rekisterinpitäjän oikeutetun edun.

48. Laillisena perusteena sille, että maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat käsittelevät hiljaisen osapuolen tietoja toisen maksupalveludirektiivin mukaisen maksupalvelujen tarjoamisen yhteydessä, voisi näin ollen olla rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu panna täytäntöön maksupalvelunkäyttäjän kanssa tehty sopimus. Hiljaisen osapuolen henkilötietojen käsittelyn tarve on rajallinen ja määräytyy näiden rekisteröityjen kohtuullisten odotusten perusteella. Toisen maksupalveludirektiivin mukaisten maksupalvelujen tarjoamisen osalta on otettava käyttöön tehokkaita ja asianmukaisia toimenpiteitä sen varmistamiseksi, että hiljaisten osapuolten etuja tai perusoikeuksia ja -vapauksia ei syrjäytetä, ja sen varmistamiseksi, että näiden rekisteröityjen henkilötietojen käsittelyä koskevia kohtuullisia odotuksia kunnioitetaan. Tältä osin rekisterinpitäjän (tilitietopalvelun tarjoaja tai maksutoimeksiantopalvelun tarjoaja) on otettava käyttöön rekisteröityjen oikeuksien suojaamiseksi tarvittavat käsittelyn suojaustoimet. Tähän sisältyy teknisiä toimenpiteitä sen varmistamiseksi, että hiljaisen osapuolen tietoja ei käsitellä muuhun tarkoitukseen kuin siihen tarkoitukseen, jota varten maksutoimeksiantopalvelun tarjoajat ja tilitietopalvelun tarjoajat alun perin keräsivät henkilötiedot. Asianmukaisen tietoturvan ja tietojen minimoinnin tason saavuttamiseksi olisi mahdollisuuksien mukaan sovellettava myös salausta tai muita tekniikoita.

4.3 Hiljaisen osapuolen henkilötietojen jatkokäsittely

49. Kuten 29 kohdassa todetaan, toisella maksupalveludirektiivillä säännellyn maksupalvelun yhteydessä käsiteltäviä henkilötietoja voitaisiin käsitellä myöhemmin palveluntarjoajalle kuuluvien

lakisääteisten velvoitteiden perusteella. Nämä lakisääteiset velvoitteet voivat koskea hiljaisen osapuolen henkilötietoja.

50. Oikeutettuun etuun perustuvan hiljaisen osapuolen tietojen jatkokäsittelyn osalta tietosuojaneuvosto katsoo, että näitä tietoja ei voida käyttää muuhun tarkoitukseen kuin siihen, johon henkilötiedot on kerätty, muutoin kuin unionin oikeuden tai jäsenvaltion lainsäädännön perusteella. Hiljaisen osapuolen suostumus ei ole oikeudellisesti toteutettavissa, sillä suostumuksen saamiseksi olisi kerättävä tai käsiteltävä hiljaisen osapuolen henkilötietoja, ja tälle ei ole olemassa yleisen tietosuoja-asetuksen 6 artiklan mukaista oikeudellista perustetta. Myöskään yleisen tietosuoja-asetuksen 6 artiklan 4 kohdassa tarkoitettulla tasapainotestillä ei voida tarjota perustetta käsittelylle muihin tarkoituksiin (esimerkiksi suoramarkkinointiin). Näiden rekisteröityjen, jotka ovat hiljaisia osapuolia, oikeuksia ja vapauksia ei kunnioiteta, jos uusi rekisterinpitäjä käyttää henkilötietoja muihin tarkoituksiin, kun otetaan huomioon asiayhteys, jossa henkilötiedot on kerätty, ja erityisesti se, että rekisterinpitäjillä ei ole mitään suhdetta rekisteröityihin, jotka ovat hiljaisia osapuolia²⁹; se, ettei minkään muun tarkoituksen ja sen tarkoituksen välillä, jota varten henkilötiedot alun perin kerättiin, ole mitään yhteyttä (eli se, että maksupalveluntarjoajat tarvitsevat hiljaisen osapuolen tietoja vain pannakseen täytäntöön sopimuksen toisen sopimuspuolen kanssa); ja kyseessä olevien henkilötietojen luonne³⁰, eli se, että rekisteröidyt eivät voi kohtuudella odottaa jatkokäsittelyä tai edes tietää, mikä rekisterinpitäjä saattaa käsitellä heidän henkilötietojaan, kun otetaan huomioon toisen maksupalveludirektiivin 66 artiklan 3 kohdan g alakohdassa ja 67 artiklan 2 kohdan f alakohdassa säädetyt käsittelyä koskevat oikeudelliset rajoitukset.

²⁹ Toisen maksupalveludirektiivin johdanto-osan 87 kappaleessa todetaan, että toisessa maksupalveludirektiivissä käsitellään ainoastaan ”maksupalvelunkäyttäjän ja -tarjoajan välisiä sopimusveloituksia ja -vastuita”. Hiljaisen osapuolen tiedot eivät näin ollen kuulu toisen maksupalveludirektiivin soveltamisalaan.

³⁰ Taloutta koskevien henkilötietojen käsittelyyn olisi kiinnitettävä erityistä huomiota, sillä tietosuoja koskevasta vaikutustenarvioinnista laadittujen ohjeiden mukaan käsittelyn voidaan katsoa lisäävän mahdollista luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvää riskiä.

5 TOISEN MAKSUPALVELUDIREKTIIVIN MUKAINEN ERITYISIÄ HENKILÖTIETORYHMIÄ KOSKEVA KÄSITTELY

5.1 Erityiset henkilötietoryhmät

51. Yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa kielletään "[s]ellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely".
52. On syytä korostaa, että joissakin jäsenvaltioissa sähköisiä maksuja käytetään jo kaikkialla ja että monet ihmiset käyttävät päivittäisissä maksutapahtumissaan sähköistä maksamista käteisen sijasta. Samalla maksutapahtumat voivat paljastaa tiettyä rekisteröityä koskevia arkaluonteisia tietoja, mukaan lukien tiedot, jotka liittyvät erityisiin henkilötietoryhmiin. Maksutapahtuman yksityiskohdista riippuen esimerkiksi poliittiset mielipiteet ja uskonnollinen vakaumus voivat paljastua poliittisille puolueille tai järjestöille, kirkkoille tai seurakunnille osoitetuista lahjoituksista. Ammattiliiton jäsenyys voi paljastua siitä, että vuosittainen jäsenmaksu vähennetään henkilön pankkitililtä. Terveyttä koskevia henkilötietoja voidaan kerätä analysoimalla rekisteröidyn terveydenhoidon ammattilaiselle (esimerkiksi psykiatrilille) maksamia terveydenhoitolaskuja. Tiettyjä hankintoja koskevat tiedot voivat myös paljastaa tietoja henkilön seksuaalisesta käyttäytymisestä tai suuntautumisesta. Kuten näistä esimerkeistä käy ilmi, jopa yksittäiset tapahtumat voivat sisältää erityisiä henkilötietoryhmiä. Lisäksi tilitietopalvelut saattavat tukeutua yleisen tietosuoja-asetuksen 4 artiklan 4 kohdassa määriteltyyn profilointiin. Kuten tietosuojatyöryhmän suuntaviivoissa automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, sellaisina kuin Euroopan tietosuojaneuvosto on ne hyväksynyt, todetaan, "[p]rofiloinnilla voidaan luoda erityisiä henkilötietoryhmiä sellaisista tiedoista tehtävillä päätelmillä, jotka sinänsä eivät kuulu erityisiin henkilötietoryhmiin, mutta joista tulee tällaisia tietoja, kun niitä yhdistetään muihin tietoihin."³¹ Tämä tarkoittaa sitä, että maksutapahtumien määrän avulla voidaan paljastaa erilaisia käyttäytymismalleja, joihin voi sisältyä erityisiä henkilötietoryhmiä. Näin ollen on huomattava mahdollisuus, että palveluntarjoaja, joka käsittelee rekisteröityjen maksutapahtumia koskevia tietoja, käsittelee myös erityisiä henkilötietoryhmiä.
53. Käsitteen 'arkaluonteiset maksutiedot' osalta tietosuojaneuvosto toteaa seuraavaa. Toisessa maksupalveludirektiivissä oleva arkaluonteisten maksutietojen määritelmä eroaa huomattavasti siitä, miten käsitettä 'arkaluonteiset henkilötiedot' yleisesti käytetään yleisen tietosuoja-asetuksen ja tietosuojan (tietosuojalainsäädännön) yhteydessä. Kun toisessa maksupalveludirektiivissä arkaluonteisilla maksutiedoilla tarkoitetaan "tietoja, joita voidaan käyttää petoksiin ja joihin kuuluvat henkilökohtaiset turvatunnukset", yleisessä tietosuoja-asetuksessa korostetaan sellaisten erityisten henkilötietoryhmien erityisen suojan tarvetta, jotka ovat yleisen tietosuoja-asetuksen 9 artiklan mukaisesti erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, kuten erityiset henkilötietoryhmät.³² Tältä osin on suositeltavaa ainakin kartoittaa ja luokitella tarkasti, millaisia henkilötietoja käsitellään. Todennäköisesti tarvitaan yleisen tietosuoja-asetuksen

³¹ 29 artiklan mukainen tietosuojatyöryhmä, suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista

asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01, s. 15.

³² Esimerkiksi yleisen tietosuoja-asetuksen johdanto-osan 10 kappaleessa erityisistä henkilötietoryhmistä käytetään nimitystä 'arkaluonteiset tiedot'.

35 artiklan mukainen tietosuoja koskeva vaikutustenarviointi, joka auttaa tässä kartoituksessa. Lisäohjeita tietosuoja koskevista vaikutustenarvioinneista on tietosuojatyöryhmän ohjeissa tietosuoja koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski” (tietosuojaneuvoston hyväksymä asiakirja).

5.2 Mahdolliset poikkeukset

54. Yleisen tietosuoja-asetuksen 9 artiklassa säädetty kielto ei ole ehdoton. On erityisesti huomattava, että vaikka yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan b–f ja h–j alakohdan poikkeuksia ei selvästikään sovelleta henkilötietojen käsittelyyn toisen maksupalveludirektiivin yhteydessä, voitaisiin harkita seuraavia kahta yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan poikkeusta:
- a) Kieltoa ei sovelleta, jos rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten (yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohta).
 - b) Kieltoa ei sovelleta, jos käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi (yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohta).
55. On syytä huomauttaa, että yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan luettelo poikkeuksista on tyhjentävä. Palveluntarjoajan on tunnustettava sen mahdollisuus, että erityisiä henkilötietoryhmiä sisällytetään minkä tahansa toisen maksupalveludirektiivin soveltamisalaan kuuluvan palvelun tarjoamiseksi käsiteltäviin henkilötietoihin. Koska yleisen tietosuoja-asetuksen 9 artiklan 1 kohdan kieltoa sovelletaan näihin palveluntarjoajiin, niiden on varmistettava, että niihin sovelletaan jotakin yleisen tietosuoja-asetuksen 9 artiklan 2 kohdassa säädettyistä poikkeuksista. On syytä korostaa, että jos palveluntarjoaja ei pysty osoittamaan, että jokin poikkeuksista täyttyy, sovelletaan 9 artiklan 1 kohdan mukaista kieltoa.

5.3 Tärkeä yleinen etu

56. Maksupalvelut voivat käsitellä erityisiä henkilötietoryhmiä tärkeää yleistä etua koskevasta syystä, mutta ainoastaan silloin, jos kaikki yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdan edellytykset täyttyvät. Tämä tarkoittaa sitä, että erityisten henkilötietoryhmien käsittely on otettava huomioon erityisessä unionin oikeuden tai jäsenvaltion lainsäädännön säännöksessä, jonka mukaisesti yleisen tietosuoja-asetuksen 9 artiklan 1 kohdasta poiketaan. Tässä säännöksessä on varmistettava oikeasuhteisuus käsittelyn tavoitteeseen nähden, ja siihen on sisällyttävä asianmukaisia ja erityisiä toimenpiteitä rekisteröidyn perusoikeuksien ja etujen turvaamiseksi. Lisäksi tässä unionin oikeuden tai jäsenvaltion lainsäädännön säännöksessä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan. Lisäksi on osoitettava, että erityisten henkilötietoryhmien käsittely on tarpeen tärkeän yleisen edun vuoksi, mukaan lukien järjestelmän kannalta merkittävät edut. Tätä poikkeusta voitaisiin soveltaa nimettyihin maksupalveluihin vain, jos kaikki nämä edellytykset täyttyvät kaikilta osin.

5.4 Nimenomainen suostumus

57. Tapauksissa, joissa ei sovelleta yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdan mukaista poikkeusta, nimenomaisen suostumuksen hankkiminen yleisessä tietosuoja-asetuksessa säädettyjen pätevän suostumuksen edellytysten mukaisesti näyttää edelleen olevan ainoa mahdollinen lainmukainen poikkeus, joka koskee kolmansien palveluntarjoajien suorittamaa

erityisten henkilötietoryhmien käsittelyä. Euroopan tietosuojaneuvoston asetuksen 2016/679 mukaista suostumusta koskevissa suuntaviivoissa 05/2020³³ todetaan, että ”tarvetta sopimuksen täytäntöön panemiseksi” ei yleisen tietosuoja-asetuksen 9 artiklan 2 kohdassa tunnusteta poikkeukseksi yleisestä kiellosta käsitellä erityisiä henkilötietoryhmiä. Rekisterinpitäjien ja jäsenvaltioiden olisi tämän ongelman ratkaisemiseksi tarkasteltava 9 artiklan 2 kohdan b–j alakohdassa säädettyjä erityisiä poikkeuksia. Kun palveluntarjoajat tukeutuvat yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohtaan, niiden on varmistettava, että niille on myönnetty nimenomainen suostumus ennen käsittelyn aloittamista. Yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohdassa tarkoitetun nimenomaisen suostumuksen on täytettävä kaikki yleisessä tietosuoja-asetuksessa säädetyt vaatimukset.

5.5 Ei soveltuvaa poikkeusta

58. Kuten edellä todetaan, jos palveluntarjoaja ei pysty osoittamaan, että jokin poikkeuksista täyttyy, sovelletaan 9 artiklan 1 kohdan mukaista kieltoa. Tällöin voitaisiin ottaa käyttöön teknisiä toimenpiteitä, joilla estetään erityisten henkilötietoryhmien käsittelyä esimerkiksi estämällä tiettyjen tietopisteiden käsittely. Tältä osin maksupalveluntarjoajat voivat pohtia teknisiä mahdollisuuksia sulkea pois erityisiä henkilötietoryhmiä ja sallia valikoitu pääsy, jolla estettäisiin kolmansien palveluntarjoajien suorittamaa hiljaisiin osapuoliin liittyvien erityisten henkilötietoryhmien käsittelyä.

³³ Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat 05/2020, Euroopan tietosuojaneuvosto, 99 kohta.

6 TIETOJEN MINIMOINTI, TURVALLISUUS, LÄPINÄKYVYYS, TILIVELVOLLISUUS JA PROFILOINTI

6.1 Tietojen minimointi ja sisäänrakennettu ja oletusarvoinen tietosuojaja

59. Tietojen minimoinnin periaate on vahvistettu yleisen tietosuojaja-asetuksen 5 artiklan 1 kohdan c alakohdassa: ”Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia [...] henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään”. Tietojen minimoinnin periaatteen mukaisesti rekisterinpitäjät eivät saisi käsitellä enempää henkilötietoja kuin on tarpeen kyseisen erityisen tarkoituksen saavuttamiseksi. Kuten 2 luvussa todetaan, maksupalvelun tarjoamiseksi tarvittavien henkilötietojen määrä ja tyyppi määräytyvät objektiivisen ja keskinäisesti ymmärrettävän sopimustarkoituksen perusteella.³⁴ Tietojen minimointia sovelletaan kaikkeen käsittelyyn (esimerkiksi henkilötietojen keräämiseen, niihin pääsyyn ja niiden pyytämiseen). Euroopan tietosuojaneuvoston suuntaviivoissa 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta todetaan, että myös henkilötietojen käsittelijät ja teknologian palveluntarjoajat tunnustetaan sisäänrakennetun ja oletusarvoisen tietosuojan keskeisiksi mahdollistajiksi, ja että niiden olisi myös oltava tietoisia siitä, että rekisterinpitäjien on käsiteltävä henkilötietoja ainoastaan sellaisten järjestelmien ja teknologioiden avulla, joissa on sisäänrakennettu tietosuojaja.³⁵
60. Sisäänrakennetun ja oletusarvoisen tietosuojan soveltamista koskevat veloitteet sisältyvät yleisen tietosuojaja-asetuksen 25 artiklaan. Nämä veloitteet ovat erityisen tärkeitä tietojen minimoinnin periaatteen kannalta. Tässä artiklassa säädetään, että rekisterinpitäjien on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi yleisen tietosuojaja-asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin. Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näitä toimenpiteitä voivat olla tietojen salaus, tietojen pseudonymisointi ja muut tekniset toimenpiteet.
61. Yleisen tietosuojaja-asetuksen 25 artiklan mukaista veloitetta sovellettaessa on otettava huomioon uusin tekniikka ja toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille. Lisäselvennyksiä tästä veloitteesta annetaan edellä mainituissa tietosuojaneuvoston 25 artiklassa vahvistettua sisäänrakennettua ja oletusarvoista tietosuojajaa koskevissa suuntaviivoissa 4/2019.

6.2 Tietojen minimointia koskevat toimenpiteet

62. Kolmannen palveluntarjoajan, joka käyttää maksutilitietoja pyydettyjen palvelujen tarjoamiseksi, on myös otettava huomioon tietojen minimoinnin periaate ja kerättävä ainoastaan henkilötietoja,

³⁴ Suuntaviivat 2/2019 yleisen tietosuojaja-asetuksen 6 artiklan 1 kohdan b alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä, Euroopan tietosuojaneuvosto, 32 kohta.

³⁵ Suuntaviivat 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, Euroopan tietosuojaneuvosto, s. 29.

jotka ovat tarpeen maksupalvelunkäyttäjän pyytämien tiettyjen maksupalvelujen tarjoamiseksi. Periaatteessa pääsy henkilötietoihin olisi rajoitettava siihen, mikä on tarpeen maksupalvelujen tarjoamiseksi. Kuten 2 luvussa todetaan, toisessa maksupalveludirektiivissä edellytetään, että tiliä ylläpitävät maksupalveluntarjoajat jakavat maksupalvelunkäyttäjän pyynnöstä maksupalvelunkäyttäjän tietoja, kun maksupalvelunkäyttäjä haluaa käyttää maksutoimeksiantopalvelua tai tilitietopalvelua.

63. Jos kaikki maksutilitiedot eivät ole tarpeen sopimuksen täytäntöön panemiseksi, tilitietopalvelun tarjoajan olisi valittava asiaankuuluvat tietoryhmät ennen tietojen keräämistä. Tietoryhmät, jotka eivät välttämättä ole tarpeen, voivat sisältää esimerkiksi hiljaisen osapuolen henkilöllisyyttä koskevat tiedot ja liiketoimen ominaispiirteet. Lisäksi hiljaisen osapuolen pankkitilin IBAN-tilinumeron ei välttämättä tarvitse olla näkyvissä, ellei jäsenvaltion lainsäädännössä tai unionin oikeudessa toisin edellytetä.
64. Tässä yhteydessä voitaisiin harkita osana yleisen tietosuojasetuksen 24 artiklan 2 kohdan mukaisen asianmukaisen tietosuojapolitiikan täytäntöönpanoa sellaisten teknisten toimenpiteiden mahdollista soveltamista, joilla mahdollistetaan kolmansien palveluntarjoajien velvollisuus saada ja hakea ainoastaan palvelujensa tarjoamiseen tarvittavia henkilötietoja tai joilla tuetaan kolmansia palveluntarjoajia tämän velvollisuuden osalta. Tältä osin tietosuojaneuvosto suosittelee digitaalisten välineiden käyttöä, jotta voidaan tukea tilitietopalvelun tarjoajia niiden velvoitteessa kerätä ainoastaan henkilötietoja, jotka ovat välttämättömiä niiden käsittelyn tarkoitusten kannalta. Esimerkiksi silloin, kun palveluntarjoaja ei tarvitse liiketoimen ominaispiirteitä (tapahtumatietueiden kuvauskentässä) palvelunsa tarjoamiseksi, digitaalinen valintaväline voisi toimia keinona, jonka avulla kolmannet palveluntarjoajat voivat jättää tämän kentän kolmannen palveluntarjoajan suorittamien käsittelytoimien ulkopuolelle.

Esimerkki 2:

HappyPayments, eli esimerkin 1 tilitietopalvelun tarjoaja, haluaa varmistaa käsittelevänsä ainoastaan niitä henkilökohtaisia maksutilitietoja, joista sen käyttäjät ovat kiinnostuneita. Pääsyn saaminen suurempaan määrään maksutilitietoja ei olisi tarpeen palvelun tarjoamiseksi. Sen ansiosta käyttäjät voivat valita, minkä tyyppisistä tiedoista ne ovat kiinnostuneita.

Käyttäjä A tahtoo yleiskatsauksen menoistaan kahdelta viimeksi kuluneelta kuukaudelta. Käyttäjä pyytää näin ollen kahta pankkitiliään, joilla on kaksi eri tiliä ylläpitävää maksupalveluntarjoajaa, koskevat tiedot kaikista kahden viimeksi kuluneen kuukauden tapahtumista, tapahtumien määristä, toteutuspäivistä ja vastaanottajan nimistä ja rastittaa vastaavat kohdat HappyPaymentsin käyttöliittymässä.

HappyPayments alkaa tämän jälkeen pyytää asianomaisilta tiliä ylläpitäviltä maksupalveluntarjoajilta ainoastaan käyttäjän A valitsemia kenttiä vastaavia tietoja ja ainoastaan kahden viimeksi kuluneen kuukauden ajalta. "Viestin" tai edes IBAN-tilinumeron kaltaisia tietoja ei pyydetä, sillä käyttäjä A ei pyytänyt näitä tietoja.

Jotta HappyPayments voisi noudattaa tietojen minimointia koskevia velvoitteitaan, tiliä ylläpitävät maksupalveluntarjoajat antavat HappyPaymentsin pyytää tiettyjen ajankohtien tiettyjen kenttien tietoja.

65. Tältä osin on myös huomattava, että toisen maksupalveludirektiivin mukaisesti tiliä ylläpitävät maksupalveluntarjoajat saavat antaa pääsyn ainoastaan maksutilitietoihin. Toisessa maksupalveludirektiivissä ei säädetä oikeusperustasta, joka koskee pääsyn antamista muiden tilien, kuten säästötilien, asuntolainatilien tai sijoitustilien, sisältämiin henkilötietoihin. Näin ollen

toisen maksupalveludirektiivin nojalla on toteutettava teknisiä toimenpiteitä sen varmistamiseksi, että pääsy rajoitetaan tarvittaviin maksutilitietoihin.

66. Sen lisäksi, että palveluntarjoajan on kerättävä mahdollisimman vähän tietoja, sen on myös otettava käyttöön rajoitettu säilytysaika. Palveluntarjoajan ei tulisi säilyttää henkilötietoja pidempään kuin on tarpeen maksupalvelunkäyttäjän pyytämiin tarkoituksiin nähden.
67. Jos rekisteröidyn ja tilitietopalvelun tarjoajan välinen sopimus edellyttää henkilötietojen siirtämistä kolmansille osapuolille, ainoastaan sopimuksen täytäntöönpanon kannalta välttämättömät henkilötiedot voidaan siirtää. Rekisteröidyille olisi myös nimenomaisesti ilmoitettava tietojen toimittamisesta ja niistä henkilötiedoista, jotka kyseiselle kolmannelle osapuolelle aiotaan siirtää.

6.3 Turvallisuus

68. Tietosuojaneuvosto on jo korostanut, että taloutta koskevien henkilötietojen loukkaamisella on ”selvästi rekisteröidyn arkeen kohdistuvia vakavia vaikutuksia”, ja mainitsee esimerkkinä maksuvälinepetosten riskin.³⁶
69. Jos tietoturvaloukkaukseen liittyy talouteen liittyviä tietoja, rekisteröity voi altistua huomattaville riskeille. Vuotaneista tiedoista riippuen rekisteröidyt voivat joutua alttiiksi identiteettivarkaudelle tai heidän tiliensä varojen ja muun omaisuuden varastamiselle. Lisäksi on mahdollista, että maksutapahtumaa koskevien tietojen paljastumiseen liittyy huomattavia yksityisyyden suojaan liittyviä riskejä, sillä maksutapahtumaa koskeviin tietoihin voi sisältyä viittauksia kaikkiin rekisteröidyn yksityiselämän osa-alueisiin. Samalla taloutta koskevat tiedot ovat luonnollisesti arvokkaita rikollisille ja siten houkutteleva kohde.
70. Maksupalveluntarjoajat ovat rekisterinpitäjinä velvollisia toteuttamaan asianmukaiset toimenpiteet rekisteröityjen henkilötietojen suojaamiseksi (yleisen tietosuoja-asetuksen 24 artiklan 1 kohta). Mitä suurempi on rekisterinpitäjän suorittamaan tietojenkäsittelyyn liittyvä riski, sitä tiukempia turvallisuusvaatimuksia on sovellettava. Koska talouteen liittyvien tietojen käsittelyyn liittyy monenlaisia vakavia riskejä, turvatoimien olisi oltava vastaavalla tavalla tiukat.
71. Palveluntarjoajien olisi noudatettava tiukkoja vaatimuksia, mukaan lukien asiakkaan vahvan tunnistamisen mekanismit ja teknisten laitteiden tiukat turvallisuusvaatimukset.³⁷ Tärkeitä ovat myös muut menettelyt, kuten henkilötietojen käsittelijöiden turvallisuusvaatimusten tarkastusprosessit ja luvattoman pääsyn estämiseen liittyvät menettelyt.

6.4 Läpinäkyvyys ja osoitusvelvollisuus

72. Läpinäkyvyys ja osoitusvelvollisuus ovat yleisen tietosuoja-asetuksen kaksi peruseriaatetta.
73. Läpinäkyvyyden (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan a alakohta) osalta yleisen tietosuoja-asetuksen 12 artiklassa täsmennetään, että rekisterinpitäjien on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaiset tiedot. Lisäksi siinä edellytetään, että henkilötietojen käsittelyä koskevien tietojen tai viestien on oltava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tiedot on esitettävä selkeällä ja yksinkertaisella kielellä ja kirjallisesti ”tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa”. Tietosuojaneuvoston

³⁶ Tietosuojatyöryhmän ohjeet tietosuojaaja koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”, WP 248 rev.01 (tietosuojaneuvoston hyväksymä asiakirja).

³⁷ Ks. tekniset sääntelystandardit.

hyväksymissä tietosuojatyöryhmän asetuksen 2016/679 mukaista läpinäkyvyyttä koskeissa suuntaviivoissa annetaan erityisiä ohjeita läpinäkyvyyden periaatteen noudattamisesta digitaalisessa ympäristössä.

74. Edellä mainituissa asetuksen 2016/679 mukaista läpinäkyvyyttä koskeissa suuntaviivoissa todetaan, että yleisen tietosuoja-asetuksen 11 artiklaa olisi tulkittava siten, että sillä varmistetaan ”todellinen” tietojen minimointi heikentämättä kuitenkaan rekisteröityjen oikeuksien käyttämistä, ja että rekisteröidyn on voitava käyttää näitä oikeuksia antamalla lisätietoja. On mahdollista, että rekisterinpitäjä käsittelee sellaisia henkilötietoja, jotka eivät edellytä rekisteröidyn tunnistamista (esimerkiksi pseudonymisoidut henkilötiedot). Tällöin voi tulla kyseeseen myös 11 artiklan 1 kohta, jonka mukaan rekisterinpitäjällä ei ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten, jos tämä olisi tarpeen vain tietosuoja-asetuksen noudattamiseksi.
75. Toisen maksupalveludirektiivin mukaisten palvelujen osalta yleisen tietosuoja-asetuksen 13 artiklaa sovelletaan rekisteröidyltä kerättyihin henkilötietoihin ja 14 artiklaa sovelletaan, jos rekisteröidyltä ei ole saatu henkilötietoja.
76. Rekisteröidylle on erityisesti ilmoitettava henkilötietojen säilytysaika, tai jos tämä ei ole mahdollista, perusteet, joiden perusteella kyseinen aika määritetään, sekä tarvittaessa rekisterinpitäjän tai mahdollisen kolmannen osapuolen oikeutetut edut. Jos käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohdassa tarkoitettuun suostumukseen tai yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohdassa tarkoitettuun nimenomaiseen suostumukseen, rekisteröidylle on ilmoitettava oikeudesta peruuttaa suostumus milloin tahansa.
77. Rekisterinpitäjän on toimitettava tiedot rekisteröidylle ottaen huomioon tietojen käsittelyyn liittyvät erityiset olosuhteet. Jos henkilötietoja käytetään viestintään asianomaisen rekisteröidyn kanssa, kuten tilitietopalvelun tarjoajien tapauksessa todennäköisesti tehdään, tiedot on toimitettava viimeistään silloin kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran.³⁸ Jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, tiedot on toimitettava viimeistään silloin, kun näitä tietoja luovutetaan ensimmäisen kerran.
78. Verkkomaksupalvelujen osalta edellä mainituissa suuntaviivoissa selvennetään, että rekisterinpitäjät voivat hyödyntää digitaalisessa ympäristössä monitasoista esitystapaa, jossa läpinäkyvyyden varmistamisessa käytetään eri menetelmien yhdistelmää. Erityisen suositeltavaa on, että tietosuojaselosteissa rekisteröidylle annettavien tietojen ryhmät tulisi yhdistää toisiinsa monitasoisesti sen sijaan, että kaikki selosteen tiedot esitettäisiin näytöllä yhdellä kertaa. Tällä tavalla voidaan välttää informaatioahkyä ja samalla varmistetaan informoinnin tehokkuus.
79. Edellä mainituissa suuntaviivoissa selvennetään myös, että rekisterinpitäjät voivat halutessaan käyttää muita keinoja, kuten tietosuojaa koskevia hallintapaneeleita, tietojen antamiseksi yksittäiselle rekisteröidylle. Tietosuojaa koskeva hallintapaneeli on sivu, jolla rekisteröidyt voivat tutustua samassa paikassa kaikkiin tietosuojaa koskeviin tietoihin ja hallita omia tietosuoja-asetuksiaan sallimalla tai estämällä henkilötietojensa eri käyttötapoja kyseisessä palvelussa.³⁹

³⁸ Yleisen tietosuoja-asetuksen 14 artiklan 3 kohdan b alakohta.

³⁹ Tietosuojaneuvoston hyväksymien asetuksen 2016/679 mukaista läpinäkyvyyttä koskevien suuntaviivojen mukaan tietosuojaa koskevat hallintapaneelit ovat käytännöllisiä erityisesti palveluissa, joita rekisteröidyt käyttävät useilla eri laitteilla, sillä paneelin avulla he voivat hallita henkilötietojaan riippumatta siitä, millä laitteella palvelua käyttävät. Kun rekisteröity voi muokata tietosuoja-asetuksiaan manuaalisesti hallintapaneelin

Tietosuoja koskevalla hallintapaneelilla voitaisiin antaa yleiskuva niistä kolmansista palveluntarjoajista, jotka ovat saaneet rekisteröidyn nimenomaisen suostumuksen, ja sillä voitaisiin myös tarjota merkityksellistä tietoa niiden henkilötietojen luonteesta ja määrästä, joihin kolmannet palveluntarjoajat ovat saaneet pääsyn. Tiliä ylläpitävä maksupalveluntarjoaja voi periaatteessa tarjota käyttäjälle yleiskatsauksen avulla mahdollisuuden peruuttaa erityinen toisen maksupalveludirektiivin mukainen nimenomainen hyväksyminen⁴⁰, mikä johtaisi siihen, että yhdeltä tai useammalta kolmannelta palveluntarjoajalta evättäisiin pääsy maksutileihin. Käyttäjä voisi myös pyytää tiliä ylläpitävää maksupalveluntarjoajaa kieltämään pääsyn maksutililleen tai maksutileilleen yhdeltä tai useammalta yksittäiseltä kolmannelta palveluntarjoajalta⁴¹, sillä käyttäjällä on oikeus käyttää tai olla käyttämättä tilitietopalvelua. Jos tietosuoja koskevia hallintapaneeleita käytetään nimenomaisen hyväksynnän antamiseen tai peruuttamiseen, ne olisi suunniteltava ja niitä olisi sovellettava lainmukaisesti ja niitä olisi erityisesti estettävä luomasta esteitä kolmansien palveluntarjoajien oikeudelle tarjota palveluja toisen maksupalveludirektiivin mukaisesti. Tältä osin ja toisen maksupalveludirektiivin sovellettavien säännösten mukaisesti kolmannelta palveluntarjoajalla on mahdollisuus saada käyttäjän nimenomainen hyväksyntä uudelleen sen jälkeen, kun hyväksyntä on peruutettu.

80. Osoitusvelvollisuusperiaate edellyttää, että rekisterinpitäjä toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan yleistä tietosuoja-asetusta ja erityisesti sen 5 artiklan 1 kohdassa säädettyjä keskeisiä tietosuojaperiaatteita. Näissä toimenpiteissä olisi otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski, ja niitä on tarvittaessa tarkistettava ja päivitettävä.⁴²

6.5 Profilointi

81. Maksupalveluntarjoajien suorittamaan henkilötietojen käsittelyyn voi sisältyä yleisen tietosuoja-asetuksen 4 artiklan 4 kohdassa tarkoitettua profilointia. Esimerkiksi tilitietopalvelun tarjoajat saattavat käyttää henkilötietojen automaattista käsittelyä arvioidakseen tiettyjä luonnollisen henkilön henkilökohtaisia ominaisuuksia. Myös rekisteröidyn henkilökohtaista taloudellista tilannetta voidaan arvioida palvelun erityispiirteistä riippuen. Käyttäjien pyynnöstä tarjottaviin tilitietopalveluihin voi sisältyä henkilökohtaisten maksutilitietojen laaja arviointi.
82. Rekisterinpitäjän on myös kerrottava rekisteröidylle avoimesti automaattisen päätöksenteon, muun muassa profiloinnin, olemassaolosta. Tällaisissa tapauksissa rekisterinpitäjän on annettava merkitykselliset tiedot käsittelyyn liittyvästä logiikasta sekä ilmoitettava, mikä on kyseisen käsittelyn merkittävyys ja mitkä ovat sen mahdolliset seuraukset rekisteröidylle (13 artiklan 2 kohdan f alakohta ja 14 artiklan 2 kohdan g alakohta sekä johdanto-osan 60 kappale).⁴³ Samoin rekisteröidyllä on yleisen tietosuoja-asetuksen 15 artiklan mukaisesti oikeus pyytää ja saada rekisterinpitäjältä tietoja automaattisen päätöksenteon, muun muassa profiloinnin olemassaolosta, käsittelyyn liittyvästä logiikasta ja seurauksista rekisteröidylle sekä tietyissä

kautta, myös tietosuojaseloste on helpompi räätälöidä yksilöllisesti niin, että siinä käsitellään vain kyseistä rekisteröityä koskevaa henkilötietojen käsittelyä.

⁴⁰ Ks. esimerkiksi toisen maksupalveludirektiivin 67 artiklan 2 kohdan a alakohdassa mainittu 'nimenomainen hyväksyminen'.

⁴¹ Ks. myös EBA/OP/2020/10, 45 kohta.

⁴² Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 24 artikla.

⁴³ Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat, WP 260 rev.01 (Euroopan tietosuojaneuvoston hyväksymä asiakirja).

olosuhteissa oikeus vastustaa profilointia riippumatta siitä, tehdäänkö pelkästään automatisoituja profilointiin perustuvia yksittäispäätöksiä.⁴⁴

83. Lisäksi tässä yhteydessä olennaista on myös se, että rekisteröidyillä on yleisen tietosuojasetuksen 22 artiklan mukaisesti oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Tähän sääntöön sisältyy tietyissä olosuhteissa myös rekisterinpitäjien tarve toteuttaa asianmukaiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi, mukaan lukien käsittelystä ilmoittaminen rekisteröidylle, oikeus vaatia, että päätöksentekoon osallistuu luonnollinen henkilö, ja oikeus esittää kantansa ja riitauttaa päätös. Kuten myös yleisen tietosuojasetuksen johdanto-osan 71 kappaleessa todetaan, tämä tarkoittaa muun muassa sitä, että rekisteröidyillä on oikeus olla joutumatta päätöksen, kuten online-luottohakemuksen automaattinen epäämisen ilman ihmisen osallistumista, kohteeksi.⁴⁵
84. Automatisoidut päätökset, mukaan lukien profilointi, joihin liittyy erityisiä henkilötietoryhmiä, ovat sallittuja vain yleisen tietosuojasetuksen 22 artiklan 4 kohdan mukaisin kumulatiivisin edellytyksin:
- on olemassa sovellettava 22 artiklan 2 kohdan mukainen poikkeus
 - ja sovelletaan 9 artiklan 2 kohdan a tai g alakohtaa. Molemmissa tapauksissa rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi.⁴⁶
85. Lisäksi olisi noudatettava näissä ohjeissa esitettyjä myöhempää käsittelyä koskevia vaatimuksia. Automatisoituja yksittäispäätöksiä ja profilointia koskevat täsmennykset ja ohjeet, jotka on annettu tietosuojaneuvoston hyväksymissä tietosuojatyöryhmän suuntaviivoissa automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, ovat täysin merkityksellisiä maksupalvelujen kannalta, minkä vuoksi ne olisi otettava asianmukaisesti huomioon.

Euroopan tietosuojaneuvoston puolesta

Puheenjohtaja

(Andrea Jelinek)

⁴⁴ Tietosuojatyöryhmän suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01.

⁴⁵ Yleisen tietosuojasetuksen johdanto-osan 71 kappale.

⁴⁶ Tietosuojatyöryhmän suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01, s. 24.