

Finanssiala ry:n pääviestit PSD2 uudelleentarkastelusta

- On liian aikaista tehdä johtopäätöksiä edellisen sääntelykierroksen vaikutuksista
- Laajentavaa lisäsääntelyä tulee välttää
- API-toiminnallisuuksien osalta tulisi määrittää perustaso palveluille, joiden on oltava niiden kautta saatavissa
- PSD2 suhde GDPR- ja AML-sääntelyyn selvennettävä
- Sääntelyn vastaista toimintaa on suitsittava tehokkaasti

1 Edellisen sääntelykierroksen vaikutukset eivät vielä ole selvillä

1.1 Maksamisen turvallisuus

Yhtenä PSD2 tavoitteista oli maksamisen turvallisuuden parantaminen. Tämä tapahtui tuomalla vahvan tunnistamisen vaatimus sähköisesti tapahtuvaan maksamiseen. Muun muassa tunnistamisen käyttöönottoon vaatimusten käyttöönotosta ja korttimaksamisen infrastruktuurin monimutkaisuudesta johtuen vahvan tunnistamisen käyttöönotto osoittautui ennakoitua vaikeammaksi ja sääntelyn voimaantuloa jouduttiin lykkäämään vuoden 2020 loppuun saakka. Tämän vuoksi tietoa vahvan tunnistamisen vaikutuksista maksamisen turvallisuuteen on kertynyt vasta varsin lyhyeltä ajalta.

On myös huomattava, että sääntely sisältää suuren määrän poikkeuksia vahvan tunnistamisen vaatimuksesta. Kannatamme Euroopan pankkivalvoja EBA:n linjausta siitä, että poikkeusten käyttöönotto on tilipankin harkinnassa. Muu vaihtoehto ei mielestämme ole mahdollinen niin kauan, kuin tilipankilla on ensi- ja viimekätinen vastuu ilman vahvaa tunnistamista tapahtuvien oikeudettomien maksutapahtumien korvaamisesta asiakkaalle. On myös huomattava, että vaikka asiakas voisikin saada korvauksen pankiltaan, tuottavat oikeudettomat maksutapahtumat aina ylimääräistä huolta ja vaivaa. Pankit ovatkin edenneet poikkeusten käyttöönotossa järkevää varovaisuutta noudattaen.

1.2 Uudet innovatiiviset, edulliset palvelut

PSD2 tavoitteena oli lisääntyvän kilpailun myötä tuottaa maksupalvelujen hyödyntäjille uusia, innovatiivisia palveluita edulliseen hintaan.

Uusia innovatiivisia palveluita ei varsinkaan Suomessa ole vielä juurikaan nähty. Maksunkäynnistyspalveluissa näyttää siltä, että perinteiset toimijat ovat siirtyneet sopimuspohjaisista, maksullisista pankkiliittymistä ilmaisten PSD2-rajapintojen käyttöön ja joitakin uusia toimijoita on tullut markkinalle. Pankkien tiedossa ei ole, onko tämä vaikuttanut esim. kauppiaiden maksupalveluistaan maksamiin hintoihin.

2 Lisäsääntelyä tulee välttää

PSD2 on erittäin monimutkainen ja -tulkintainen sääntelykokonaisuus, jonka vaikutuksista ei ole vielä saatavilla riittävästi tietoa ja kokemuksia. Uusien asioiden tuominen sääntelyn piiriin lisäisi monimutkaisuutta ja toisi uusia tulkintakysymyksiä. Erityisesti haluamme tuoda esiin seuraavat näkökulmat

2.1 API-rajapinnat

Sääntelyssä omaksuttiin alun perin lähtökohta, että PSD2 mukaisten API-rajapintojen määrittely ja rakentaminen tapahtuu markkinaehtoisesti. Tämä johti siihen, että syntyi useampia markkinastandardeja ja näiden muunnelmia, joiden mukaan tilinpitäjät ovat toteuttaneet rajapintojaan. API-rajapintojen hyödyntäjien oli siis rakennettava erilaisia integraatioita eri tilinpitäjiin nähden.

Vaikka tällainen useamman eri integraation tilanne ei ole optimaalinen, ei lisäsääntely yhden standardin luomiseksi tässä vaiheessa ole tervetullutta. On huomioitava, että integraatioiden vaatimat investoinnit on jo tehty. Yhden standardin käyttöönotto lainsäädäntötoimin aiheuttaisi sen, että investoinnit jouduttaisiin tekemään uudestaan.

Mielestämme mahdollisen yhden standardin kehittäminen tulisi jättää markkinoiden tehtäväksi. Sellainen kehittyä ajan kuluessa, mikäli se katsotaan liiketoiminnallisesti kannattavaksi ja siihen liitytään siinä tahdissa kuin se toimijoiden talouden kannalta on järkevää.

API-rajapintojen kautta tarjottavien palveluiden sääntelyä tulee myös muuttaa. Malli, jossa tilinpitäjäpankkien on rakennettava kaikki uudet toiminnallisuudet, tekniset ratkaisut ja palvelut myös PSD2-rajapinnan kautta tarjottavaksi, on erittäin raskas ja lisää kehittämisen kustannuksia kohtuuttomasti. Tämä on voi rajoittaa tilinpitäjien mahdollisuuksia uusien palveluiden kehittämiseen ja aiheuttaa sekä kilpailun vääristymistä että vähemmän kuluttajia hyödyttäviä innovaatioita.

2.2 Pankkipalvelujen saavutettavuus (Financial Inclusion)

Kuluttajien oikeudesta ns. peruspankkipalveluihin on säädetty EU:n Maksutilidirektiivissä (Payment Accounts Directive, PAD). Sen mukaan kaikilla EU-/ETA-alueella laillisesti asuvilla henkilöillä on oikeus perusmaksutilin ja siihen liittyvien palvelujen saamiseen. Edellytykset tilin avaamisesta kieltäytymiselle ovat erittäin tiukat; se on mahdollista ainoastaan, jos pankilla on perusteltu syy epäillä asiakkaan osallisuutta rahanpesurikollisuuteen tai terrorismin rahoittamiseen. Käytännössä myös henkilöllisyyden todistavien asiakirjojen puute voi estää tilin avaamisen. Luonnollisten henkilöiden osalta nykysääntely siis mahdollistaa pankkipalvelujen auki saamisen aina, kun se muun lainsäädännön estämättä on mahdollista.

Jonkin verran esillä ollut peruspankkipalveluoikeuden laajentaminen (pien)yrityksiin vaatii tarkkaa harkintaa. Se olisi iso periaatteellinen kavennus pankkien mahdollisuuteen päättää itsenäisesti omista liiketoimintastrategioistaan ja luoda palvelumalleja, joissa keskitytään tietyn tyyppisten yritysasiakkaiden palvelemiseen. On myös huomattava, että yritysten pankkiasioinnissa tarvittavat tuotteet ovat erilaiset ja usein laajemmat kuin yksityishenkilöiden asiointinsa tarvitsemat. Yritysten

pankkiasioinnin tavat myös vaihtelevat paljon eri Euroopan maissa. Näin ollen yhden Euroopan-tasoisien peruspalvelupaketin määrittäminen olisi erittäin haastava tehtävä.

3 Sääntelyn suhde tietosuojasääntelyyn tulee selventää

PSD2-sääntelyn peruseräite on, että tilinpitäjäpankin ja PSD2 API-rajapintoja hyödyntävien palveluntarjoajien välillä ei ole sopimussuhdetta. Osapuolten ei siis ole mahdollista neuvotella rajapintojen käytöstä ja esim. niiden kautta jaettavista tiedoista. Lähtökohta on, että asiakas eli tilinomistaja tekee sopimuksen palveluntarjoajan kanssa ja antaa tälle suostumuksensa tilille pääsyyn API-rajapinnan kautta. PSD2 lähtee siitä, että asiakkaan ja palveluntarjoajan käytettävissä ovat samat toiminnallisuudet ja palvelut kuin niissä sähköisissä palveluissa, joita pankki itse tarjoaa asiakkailleen.

PSD2 lähtökohta, jonka Euroopan pankkivalvontaviranomainen EBA myös on omassa kannanotoissaan vahvistanut, on siis se, että PSD2 rajapintojen kautta jaetaan kaikki sama tieto, joka on asiakkaan saavutettavissa pankin tarjoamassa verkkopalvelussa. Euroopan tietosuojaviranomainen EDPB on kuitenkin omassa, PSD2 voimaantulon jälkeen julkaistussa ohjeessaan omaksunut tästä lähtökohdasta poikkeavia näkemyksiä. Sen mukaan pankkien tulisi esim. suodattaa rajapintojen kautta annettavia tietoja siten, että ns. arkaluonteisia (esim. terveydentilaan tai poliittiseen vakaumukseen liittyviä) henkilötietoja ei anneta niiden kautta.

EDPB:n ohje, joka toistaiseksi on suosituksen tasolla, on siis ristiriidassa PSD2 periaatteiden kanssa. Tällainen ristiriita kahden eri valvojan ohjeistuksen välillä asettaa pankit erittäin hankalaan tilanteeseen, koska molemmilla valvojilla on itsenäinen ja toisistaan riippumaton oikeus määrätä sanktioita omaan hallinnonalaansa kuuluvan lainsäädännön ja ohjeistuksen noudattamatta jäämisestä.

Käytännössä PSD2 API-toiminnallisuuksien muokkaaminen mahdollistamaan EDPB:n ohjeen mukainen tietojen suodattaminen veisi järkevyyden esim. PSD2 mukaiselta tilitietopalvelulta. Kyseisessä palvelussa on kysymys siitä, että asiakas voi kerätä eri pankeissa olevien tiliensä tilitapahtumat ja saldot yhdessä sovelluksessa tarkasteltavaksi. Mikäli tilitietopalveluun tuotaisiin suodatettua tietoa, jäisi tietoja, esim. maksunsaajien nimiä, puuttumaan maksutapahtumilta, jolloin tiedon käytettävyys rapautuisi. Suodatusten vaatimien päättelyiden rakentaminen pankeissa olisi myös suuri työ ja sisältäisi paljon epävarmuustekijöitä.

PSD2 ja GDPR välinen suhde tulisi PSD2 uudelleentarkastelun yhteydessä kirkastaa.

4 Sääntelyn vastaista toimintaa on suitsittava tehokkaasti

PSD2 säätämisen yhtenä ponttimena oli tehdä laittomiksi markkinoilla kehittyneet tavat, joilla pankkien ulkopuoliset palveluntarjoajat mahdollistivat asiakkaan tilille kirjautumisen (Screen Scraping, Reverse Engineering jne) ja korvata ne PSD2 API:en kautta tapahtuvalla, luvanvaraisella asioinnilla.

Tällä hetkellä näyttää kuitenkin siltä, että em. menetelmiä on edelleen markkinoilla käytössä. Olisi erittäin tärkeää, että valvontaviranomaiset puuttuisivat näihin käytäntöihin tehokkaasti.

Ennen PSD2 voimaantuloa ennakoitiin, että markkinoille saattaisi tulla ns. API-integraattoreita, jotka tarjoaisivat lisensoiduille kolmansille (Third Party Providers, TPP) toimijoille valmiita teknisiä ratkaisuja useampien pankkien API-rajapintojen hyödyntämiseen. Suomessa näyttää kuitenkin kehittyneen ns. TPP-as-a-service -malleja TPPaaS), joissa yksi lisensoitu toimija hyödyntää pankin API-rajapintaa ja tarjoaa tätä palvelua muille toimijoille, jotka tarjoavat palveluja loppukäyttäjille eli tilinomistajille. Tässä mallissa jää epäselväksi, kenen kanssa asiakkaalla on sopimus palvelusta, kenelle hän on antanut suostumuksensa tilille pääsyyn ja millä palveluntarjoalla on (tilipankin lisäksi) vastuu esim. oikeudettomista maksutapahtumista.

PSD2 uudelleentarkastelun yhteydessä tulisi ottaa kantaa TPPaaS-palvelun lainmukaisuuteen sekä arvioida uudelleen esim. vastuu- ja suostumuksen antamiskysymyksiä.

FINANSSIALA RY

Hannu Ijäs