M Ö T E S A N T E C K N I N G A R

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Datum 2018-07-20 FI Dnr 18-9872
Författare Finansinspektionen
Möte Rundabordssamtal om PSD 2
(Närvarande) Deltagare från branschen

Branschsamtal om det andra betaltjänstdirektivet (PSD 2)

Mot bakgrund av det andra betaltjänstdirektivet (PSD 2) som trädde i kraft den 1 maj 2018 bjöd Finansinspektionen (FI) in till ett rundabordssamtal med finansiella företag, branschföreningar och myndigheter som berörs av regelverket. Samtalen ägde rum den 18 juni. De finansiella företagen bjöds in via olika branschorganisationer.

Syftet med samtalen var att ge relevanta parter ett tillfälle att diskutera de hinder och problem som aktörer på marknaden upplever inom ramen för det nya regelverket. Nedan följer en sammanfattning av de mest förekommande hinder som diskuterades under samtalen samt konsekvenser och aktörernas förslag på lösningar på identifierade problem.

Resultatet från samtalen kommer av den diskussion som hölls av deltagarna i grupper. Vid samtalen har representanter från FI fört anteckningar och därefter sammanställt anteckningarna. Anteckningarna är baserade på deltagarnas upplevda hinder och inte myndighetens. FI kommer däremot att arbeta med de frågor och hinder som diskuterades under mötet och ha som ambition att försöka besvara dessa i form av en promemoria så snart som möjligt men senast i slutet av 2018.

Sammanställda anteckningar från samtalen

Nedan följer identifierade problem (hinder, begränsningar och osäkerheter):

1. Ansvar vid flerpartsförhållanden avseende kundens data

Vem ansvarar för kundens information? Vad händer om kundens information sprids till fler aktörer än tredjepartsleverantören? Finns det garantier för att tredjepartsleverantör inhämtat nödvändigt samtycke från kunderna? Kan tredjepartsleverantören inhämta mer information än betalkontoinformation och vem kontrollerar att informationen inte sprids på fel sätt?

2. Otydliga regler

Reglerna kring betaltjänster är inte tydliga och det kan skapa problem för mindre aktörer. Större aktörer har generellt bättre resurser och är bättre förberedda på nya krav. EBA:s riktlinjer lämnar vidare utrymme för olika tolkningar av reglerna. Det

finns också en osäkerhet kring definitionen av ett betalkonto då tjänster som ryms inom definitionen betalkonto varierar mellan olika institut.

3. Autentisering
Olika aktörer tillhandahåller olika metoder för autentisering, till exempel kortläsare, säkerhetsdosa och användarnamn/lösenord. Det innebär att det ställs krav på företag som utvecklar API:er att skapa en autentiseringslösning som kan hantera många olika metoder för autentisering.

4. Godkännande av API:er
Det finns frågetecken gällande godkännandeprocessen för API:er enligt artikel 33.6 i RTS (EU) 2018/389. Hur ska en ansökan gå till praktiskt och vilka parametrar kommer att mätas? Det är även oklart vad som avses med uttrycket att en API har använts i stor utsträckning. Det är oklart hur kriterierna kommer att bedömas. Det finns också en osäkerhet om kriterierna och bedömningarna kommer att vara gemensamma för hela EU. Det förutspås kunna leda till problem om det inte fungerar på ett likartat sätt inom EU. Tiden är en annan viktig aspekt vid ansökningstillfället. Om en aktör byggt ett API som inte uppfyller kraven innebär det att aktören får mindre tid på sig än vad som krävs för att bygga en fallbacklösning.

5. Undantagsmöjligheten (eng. fall back solution)
Det finns oklarheter kring undantagsmöjligheten. Vad är definitionen av ”fall back solution”? Vilken nytta har undantagsmöjligheten då de tekniska kraven som ställs är nästintill att likställa med att utveckla API:er? Undantagsmöjligheten bedöms som kontraproduktiv eftersom att enkelheten med API:er och den tekniska utvecklingen kan komma att hindras. Hur ska bolagen förhålla sig i avvaktan på att FI granskar kontoförande instituts ansökan om att få utnyttja undantagsmöjligheten? Det bedöms vara resurskrävande för såväl kontoförande institut som tredjepartsleverantör att vara förberedda på att kunna använda två olika tekniska ingångar för tillgång till betalkontoinformation (API och fall back solution), samt att snabbt kunna växla mellan dessa tekniker.

Ett annat frågetecken kring EBA:s riktlinjer är att ett kontoförande institut kan beviljas dispens från kravet att ha en undantagsmöjlighet innan ett API har prövats av marknaden. Det kan finnas brister i API funktioner som inte fångas upp av en prövning baserad på vissa kriterier.

6. Omdirigering
Det saknas en närmare definition av vad som ska betraktas som ett hinder av tillhandahållandet av betalningsinitierings- och kontoinformationstjänster enligt artikel 32.3 i RTS (EU) 2018/389. Detta gäller särskilt vid omdirigering.
Det måste finnas en tillit till den första autentiseringen i kedjan och att det räcker för betaltjänstanvändaren att endast identifiera sig en gång. Om tredjepartsleverantörer ska kunna konkurrera med banker (eller Swish) måste kundens identifiering vara enkel. Om det finns krav på att identifiera sig flera gånger finns risken att kunden väljer en annan aktör. Möjligheten för tredjepartsleverantörer att inte använda omdirigering är en förutsättning för

konkurrens på marknaden.

7. **Identifiering**
Hur ska ett kontoförande institut avgöra om en juridisk person har samtliga nödvändiga tillstånd för att vara en tredjepartsleverantör? Det finns standarder för certifiering men inte tillräckligt många företag uppfyller kraven för att vara kvalificerade tillhandahållare av betrodda tjänster. Det finns också en viss osäkerhet hos tredjepartsleverantörer avseende hur de ska säkerställa att de identifierar sig mot rätt aktör och inte mot en bedräglig aktör som utger sig för att vara ett kontoförande institut.

Nedan följer identifierade konsekvenser på några av ovanstående problem:

- **Ansvar vid flerpartsförhållanden avseende kundens data**
- Eventuella ingripanden från Datainspektionen.
- Eventuellt missnöje från kunden riktas mot det kontoförande institut som tillhandahåller kundens betalkonton även i de fall då det är tredjepartsleverantören alternativt en ytterligare aktör som använt eller spridit kundens uppgifter mot dess intresse.
- Det kontoförande institutet saknar möjligheter att kontrollera och ansvara för hur och av vem kundens data används efter att de lämnat informationen till en tredjepartsleverantör.
- En allmän risk för rättslig osäkerhet.
- Kundupplevelsen försämras om tredjepartsleverantörer inte får tillgång till viss data (sådan som faller utanför PSD 2).

- **Autentisering**
- Det går inte att bygga färdigt lösningar innan det står klart hur certifikaten för betrodda tjänster ska fungera.
- När det gäller utvecklandet av API:er finns risk att de kontoförande instituten parallellt måste upprätta en fall back lösning vilket kan bli kostsamt.
- Det finns en ryktesrisk om API:er inte blir godkända.
- Kundupplevelsen kan försämras om identifiering tar för lång tid eller måste upprepas.

- **Undantagsmöjligheten (fall back solution)**
- Det finns en risk att aktörerna arbetar med att anpassa teknik efter en tänkt lösning som sedan inte godkänns av FI.
- Det är kostsamt och resurskrävande att ta fram och förvalta de två olika ingångarna (API och fall back solution).

- **Omdirigering**
- Konsekvensen av att regelverket inte är tydligt kan skapa osäkerhet på marknaden.

- **Identifiering**

- Det finns en risk att legitima tredjepartsleverantörer stängs ute på fel grunder.
- Risk att ”bedrägliga” tredjepartsleverantörer får tillgång till betalkontoinformation utan att ha rätt till det.

Nedan följer identifierade lösningsförslag på några av ovanstående problem:

- **Ansvar vid flerpartsförhållanden avseende kundens data**

- Tydlig och transparent dialog mellan parterna. Tredjepartsleverantören skulle därigenom kunna leverera uppgifter till det kontoförande institutet avseende vem de överlämnat information till samt vilka uppgifter som överlämnats. På så sätt kan det kontoförande institutet få bättre kontroll över kundens data vilket kan underlätta i kontakten med kunden.

- **Autentisering**

- Tidig och tydlig vägledning från FI på en rad områden.
- Lösningarna behöver vara gemensamma för hela EU.
- När det gäller frågan om kvalificerade tillhandahållare av betrodda tjänster skulle det underlätta med en lösning från FI som möjliggör överblick över betrodda företag.
- API måste möjliggöra smidig autentisering.

- **Undantagsmöjligheten (fall back solution)**

- Det behövs tydlig vägledning från FI samt samarbete mellan aktörerna.
- Det behövs ett tydligt ramverk för hur prövningen av API:er går till.
- Kravet på att det särskilda gränssnittet ska ha använts i stor utsträckning under minst tre månader enligt artikel 33.6 i RTS (EU) 2018/389 bör inkludera en översyn över eventuella klagomål som framförts av tredjepartsleverantörer.
- När kontoförande institut ansöker om undantaget bör det bifogas en lista på samtliga klagomål som riktats mot dem och vilka åtgärder som vidtagits av de kontoförande instituten för att åtgärda problemen.

- **Omdirigering**

- Det behövs tydlig vägledning från FI avseende hinder vid omdirigeringen.

- **Identifiering**

- Det förslag på identifieringslösning som presenterades av FI i samband med mötet kan vara ett tänkbart sätt att lösa problemet. Dock kvarstår problematiken med gränsöverskridande aktörer.