



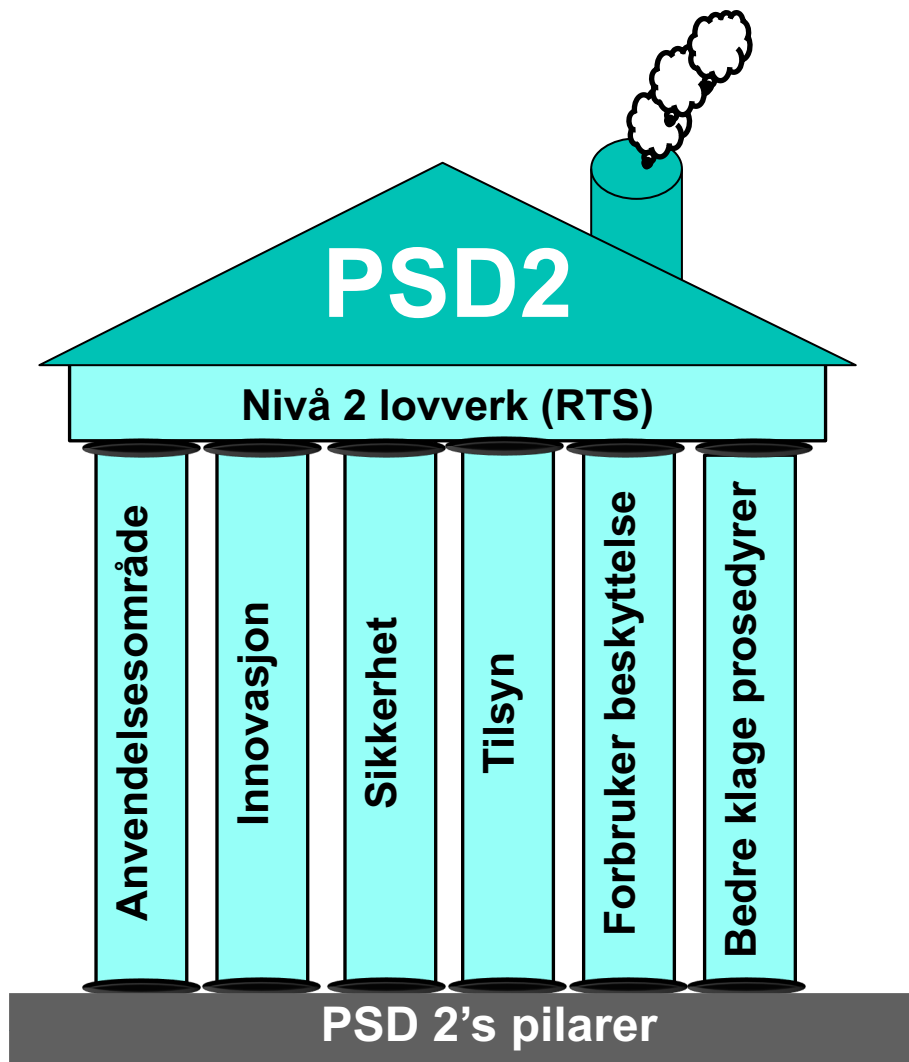
FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

PSD 2

Olav Johannessen
Seksjonsleder tilsyn IT og betalingstjenester
Finanstilsynet

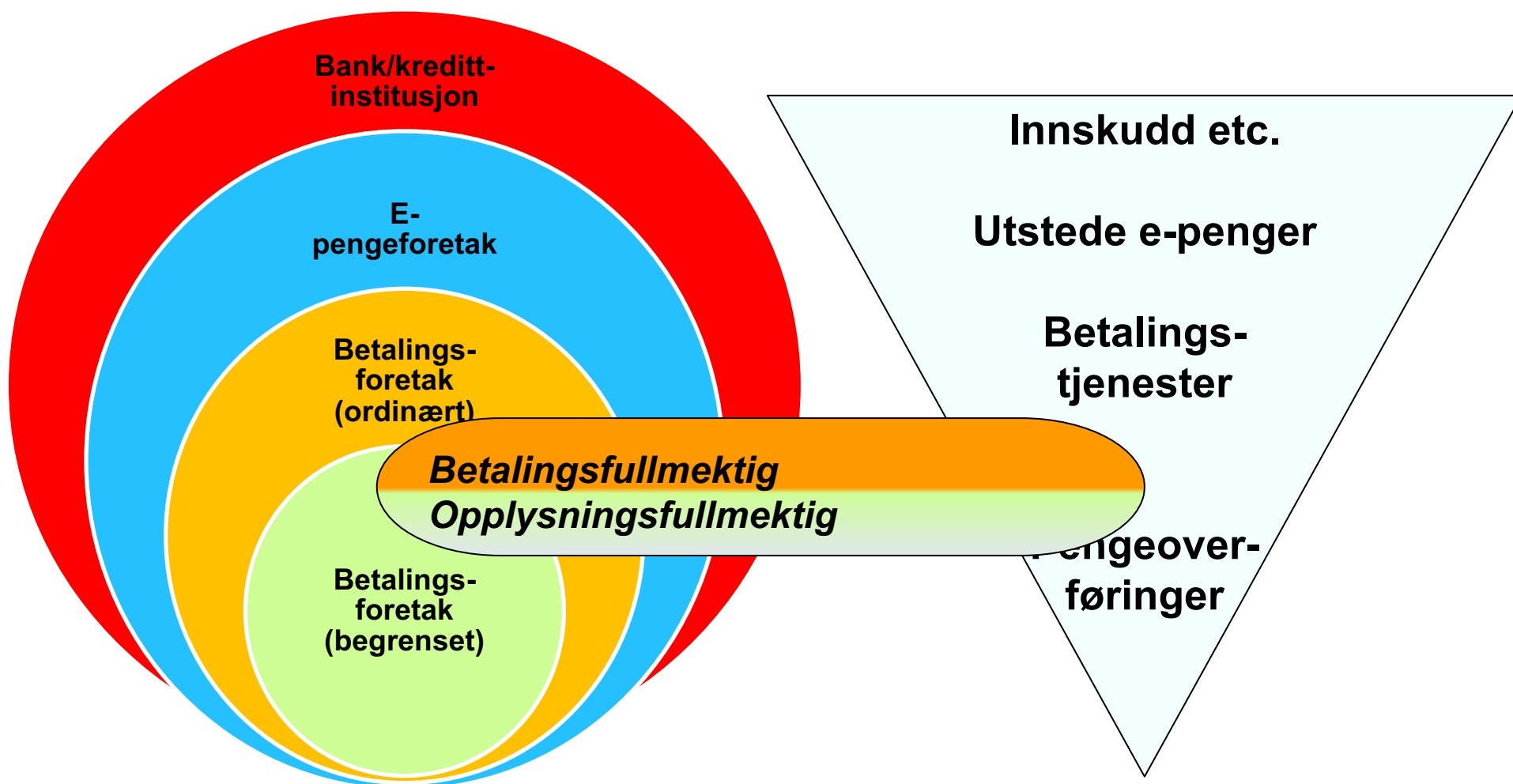
PSD 2 - Hovedhensikter



PSD 2 skal

- Fremme **innovasjon** gjennom **økt konkurranse** mellom eksisterende og nye aktører
- Åpne opp for **flere aktører som betalingstjeneste tilbydere**
- Gi **bredere anvendelsesområde**
- Bidra til **forsterket tilsyn og tilsynssamarbeid** ved grensekryssende virksomhet
- Forsterke **forbruker beskyttelsen**
- Bidra til **høyere sikkerhetskrav** for alle elektroniske betalinger og alle betalingstjeneste tilbydere

Tilbydere av betalingstjenester - Konsesjonstyper



PSD 2 mandater EBA

Leveranser		Milepæler		
		Milestone 2: EBA has published CP with draft GL/TS	Milestone 3: EBA has published Final draft TS or Final GL	Milestone 4: EBA has published GL Compliance table or Commission has published TS in OJ
1	RTS on Passporting Notifications under PSD2	✓	✓	✓
2	GL on Professional Indemnity Insurance under PSD2	✓	✓	✓
3	GL on Incident Reporting under PSD2	✓	✓	✓
4	GL on Authorisation of payment institutions under PSD2	✓	✓	✓
5	GL on Complaints Procedures by CAs under PSD2	✓	✓	✓
6	RTS on Strong Authentication & Secure Comms. under PSD2	✓	✓	✓
7	GL on Operational & Security Measures under PSD2	✓	✓	✓
8	RTS on Central Contact Points under PSD2	✓	✓	✓
9	RTS & ITS on EBA Register under PSD2	✓	✓	2018Q2
10	GL on fraud reporting under PSD2	✓	2018Q2	2018Q3/4
11	RTS on home-host coordination under PSD2	✓	2018Q2	2018 ?

Retningslinjer – Konsesjons-/ Tillatelseskrav (strengt krav)

KONSESJONSKRAV

- ❖ Generelle krav
- ❖ Selskapsinformasjon
- ❖ Beskrivelse og informasjon om tjenesten(e)
- ❖ Forretningsplan
- ❖ Organisasjonsplan
- ❖ Kapitalkrav
- ❖ Sikring av midler
- ❖ Styring og kontroll av virksomheten
- ❖ Hendelseshåndtering og kundeklager
- ❖ Logging og overvåkning av trafikk og hindre tilgang til sensitive betalingsdata
- ❖ Kontinuitetsplaner for virksomheten
- ❖ Rapportering av statistikker på drift, transaksjoner, svindel
- ❖ Sikkerhetspolicy
- ❖ Internkontroll og AML/FT
- ❖ Eierstruktur, Egnethet, finansiering, etc
- ❖ Ledelse, egnethet
- ❖ Revisor
- ❖ Forsikring / garantier / etc

Nye aktører – endret risiko?

Omfattende krav til den operasjonelle virksomheten	Betalings-foretak	Betalings-fullmektig	Opplysnings-fullmektig
Forretningsplan og tjenestene som skal tilbys	V	V	V
Hvordan midler skal sikres	V		
Hvordan virksomheten skal styres og dens kontroll ordninger	V	V	V
Hvordan sikkerhetshendelser skal overvåkes og håndteres	V	V	V
Håndteringen av sensitive betalingsdata	V	V	V
Beredskapsplaner	V	V	V
Operative, mislighets og transaksjons statistikker	V	V	
Sikkerhetspolicy for tjenestene og IT-virksomheten	V	V	V
Hvitvaskingsrutiner	V	V	
Kapitalkrav / Forsikrings-/garantiordninger	V	V	V

Bestemmelser om sterk kundeautentisering og sikre åpne standarder for kommunikasjon er nå fastsatt og vil gjelde fra 14. september 2019. Spesifikasjoner og testfasiliteter klare og tilgjengelig fra 14. mars 2019.

- Spesifiserer krav til bruk av sterk autentisering (SCA)
- Angir unntaksbestemmelser basert på blant annet
 - forhold som risikoprofil for betalingen (risk based), kanal for betalingen, type betaling, betalingsmottaker og beløp
- Angir omfattende krav til ivaretagelse av konfidensialitet og integritet av betalers personlige sikkerhetsinformasjon både når det gjelder bruk og utlevering
- Spesifiserer krav til autentisering og kommunikasjon mellom eksisterende aktører/tilbydere av betalingskonto og nye/eksisterende aktører, som ønsker å tilby de nye betalingstjenestene
- Angir krav til at betalingskontotilbydere må stille til rådighet minst et grensesnitt som tilbyr samme tilgjengelighet, ytelse, support og beredskapstiltak som de grensesnitt som er gjort tilgjengelig for betalingstjenestebrukers direkte tilgang til sine betalingskontoer.
- Angir krav til datautveksling, der bl.a. informasjonen som skal gjøres tilgjengelig gjennom grensesnittene av betalingskontotilbyder skal være minst den samme som ved betalingstjenestebrukerens direkte tilgang.
- Pågående arbeid for å harmonisere tilsynsforståelse og –praksis knyttet til RTS
- Utarbeidelse av dokumentasjon, EBA opinion implementering av RTS, til bruk for tilsynsmyndighetene
- Observatør i API Evaluation Group, etablert av kommisjonen for å rådgive næringen
- EBA's Q&A

Sterk kundeautentisering og sikre åpne standarder for kommunikasjon

- Godkjenning av sikkerhetsmekanismer (tilfredsstille kravet til sterk autentisering).
- Krav til revidering av sikkerhets tiltak av revisor med ekspertise i IKT sikkerhet.
- Unntak fra kravet om SCA ved bedriftsbetalinger gjennom dedikerte betalingsprosesser eller – protokoller
- Krav til dokumentering av metode og modell for å kalkulere svindelnivåer, samt svindelnivåene i seg selv.
- Ved bruk av transaksjonsrisikoanalyse (TRA).
 - skal meddeles tilsynsmyndigheten rimelig tid i forkant
 - krav til umiddelbar rapportering om svindelgrenser overstiges
- Krav til overvåkning og lagring av informasjon ved bruk av unntaksbestemmelser fra krav til sterk autentisering.
- Tilsynsmyndigheten skal følge opp at kontotilbydere til enhver tid etterlever kravene stilt til grensesnitt for tredjepartstilbydere.
- Kontotilbyderes grensesnitt med tilhørende servicenivåer, minst like gode som grensesnitt mot deres kunder, **skal overvåkes og det stilles krav til stresstesting**.
- Krav til rapportering om problemer ved grensesnittene, både for kontotilbyder og tredjepartstilbydere
 - kan synes å gå noe ut over kravene til hendelsesrapportering.
- Unntaksregelverk for å tilby alternativt grensesnitt (les – samme som tilbys kontotilbyders kunder) dersom det er **etablert kontinuitetsløsninger** som tilfredsstiller forskriftens krav.

Forbedret grensekryssende samarbeid

- **Tilsyn & informasjon/statistisk informasjon**
- **Forbedret grensekryssende samarbeid**
 - Et kontaktpunkt hos tilsynsmyndighetene
 - Initiering av tilsyn og tilsynsdeltakelse
 - Varsling mistanke om overtredelse
 - Statistisk og aktivitetsrapportering
- **Mulighet for sentralt kontaktpunkt for agenter – (10 / omsetning 3 mill EUR / 100 000 transaksjoner)**

Retningslinjer – Hendelsesrapportering, artikkel 96

- Kravene i PSD 2 hovedsakelig i tråd med IKT-forskriftens bestemmelser.
- Retningslinjene gir utfyllende bestemmelser om krav til rapporteringen.
- Norge meddelt EBA etterlevelse av retningslinjene når PSD 2 trer i kraft i Norge.
- *Finanstilsynet vil legge disse til grunn for hendelsesrapportering generelt.*
- Krav til standardisert rapportering iht mal, ref bilag 1 til retningslinjene.
- Finanstilsynet har under utvikling tekniske løsninger.
- Relevant informasjon om hendelser knyttet til betalingstjenester skal meddeles EBA og ECB

Retningslinjer – Svindelrapportering, artikkel 96

- Kravene i PSD 2 hovedsakelig i tråd med dagens krav til svindelrapportering.
- Retningslinjene vil gi utfyllende bestemmelser om krav til rapporteringen. Disse synes mer omfattende en dagens norske rapporteringskrav.
- Det legges til grunn at Norge vil meddele EBA etterlevelse av retningslinjene når PSD 2 trer i kraft i Norge.
- Forslag til retningslinjer har vært på høring.
- Krav til svindelrapportering etter PSD 2 avstemt med ECB's krav til rapportering av betalingsstatistikk.
- I revidert forslag til svindelrapportering er det foreslått forenklinger.
- Det er også foreslått halvårlig rapportering (uten kvartalsvis oppdeling) og ikke kvartalsvis som tidligere.
- Finanstilsynet vil utarbeide skjema når retningslinjene er fastsatt.

Retningslinjer – Operasjonell og sikkerhetsmessig risiko

- **Proporsjonalitet** (bl.a. størrelse, virksomhet, tjenester)
- **Governance**
 - ✓ Rammeverk (systemer og kontrollmekanismer) for operasjonell og sikkerhetsmessig risiko.
 - ✓ Risikostyring og –kontroll. Utkontraktering.
- **Risikovurderinger**
 - ✓ Identifisering, klassifisering og risikovurdering av funksjoner, prosesser og aktiva.
- **Beskyttelse**
 - ✓ Data og system, integritet og konfidensialitet. Fysisk sikring. Tilgangskontroller.
- **Overvåking / Identifisering (deteksjon)**
 - ✓ Løpende overvåkning, oppdaging og identifisering
 - ✓ Overvåkning og rapportering av operasjonelle eller sikkerhetsmessige hendelser
- **Forretningsmessig kontinuitet**
 - ✓ Scenariobasert forretningsmessig kontinuitetsplanlegging, Testing av forretningsmessig kontinuitetsplan, Kommunikasjon ved kriser
- **Testing av sikkerhetstiltak**
- **Situasjonsforståelse/-bevissthet og kontinuerlig læring**
 - ✓ Trussellandskapet og situasjonsforståelse. Opplærings- og sikkerhetsfortståelseprogrammer.
- **Opplæring og informasjon ovenfor betalingstjenestebrukerne**
 - ✓ Betalingstjenestebrukernes bevissthet om sikkerhetsrisiko og risikoreduserende tiltak

Vellykket implementering av PSD 2

- Konsesjonsbehandling iht fastsatt regelverk (mer omfattende enn for PSD 1)
- God kommunikasjon med næringen, både eksisterende aktører og nye aktører når det gjelder
 - ✓ Informasjon om regelverket, konsesjonskravene og konsesjonsprosessen
 - ✓ Forståelse av regelverket
 - ✓ Oppmuntre til å tilpasse seg fastsatt regelverk (jo før jo bedre), selv om det ennå ikke har trådt i kraft (særlig RST SCA & CSC), ref EBA Opinion
 - ✓ Forventet etterlevelse av regelverket
- Sikre at fastsatt regelverk etterleves både ifm
 - ✓ Konsesjonsgivingen
 - ✓ Løpende oppfølging av foretakene
 - ✓ Tilsyn
 - ✓ Mao – sikre at kontotilbydere ivaretar sine forpliktelser og at aktører som vil tilby de nye betalingstjenestene basert på rett til tilgang til betalingskonto ivaretar sine forpliktelser
- Ivareta forpliktelsene som følger av regelverket
- Sikre best mulige rapporteringsløsninger for påkrevd rapportering
- Samhandle med medlemslandene i EU, særlig de nordiske og bidra til et forbedret grensekryssende samarbeid
- Bidra til regulatorisk harmonisering (regulatory convergence) innenfor EU/EØS



FINANSTILSYNET

English

Søk

Konsesjon



Finansiell teknologi (FinTech)



Tilsyn



Forbrukerinformasjon



Rapportering



Hvitvasking



Regelverk



Publikasjoner og analyser



Nyhetsarkiv



Konsesjonsregisteret



Markedsadvarsler



Shortsalgregisteret (SSR)



Prospekter



FINANSTILSYNET

Revierstredet 3

Postboks 1187 Sentrum

0107 Oslo

www.finanstilsynet.no



Takk for oppmerksomheten!

Olav Johannessen, Seksjonssjef seksjon for tilsyn med IT og betalingstjenester

E-post: ola@finanstilsynet.no