FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Vedlegg 1

NOTAT

29. august 2025

Finanstilsynets og Datatilsynets regulatoriske sandkasser – 2025

Innledning

I regulatoriske sandkasser får virksomheter mulighet til å teste nye produkter og teknologier under etatenes oppfølging. Formålet er blant annet å bidra til økt teknologisk innovasjon, gi virksomheter økt kunnskap om regelverket og gi myndighetene bedre forståelse av nye teknologiske løsninger.

I november 2024 gikk Datatilsynet og Finanstilsynet sammen om å invitere banker til å delta med prosjekter som utforsker mulighetene for datadeling med formål å bekjempe økonomisk kriminalitet. Dette resulterte i fem søknader, og i februar 2025 ble det besluttet å ta inn alle søkerne i etatenes regulatoriske sandkasser:

- DNB sammen med Norsk Regnesentral, Sparebank 1, Nordea og Eika: Prosjekt om informasjonsdeling for å forhindre betalingsbedragerier.
- BankID BankAxept (nå Stø AS): Prosjekt om utvidet innsamling av data for bekjempelse av svindel, særlig problemstillinger rundt utvidet innsamling og behandling av data fra brukerstedene.
- BN Bank og Norges miljø- og biovitenskapelige universitet (NMBU): Bedre utnyttelse av informasjonen som samles inn og rapporteres av banker til enheten for finansiell etterretning (FIU) i Økokrim.
- Finans Norge Forsikringsdrift: Etablering av tipskanal for å redusere forsikringssvindel.
- Eika/KPMG: Felles transaksjonsovervåkning for å hindre hvitvasking, og vurdere mulighetsrommet for mer sentralisering av antihvitvaskingsarbeidet til bankene i Eika-gruppen.

Arbeidet med prosjektene i sandkassen startet opp i slutten av mars 2025 og følges opp av Datatilsynet og Finanstilsynet i fellesskap. I henhold til framdriftsplan skal prosjektene ferdigstilles i løpet av høsten 2025. Prosjektene vil hver for seg utarbeide en sluttrapport som oppsummerer arbeidet og eventuelle avklaringer. Rapportene vil publiseres slik at også resten av næringen kan dra nytte av arbeidet.

Tre av prosjektene har som formål å utforske mulighetene for informasjonsdeling for å styrke arbeidet med å forebygge og avdekke bedrageri. Hovedspørsmålene som vurderes, er rekkevidden av taushetspliktregelen i finansforetaksloven, og deling av data etter personvernreguleringen. En nærmere beskrivelse av disse prosjektene følger nedenfor og baserer seg på opplysninger gitt i søknadene, prosjektplaner og informasjon som så langt har blitt presentert i arbeidsmøtene. Finanstilsynets foreløpige beskrivelse av eventuelle regulatoriske hindringer er begrenset til finansforetaksloven.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Anne-Kari Tuv
Dir. tlf. 22 93 98 04

DNB, Sparebank 1, Nordea, Eika og Norsk Regnesentral – informasjonsdeling med formål å bekjempe bedrageri

Generelt

Prosjektet gjennomføres i et samarbeid mellom DNB Bank, Sparebank 1 Utvikling, Eika-gruppen samt den norske filialen til Nordea. I tillegg deltar Norsk Regnesentral, som bidrar med kompetanse på analyse og modellering av dataene som deles. Hensikten med å ta prosjektet inn i sandkassen er å tydeliggjøre rammene for data- og informasjonsdeling med sikte på systematisk operasjonalisering, for å legge til rette for mer utstrakt deling i finansnæringen, med en målsetting om å redusere omfanget og konsekvensene av betalingsbedragerier.

Data som vurderes å ha stor betydning i antisvindelarbeid, er blant annet informasjon som kan identifisere svindeloffer, kriminelle, såkalte muldyr mv. Prosjektet skal kartlegge hvilke data som kan deles, i hvilke situasjoner og mellom hvilke aktører, innenfor rammen av gjeldende regelverk, særlig finansforetaksloven og personvernregelverket. Det skal også vurdere behovet for eventuelle regelverksendringer som muliggjør mer effektiv informasjonsdeling.

Nærmere om informasjonsdelingen

Bankene sitter på informasjon om egne kunder, deres adferd og transaksjoner. Disse dataene brukes i interne antisvindelsystemer og prosesser. Mer deling av data mellom banker og andre offentlige og private aktører, som eksempelvis politi og tilbydere av elektroniske kommunikasjonstjenester (ekomtilbydere), vil skape muligheter til å forhindre flere betalingsbedragerier gjennom at datasettet som benyttes i antisvindelsystemer blir vesentlig beriket. Dette vil ikke bare ha effekt for bankens egne kunder, men også for kunder i andre banker og for kunder som har kundeforhold i flere banker.

Prosjektet ser på alternative måter å dele dataene på, herunder deling gjennom en sentralisert løsning, der bankene vil kunne dele informasjonen via API-er. Automatisk og umiddelbar deling vil effektivisere bankenes arbeid med å bekjempe betalingsbedragerier.

Regulatoriske rammer

Taushetsplikten i finansforetaksloven oppleves ofte som et hinder mot å dele. Avsløringsforbudet i hvitvaskingsloven fører til usikkerhet rundt hva og med hvem informasjonen kan deles. I tillegg fungerer personvernet som en barriere og gjør bankene nølende til å delta i samarbeidet.

Når det gjelder taushetsplikten, er det gjennom arbeidet i sandkassen så langt lagt til grunn at finansforetaksloven § 13-21 dekker de fleste relevante aktiviteter knyttet til bankenes antisvindelarbeid[1] og åpner for deling av de definerte datapunktene mellom banker innenfor rammene av nødvendighetskravet. I tillegg åpner finansforetaksloven § 16-2 første ledd for at banker som er utsatt for straffbar handling, kan dele taushetsbelagte opplysninger med politiet, for eksempel gjennom en anmeldelse av forholdet. Dette vil f.eks. kunne være opplysninger om en person som opptrer som "muldyr". Men regelverket åpner ikke for en generell deling av slike opplysninger, og heller ikke om personer som banken gjennom sine antisvindelsystemer ser at

[1] Det er definert enkelte datapunkter som kan være i ytterkant av hva som anses som naturlig språklig forståelse av "annen betalingsinformasjon" i finansforetaksloven § 13-21. Dette knytter seg til opplysninger modus, bankenes egne kategoriseringer, dato for opprettelse av konto- og kundeforhold og etterretningsinformasjon. Forarbeidene og PSD2 artikkel 94 taler for at dette likevel ligger innenfor rammene av bestemmelsen.

opptrer i nettverk av kriminelle som utfører bedragerier. Det er heller ikke i dag adgang for å dele taushetsbelagte opplysninger med ekomtilbydere.

Det er ellers lagt til grunn at delingen skjer for å forebygge, etterforske eller avsløre selve bedrageriet, som er primærforbrytelsen. Det må derfor antas at delingen normalt kan skje uten at den berøres av avsløringsforbudet i hvitvaskingsloven § 28.

Stø AS – Antisvindel 2.0

Generelt

Stø AS utvikler, driver og forvalter BankID på vegne av utstedere med grunnlag i avtale og i henhold til lov om elektroniske tillitstjenester. BankID er i dag den mest brukte elektroniske autentiserings- og signeringsløsningen i Norge. Tjenesten brukes for innlogging og autentisering på offentlige og private brukerstedet (ID-porten, nettbanker og kommersielle tjenestetilbydere) samt for å signere avtaler og andre rettsdisposisjoner digitalt.[2] *Utstedere* av BankID er i dag banker og bankgrupperinger, samtidig som banker og andre finansforetak også er *brukersteder* av BankID.[3]

Rammebetingelsene for elektronisk ID er i endring, blant annet gjennom rask teknologisk utvikling, revidert eIDAS-regelverk fra EU og nasjonal eID-strategi. For å møte framtidige forventninger og krav, er det behov for å forenkle og modernisere BankIDs verdikjede. For å bidra til dette er banknæringen og styret i Stø AS i gang med å samle all formell utstedelse hos Stø AS. Planlagt overgang vil skje i løpet av 2026.

BankID antisvindel er en del av BankID-tjenesten, og er nødvendig for å sikre et tilstrekkelig sikkerhetsnivå i tjenesten. BankID Antisvindel 2.0 er en oppgradering av tidligere antisvindelsystem og forutsetter utvidet innsamling av data, dvs. mer informasjon fra blant annet finansforetak og brukersteder enn tidligere, både for å gi et samlet bilde av sluttbrukers atferd, men også for å vise kontekstinformasjon og for å vise brukshistorikk.

Funksjonaliteten i løsningen vil kunne kategorisere hva slags type transaksjon som er i ferd med å initieres og se svindelmønstre på tvers av alle brukerstedene, for eksempel betalinger fra sluttbrukers konto til kjente svindlerkontoer. Mens dagens løsning kun prosesserer logger som er frambrakt *etter* at BankID-transaksjonen er fullført, vil den nye løsningen kunne bidra til å stanse svindelforsøk *før* transaksjonen er fullført av sluttbruker. Dette vil gjøre det mulig å håndtere en pågående svindeltransaksjon, og sette brukerstedet i stand til å iverksette tiltak.

I sandkassen er målet for Stø AS å dokumentere rettslige vurderingstemaer for å kartlegge muligheten for å avtaleregulere forpliktelser for BankID-brukersteder (banker, finansforetak og brukersteder utenfor finanssektoren) om å sende inn mer data til BankID Antisvindel 2.0. Ett av vurderingstemaene er å vurdere mulighetsrommet for innsamling og utlevering av datapunkter fra finansforetak, telekom og andre typer BankID-brukersteder – innenfor rammene av lovbestemt taushetsplikt.

[2] Reguleres av lov 15. juni 2018 nr. 44 om elektroniske tillitstjenester og forskrifter, som blant annet gjennomfører EUs forordning (910/2014) om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.

[3] Regler om BankID

Nærmere om informasjonsdelingen

Transaksjonsflyten begynner i det øyeblikket en sluttbruker som er på et brukersted initierer en BankID-sesjon. BankID-klienten vil samle inn informasjon (datapunkter) fra sluttbrukers enheter (PC, og mobil hvis BankID-app er benyttet) og fra brukersted.

Eksempler på datapunkter er IP-adresse, operativsystem, hva BankID brukes til, kontekstinformasjon og lignende. Datapunktene som samles brukes til å sammenligne sluttbrukers adferd med historisk bruk, og for å se etter uvanlig aktivitet. Hva som er uvanlig aktivitet, avhenger av sluttbrukers historiske bruk.

I det tilfelle systemet avdekker mistenkelig adferd og høy sannsynlighet for svindel, vil det trigge en alarm som sendes til utstederen av BankID og til brukerstedet der sluttbruker/svindler forsøker å bruke BankID. Ved en sendt alarm vil brukerstedet og/eller utsteder gi en tilbakemelding på om det var svindel eller ikke, til et endepunkt hos Stø. Dette vil brukes til videre analyse for å fjerne falske positive, og generelt øke kvaliteten på tjenesten.

Regulatoriske rammer

I prosjektet er det lagt til grunn at det er lang og fast praksis for at finansforetak kan dele taushetsbelagte opplysninger med sine tredjepartsleverandører av IKT-tjenester. Forutsetningen er at IKT-tjenesteleverandøren har saklig begrunnet behov for kundeopplysningene med formål å gjennomføre den avtalebaserte tjenesten. Ved mottak av taushetsbelagte opplysninger blir IKT-tjenesteleverandøren omfattet av finansforetakets taushetsplikt.

For å kunne motta nødvendige opplysninger (valgte datapunkter) fra finansforetak uhindret av taushetsplikten, vil Stø AS, som tilbyder av BankID og antisvindel 2.0, måtte videreføre rollen som IKT-tjenesteleverandør.

Etter dagens utstedermodell vil utstederbanken måtte vurdere om BankID-en skal sperres når det genereres en alarm basert på data fra et brukersted. I den grad utstederbanken for dette formålet mottar opplysninger som nærmere beskriver årsaken til alarmen, vil dette omfattes av taushetsplikten i finansforetaksloven § 16-2 første ledd.

Mottaker av kundeopplysningene vil teknisk sett være Stø AS (i egenskap av å være IKT-tjenesteleverandør for utstederbanken) og vil motta opplysninger i medhold av finansforetaksloven § 9-6 første ledd. Det foreligger imidlertid ikke samme tjenesteavtaleforhold mellom Stø AS og brukerstedet. Et spørsmål blir da om hva som gjelder for adgangen til å utlevere opplysninger fra brukerstedet (banken der id-en benyttes til for eksempel en pengeoverføring eller låneopptak) og til utstederbanken.

Basert på blant annet forpliktelsen utstederbanken har til å beskytte sluttbrukeren mot at id-en misbrukes, kan det argumenteres for at utstederbanken har et saklig behov for å motta kundeopplysninger fra brukerstedet der det genereres en alarm. Utstederbanken vil dermed etter en konkret tolkning kunne anses som "vedkommende" etter finansforetaksloven § 16-2 første ledd for de kundeopplysningene brukerstedet utleverer. Dette er imidlertid ikke nødvendigvis et tilfredsstillende og hensiktsmessig rettsgrunnlag for generell og løpende utveksling av taushetsbelagte kundeopplysninger gjennom et IKT-basert antisvindelsystem.

Utlevering av kundeopplysninger fra brukerstedet til utstederbanken kan også etter omstendighetene falle inn under utleveringsadgangen (unntakene fra taushetsplikten) i §§ 16-2 tredje ledd og 13-21, men disse unntakene har ulike praktiske og rettslige begrensninger som i flere situasjoner ikke vil gi tilstrekkelig hjemmel for utlevering av kundeopplysninger mellom finansforetak.

Endringen av utstedermodellen som Stø AS har planlagt å gjennomføre i 2026, vil innebære at banker ikke lenger vil være utstedere av BankID. Dette vil medføre at behovet for å dele opplysninger mellom banker faller bort, fordi kommunikasjonen om mulig id-misbruk bare vil gå mellom et brukersted (for eksempel en bank) og Stø AS som utsteder. I den grad det skulle bli behov for å utveksle taushetsbelagte opplysninger som BankID har mottatt fra en bank, med for eksempel offentlige myndigheter eller ekomtilbydere, må det etableres hjemmel for dette i finansforetaksloven.

Finans Norge Forsikringsdrift – tipskanal

Generelt

Finans Norge Forsikringsdrift (FNF) er en medlemsorganisasjon for forsikringsbransjen som utvikler og forvalter digitale fellesløsninger, tjenester og retningslinjer for bransjen. FNF har styre sammensatt av representanter fra forsikringsforetak i Norge. FNF driver blant annet forsikringsbransjens fellesregistere for svindelbekjempelse, FOSS og ROFF.

Hovedmålet for sandkasseprosjektet er å etablere en digital tipskanal som sikrer at informasjon fra publikum og offentlige myndigheter knyttet til å avdekke og bekjempe forsikringssvindel, kommer fram til forsikringsforetakene. Videre at det legges til rette for samarbeid mellom forsikringsforetakene om saker som gjelder organisert kriminalitet og involverer flere forsikringsforetak. Videre begrunner FNF prosjektet slik:

> *Siden det i dag er mangel av en slik kanal er det tilfeldig hvem som mottar tips om mulig forsikringssvindel. Personer som ønsker å tipse om et forhold har sjelden informasjon om hvilket foretak som er forsikringsgiver, og tipsene sendes derfor til feil foretak eller til tilfeldige ansatte i FNF. Det kan heller ikke utelukkes at manglende informasjon om hvem som er rette vedkommende medfører at man i stedet unnlater å tipse om aktuelle forhold. I tillegg er det et problem at tipsene ikke inneholder tilstrekkelig informasjon til at foretakene kan nyttiggjøre seg av dem, samtidig som de kan inneholde informasjon som ikke er relevant. Dersom FNF kan via en sikker kanal motta og verifisere tipsene og videreformidle til korrekt foretak, vil det opprettes bedre kontroll. Både FNF og foretakene vil kunne ta kontroll på behandlingen, og påse at denne skjer i samsvar med vilkårene i personvernregelverket.*

En lignende type tipskanal finnes i dag i Sverige[4], som drives av Larmtjänst AB. Tipskanalen mottar rundt 400 tips i året.

Nærmere om informasjonsdelingen

Tipskanalen skal ta imot og lagre tips om mulig forsikringssvindel fra publikum (enhver), forsikringsforetak og politiet. I tillegg vurderes det i en eventuell neste fase å inkludere tips fra

[4] Larmtjenst AB, et datterselskap til Svensk Försäkrings Service AB og en del av bransjeorganisasjonen Svensk Försäkring

andre offentlige myndigheter som NAV, Helfo, Skatteetaten og Arbeidstilsynet. Informasjonsflyten vil være lik for de tre kategoriene tips.

Tips er tenkt mottatt gjennom en webløsning med skjema med definerte felter som tipser kan fyller ut. Dette vil være opplysninger om navn, adresse og eventuelt registreringsnummer på kjøretøy eller matrikkelinformasjon for eiendom, samt et eventuelt fritekstfelt for eventuelle helseopplysninger eller andre opplysninger av sensitiv karakter. Tipser skal ha mulighet til å være anonym.

Tipskanalen skal:

- undersøke informasjonen i tipset mot åpne kilder med formål å finne ut hvilket forsikringsforetak tipset berører,
- fjerne informasjon som ikke er nødvendig for videre håndtering,
- tilgjengeliggjøre tipset for aktuelle forsikringsforetak (fortrinnsvis innen 24 timer). Dette skjer ved en notifikasjon på e-post til dedikert person hos forsikringsforetaket, som basert på intern tilgangsstyring må logge seg på portalen for å lese tipset,
- dersom tipset omhandler forsikringsforetakets kunde, kan det velge å ta inn tipset og dermed ansvaret for personopplysningene. Foretaket kan benytte tipset videre i sin interne utredning,
- når tipset blir kanalisert til forsikringsforetaket, slettes det fra portalen. Tipset slettes uansett etter 30 dager.

Regulatoriske rammer

Utover de regulatoriske kravene i personvernlovgivningen, er problemstillingene knyttet til taushetsplikten i finansforetaksloven om det enkelte forsikringsforetaket kan formidle tips, og dermed opplysninger om sine eventuelle kunder til FNF eller et annet forsikringsforetak. Videre om FNF kan formidle kundeopplysninger i forbindelse med tips mottatt fra et forsikringsforetak eller fra en privat aktør til det aktuelle forsikringsforetaket og til offentlig forvaltningsorgan som politiet eller NAV.

Utgangspunktet er at FNF som driver av tipskanalen ikke er et finansforetak og ikke omfattes av finansforetakslovens taushetsplikt med mindre FNF utfører oppdrag på vegne av et finansforetak.

Når informasjonen til tipskanalen kommer fra allmenheten, eller eventuelt fra offentlige myndigheter, gjelder bare taushetsplikten i finansforetaksloven for forsikringsforetaket som senere mottar tipset. Men det er som nevnt en målsetting for prosjektet at forsikringsforetakene også skal kunne utlevere opplysninger om mulig forsikringssvindel til tipskanelen. Dette vil bare være aktuelt når tipset foretaket mottar, ikke gjelder en av deres egne kunder, og foretaket behøver bistand til å finne ut hvor den det tipses om er forsikret.

Det legges foreløpig til grunn at FNF, som driver av tipskanalen, vanskelig kan anses å utføre oppdrag for et finansforetak i relasjon til finansforetaksloven § 9-6. Finansforetaksloven § 16-2 første ledd vil dermed være til hinder for at et forsikringsforetak kan utlevere taushetsbelagte opplysninger til tipskanalen.