Datadeling for å bekjempe bedrageri

Sluttrapport fra sandkasseprosjekt

Av DNB, Nordea, SpareBank 1, Eika Gruppen og Norsk Regnesentral

Januar 2026

Innhold

1. Innledning

1.1 Bakgrunn og mål med regulatoriske sandkasse

Høsten 2024 inviterte Finanstilsynet og Datatilsynet finansforetak til å søke om å delta med prosjekter som utforsker muligheter for datadeling. Sandkasseprosjektet omtalt i denne sluttrapporten gjelder mulighetsrommet for deling av data mellom tilbydere av betalingstjenester for å forebygge, etterforske eller avdekke betalingsbedragerier. Diskusjonen har særlig angått rekkevidden av finansforetaksloven § 13-21, og personvernregelverket. Etter å ha identifisert eksisterende handlingsrom, har prosjektet også hatt som mål å identifisere og diskutere behov for regelverksendringer.

Denne sluttrapporten – utarbeidet av DNB, Nordea, SpareBank 1, Eika Gruppen, og Norsk Regnesentral – oppsummerer de vurderingene som er gjort i prosjektet. Vurderingene bygger på veiledning fra Datatilsynet og Finanstilsynet gjennom det regulatoriske sandkassearbeidet.

1.2 Samarbeid om bekjempelse av bedrageri

Bedrageri er et stort og økende samfunnsproblem som fører til økonomisk tap for privatpersoner, bedrifter, staten og finansinstitusjoner. Finanstilsynets siste ROS-rapport[1] publisert i mai 2025 viser at tapene relatert til bedrageri fortsetter å øke. Fra 2023 til 2024 økte tapene med 299 millioner norske kroner, noe som tilsvarer en økning på 32 %. Bedrageri truer den høyt verdsatte tilliten vi har i Norge, ved at svindlere utgir seg for å være banker, offentlige etater og andre velkjente aktører. Å bekjempe bedrageri krever utstrakt samarbeid i alle samfunnsledd, også mellom private og offentlige aktører.

Det pågår initiativ både på nasjonalt nivå og næringsnivå i regi av Finans Norge[2] for å bekjempe bedrageri. For finansnæringen ble Fagutvalg Antisvindel Bank etablert i 2023 i regi av Finans Norge som følge av prosjektet «Trygge forbrukere» der en rekke tiltak for å snu svindeltrenden ble foreslått. Fagutvalget jobber aktivt med å følge opp ulike tiltak, men også foreslå nye tiltak basert på det nåværende trusselbildet. Videre har Nordisk Finans Cert (NFCERT) lenge vært bankenes samlingspunkt for å dele informasjon om svindelmodus og trender, samt begrensede data mellom medlemsbanker på nasjonalt og nordisk nivå.

Finansforetak har en nøkkelrolle i å beskytte både kunder og samfunnet mot bedrageri. For å møte et stadig mer sofistikert trusselbilde benytter foretakene avanserte teknologiske systemer for å identifisere, forebygge og avverge bedrageri. Den tekniske tilnærmingen er kompleks og kombinerer regelbaserte mekanismer med algoritmedrevne deteksjonssystemer. Systemene monitorerer og analyserer aktivitet på tvers av digitale kanaler. Dette gjør det mulig å oppdage uvanlige handlingsmønstre, risikable betalinger og forsøk på uautorisert tilgang.

---

[1] Finanstilsynet, Risiko- og sårbarhetsanalyse (ROS) 2025, https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/risiko--og-sarbarhetsanalyse-2025/ros-2025/risiko--og-sarbarhetsanalyse-ros-2025/#6-svindel

[2] Finans Norge, Økonomisk kriminalitet – Svindel https://www.finansnorge.no/tema/okonomisk-kriminalitet/svindel/

Monitoreringen skjer i sanntid og dekker et bredt spekter av aktiviteter. Systemene vurderer disse aktivitetene, og når mistenkelig eller avvikende atferd oppdages, kan bankenes antisvindelsystemer iverksette tiltak for å beskytte kunden. Dette kan eksempelvis innebære å stanse betalinger. Denne responsen balanserer effektiv svindelbekjempelse med behovet for en god brukeropplevelse for legitime kunder.

For å oppnå effektiv svindelbekjempelse er nøkkelen å ha situasjonsforståelse av dagens trusselbilde. Dette er krevende med kriminelle som kontinuerlig tilpasser seg og leter etter nye sårbarheter. For å oppnå bedre situasjonsforståelse, kreves samarbeid og deling mellom bankene. Deling av informasjon gjøres allerede blant kriminelle, som samarbeider og bytter tjenester seg imellom i et åpent marked, uten å ta hensyn til reguleringer. Finansforetakene derimot arbeider i siloer med svært begrenset deling av informasjon. Dette gir de kriminelle et forsprang sett opp mot finansforetakene som må forholde seg til et omfattende regulatorisk rammeverk.

2. Organisering

2.1 Deltakere

Følgende aktører har deltatt i prosjektet om informasjonsdeling for å forhindre betalingsbedragerier:

- DNB
- SpareBank 1
- Nordea
- Eika
- Norsk Regnesentral

Prosjektgruppen har bestått av representanter fra de overnevnte aktørene, som har fått veiledning og råd av Datatilsynet og Finanstilsynet. I tillegg har prosjektgruppen hatt dialog med Finans Norge, BITS og NFCERT, særlig med hensyn til operasjonalisering av datadelingen.

2.2 Arbeidsmetodikk

Prosjektgruppen har diskutert problemstillinger knyttet til datadeling gjennom en strukturert dialog med tilsynsmyndighetene. Prosjektgruppen har tatt utgangspunkt i faktiske og konkrete situasjoner (scenarioer) der foretak som yter betalingstjenester (heretter omtalt som «foretakene» eller «foretak») sin vurdering er at datadeling kan bidra til mer effektiv bekjempelse av bedragerier. Basert på disse scenariene har prosjektgruppen gjennomført en kvalitativ vurdering og prioritering av hvilke tiltak som antas å ha størst effekt på bekjempelse av betalingsbedrageri.

Det har blitt gjennomført seks arbeidsmøter med tilsynsmyndighetene over en periode på åtte måneder, fra april til november 2025. I disse arbeidsmøtene har blant annet følgende blitt diskutert:

- De identifiserte scenariene for datadeling
- Hvilke data som er relevante å dele
- Deling mellom foretakene, politi og telekom

- Måter å operasjonalisere datadeling på
- Juridiske rammer for datadeling, både mulighetsrommet i eksisterende regelverk og behovet for regelverksendringer.

Diskusjonene har bidratt til en felles forståelse av muligheter og begrensninger knyttet til datadeling for bedrageribekjempelse, og prosjektgruppen har utformet sine juridiske vurderinger i samråd med tilsynsmyndighetene.

3. Alternative utvekslingsmetoder

I sandkassen har prosjektgruppen diskutert med Datatilsynet og Finanstilsynet hvordan delingen kan gjennomføres. Det har ikke vært anledning til å gå i detalj når det gjelder oppsett eller tekniske løsninger, men prosjektgruppen og tilsynene har på et overordnet nivå diskutert følgende alternativer:

Alternativ 1: Bilateral deling
Foretakene deler informasjon direkte med hverandre, enten én-til-én eller én-til-flere. Dette alternativet kan raskt etableres og gir mulighet for økt datadeling på kort sikt, men er ressurskrevende og lite effektivt i større skala. En utfordring er at det utleverende foretaket ofte ikke har oversikt over hvilke andre foretak som bør motta informasjonen, noe som kan føre til at andre ikke blir varslet i tide, eller alternativt at dataen må deles med flere, for å sikre at alle relevante foretak får informasjonen.

Alternativ 2: Deling via sentral «hub»-løsning
Foretakene deler relevante data via en sentralisert «hub», som fungerer som et bindeledd og sørger for at dataene distribueres videre til de foretakene som har lovlig behov for dataen. Dette muliggjør en mer automatisert og strukturert datadeling, hvor informasjonen lettere kan integreres i foretakenes egne antisvindelsystemer. I tillegg kan data lagres i «hub-en», slik at de også er tilgjengelige for andre foretak på et senere tidspunkt, dersom det blir relevant og nødvendig. Denne sentraliserte tilnærmingen gir dermed både økt effektivitet og bedre treffsikkerhet i delingen av informasjon mellom foretak.

4. Finansregulatoriske rammer for deling

4.1 Deling mellom foretak som yter betalingstjenester

Foretakene har taushetsplikt om kunders og andres forhold som de blir kjent med under utøvelsen av sin virksomhet, jf. finansforetaksloven § 16-2 første ledd og § 9-6. Det sentrale formålet er å beskytte kundene, å forhindre at kundeopplysninger misbrukes, og ivareta det overordnede hensynet til allmennhetens tillit til det enkelte finansforetaket og finansmarkedet som helhet.

Etter finansforetaksloven § 16-2 (3) bokstav a følger det at taushetsplikten ikke er til hinder for at et finansforetak "i særlige tilfelle" gir et annet finansforetak opplysninger som foretaket har mottatt under utøvelsen av virksomheten dersom "formålet er å avdekke eller motvirke økonomisk kriminalitet eller annen alvorlig kriminalitet". Det følger av § 16-2 (3) siste punktum at utlevering av opplysninger etter § 16 (3) bokstav a, bare kan skje i henhold til styrevedtak. Det fremgår av forarbeidene at

bestemmelsen ikke krever at hver enkeltstående utlevering av informasjon må være behandlet i styret, men styret må fastsette retningslinjer som et minimum må ta stilling til forskjellige typetilfeller. Det er presisert at det ikke er adgang for styret til å fastsette retningslinjer som gir en helt generell adgang til rutinemessig utveksling av opplysninger mellom finansforetak. I praksis har kravet om styrevedtak gjort bestemmelsen vanskelig å anvende. Videre begrenser vilkåret om "særlige tilfelle" bestemmelsens praktiske rekkevidde.

På denne bakgrunn har prosjektgruppen fokusert på hvilke muligheter finansforetaksloven § 13-21 gir. Denne bestemmelsen gir unntak fra taushetsplikten, og hjemmel for at foretakene kan samle inn, bearbeide og utveksle transaksjonsopplysninger og annen betalingsinformasjon, når dette er nødvendig for å forebygge, etterforske eller avsløre betalingsbedrageri:

> *«§ 13-21 Adgang til behandling og utveksling av betalingsinformasjon*
>
> *(1) Foretak som yter betalingstjenester, kan samle inn, bearbeide og utveksle seg imellom transaksjonsopplysninger og annen betalingsinformasjon når dette er nødvendig for å sikre forebygging, etterforskning eller avsløring av betalingsbedragerier.* […]»

Bestemmelsens annet ledd gir forskriftshjemmel for å fastsette nærmere regler om informasjonsbehandlingen.

Sentrale diskusjoner av bestemmelsen oppsummeres i det følgende:

- Begrensning til betalingsbedragerier: Bestemmelsen gjelder «betalingsbedragerier», ikke andre former for bedragerier eller annen kriminalitet. Begrepet er ikke legaldefinert og har et vidt nedslagsfelt. På bakgrunn av veiledning fra Finanstilsynet kom prosjektgruppen til at betalingsbedragerier omfatter både svindelbetalinger hvor den kriminelle skaffer seg kontroll over hele eller deler av betalingsinstrumentet og autorisasjonshandlingen, og bedragerier der kunden forledes til selv å gjennomføre betalingen. Dette innebærer at for eksempel kjærlighetssvindel, investeringssvindel og andre svindelbetalinger under sosial manipulasjon anses som betalingsbedragerier.

- Hvem kan behandle: Regelen gjelder behandling i og mellom banker og andre foretak som yter betalingstjenester (f.eks. Vipps). Bestemmelsen angir ingen personelle krav til hvem som kan dele informasjonen, og heller ingen krav til styrevedtak eller lignende, sml. finansforetakslovens § 16-2 (3).

- Type informasjon: Finansforetaksloven § 13-21 gjelder behandling av «transaksjonsopplysninger og annen betalingsinformasjon», som ikke er definert uttrykkelig i loven. Ordlyden favner vidt, og eksempler (ikke uttømmende) nevnt i lovkommentaren er opplysninger om betaler, betalingsmottaker, kontonummer, transaksjonsbeløp og IP-adresser. På bakgrunn av veiledning fra Finanstilsynet har prosjektgruppen kommet til at ordlyden i § 13-21 er utformet slik at enhver opplysning som er relevant for gjennomføringen av betalinger og transaksjoner, kan anses som «annen betalingsinformasjon». Etter prosjektgruppens oppfatning får denne

avgrensningen derfor begrenset betydning i praksis.

En av flere diskusjoner i sandkassen har vært om modus og foretakenes egen tilhørende kategorisering/vurdering av situasjonen, kan deles i henhold til finansforetaksloven § 13-21. Etter prosjektgruppens oppfatning var det ikke umiddelbart opplagt at slik informasjon vil falle innenfor ordlyden "transaksjonsopplysninger og annen betalingsinformasjon". På bakgrunn av veiledning fra tilsynene har prosjektgruppen konkludert med at gode grunner tilsier at disse typer opplysninger likevel kan anses omfattet. Årsaken er dels at PSD2 artikkel 94 ikke inneholder tilsvarende begrensninger, formålsbetraktninger som også fremkommer av lovforarbeidene, og at det i praksis bør være om dette er opplysninger som er nødvendige for å oppnå formålet bak bestemmelsen, som utgjør begrensningene.

- Behandlingsaktiviteter: Bestemmelsen angir et konkret område for selve håndteringen av opplysningene («samle inn, bearbeide og utveksle seg imellom»). Lest i sammenheng med PSD2 artikkel 94 (1) om «behandling» av opplysninger, må det anlegges en vid tolkning av hvilke behandlingsaktiviteter som omfattes, og avgrensningen vil derfor være lite relevant.

- Formålsbegrensning: Behandlingen av den relevante informasjonen er kun tillatt «når dette er nødvendig for å sikre forebygging, etterforskning eller avsløring av betalingsbedragerier».

- Taushetsplikten og personopplysningsloven: Finansforetaksloven § 13-21 innebærer en uttrykkelig adgang til å utveksle opplysninger. Ved utveksling i samsvar med bestemmelsen foreligger det ikke taushetsplikt etter § 16-2 første ledd. Personopplysningsloven og EUs personvernforordning (GDPR) gjelder for behandlingen av personopplysninger med hjemmel i § 13-21.

- Sentralisert løsning: Det har vært diskutert om det er adgang til å benytte en sentralisert løsning (omtalt som Alternativ 2 i punkt 3 ovenfor). På bakgrunn av veiledning fra Finanstilsynet, er det enighet i prosjektgruppen om at det ikke er det finansregulatoriske regelverket som setter eventuelle begrensninger i å operasjonalisere delingen gjennom en slikt sentralisert «hub» – ettersom finansforetaksloven § 16-2 andre ledd, jf. § 9-6 åpner for utlevering av taushetsbelagte opplysninger til "enhver som utfører oppdrag for et finansforetak". Foretakene er innforstått med at leverandøren av den sentraliserte løsningen også vil måtte overholde andre relevante regulatoriske krav, herunder reglene i DORA. Lovligheten av Alternativ 2 vil i hovedsak bero på vurderinger etter GDPR, og omtales nærmere i punkt 5.7.

Oppsummert er prosjektgruppens vurdering, utarbeidet i samråd med tilsynsmyndighetene, at finansforetaksloven § 13-21 gir et betydelig handlingsrom for foretakene til å kunne dele opplysninger seg imellom for å bekjempe og forebygge betalingsbedragerier.

Det finnes likevel klare begrensninger i bestemmelsen som påvirker hva som kan deles, for hvilke formål og med hvilke aktører, jf. ovenfor. Prosjektgruppen har på denne bakgrunn identifisert og diskutert behov for regelverksutvikling med

Finanstilsynet. Blant annet som følge av disse diskusjonene i prosjektet, har Finansdepartementet sendt på høring forslag om endringer i finansforetaksloven. Den utvidede delingsadgangen i høringsforslaget vil bidra til å gi betraktelig bedre rammevilkår for deling av data for å motvirke betalingsbedragerier og annen økonomiske kriminalitet.

4.2 Deling med andre aktører

Deling fra foretak til politi
I dagens regelverk er det begrenset adgang til å dele informasjon fra foretakene til politi, slik dette er redegjort for i brev av 6. september 2024 fra DNB til Justis- og beredskapsdepartementet, Finanstilsynet og Finansdepartementet.

Det er først og fremst i forbindelse med utleveringspålegg fra påtalemyndigheten eller ved foretakenes anmeldelse av et forhold, at foretakene kan dele opplysninger uten å være begrenset av taushetsplikten. Dette står i ubalanse i forhold til informasjonsretten som politiet har til finansforetakene, jf. blant annet politiregisterloven § 27 og politiregisterforskriften § 9-7. Prosjektgruppen har i flere arbeidsmøter med tilsynsmyndighetene diskutert behovet for at foretakene skal kunne varsle politiet og utveksle informasjon på eget initiativ, utover de snevre tilfellene som dagens regelverk åpner for.

I Finanstilsynets høringsnotat er det foreslått å gi en utvidet delingsadgang til politiet. Prosjektgruppen er positive til en slik utvidet delingsadgang.

Deling fra foretak til teleoperatør
I gjeldende regelverk er det begrenset adgang til å dele informasjon fra foretakene til teleoperatør. Prosjektgruppen mener dette er utfordrende, ettersom det å effektivt kunne utveksle informasjon med teleoperatører vil kunne være et vesentlig bidrag til å avdekke, forhindre og etterforske betalingsbedrageri – noe som har blitt nøye kartlagt/begrunnet i arbeidsmøter. SMS og telefonsamtale er blant de mest brukte angrepsvektorene i dagens bedragerier, og teleoperatørene spiller derfor en nøkkelrolle i bekjempelsen av slike bedragerier. Ved å dele informasjon, slik som telefonnumre som foretakene har observert blitt brukt i bedrageri, eller som svindlerne har overtatt fra svindelofferet gjennom sosial manipulering (SIM-overtakelse), kan teleoperatørene iverksette tiltak for å hindre at disse numrene brukes videre i svindelsammenheng.

I Finanstilsynets høringsnotat er det foreslått å gi økt adgang til å dele opplysninger med teleoperatører. Prosjektgruppen er positive til slik utvidet delingsadgang.

5. Personvern

5.1. Formålet med behandlingen

Etter personvernregelverket er det sentralt å kartlegge *formålet* med behandlingen av personopplysninger. Det har blitt diskutert i sandkassen om den aktuelle delingen forfølger ett eller flere formål.

Diskusjonen har tatt utgangspunkt i ordlyden til finansforetakslovens § 13-21: «å forebygge, etterforske og avsløre betalingsbedrageri». Det har blitt diskutert om disse

utgjør distinkt forskjellige og atskilte formål og om det er naturlig å sondre mellom forebygging av betalingsbedrageri og etterforskning/avsløring av betalingsbedrageri.

- *Forebygging* omfatter både det å forhindre at pågående forsøk på betalingsbedrageri blir gjennomført og/eller begrense skadevirkningene av et pågående betalingsbedrageri, samt forebygge at nye betalingsbedrageri gjennomføres.

- *Etterforskning/avsløring* omfatter å avdekke et utført eller pågående betalingsbedrageri.

Prosjektgruppen har kommet til at det er utfordrende å skille disse fra hverandre i praksis ettersom de delvis glir over i hverandre og har en innbyrdes nærhet og sammenheng. Ofte er forutsetningen for å kunne *forebygge* betalingsbedrageri, at det har pågått *etterforskning og/eller avsløring* av betalingsbedrageri. Samtidig vil tiltak som iverksettes for å etterforske/avsløre betalingsbedrageri, også kunne ha en preventiv effekt, ved at de reduserer risikoen for at bedrageri lykkes – og på den måten bidra til å forebygge. Prosjektgruppen anser derfor at det som utgangspunkt ikke vil være nødvendig å sondre skarpt mellom nevnte formål, men likevel slik at det vil kunne være nødvendig med nærmere vurderinger i konkrete tilfeller. Særlig gjelder dette med tanke på at det primære formålet med delingen vil kunne være førende for hva som er nødvendig å dele (dataminimering).

5.2. Behandlingsgrunnlag - artikkel 6 nr. 1 bokstav f eller bokstav e?

GDPR artikkel 6 nr. 1 angir en uttømmende liste av tilfeller (grunnlag) for når behandling av personopplysninger er lovlig. Enhver behandling av personopplysninger må være i overenstemmelse med minst ett av de grunnlag bestemmelsen angir. Dersom behandlingen er lovlig etter ett grunnlag, er det ikke nødvendig å avklare om behandlingen også kan være lovlig etter et annet grunnlag.[3]

Finansforetaksloven § 13-21 innebærer ingen plikt til å dele. *GDPR artikkel 6 nr. 1 bokstav c*, rettslig forpliktelse, er følgelig ikke anvendelig.

Prosjektgruppen har i samråd med Datatilsynet diskutert om *GDPR artikkel 6 nr.1 bokstav f* kan fungere som behandlingsgrunnlag. Grunnlaget fremstår som et nærliggende valg, blant annet fordi bekjempelse av bedrageri har blitt fremhevet som en berettiget interesse, både av EDPB[4] og i fortalen til GDPR.[5] Disse kildene indikerer at behandling for å motvirke bedrageri m.m. kan forankres i GDPR artikkel 6 nr. 1 bokstav f.

Det har også blitt diskutert med Datatilsynet om *GDPR artikkel 6 nr. 1 bokstav e* er et egnet behandlingsgrunnlag. GDPR artikkel 6 nr. 1 bokstav e understreker/formaliserer tilknytningen til finansforetaksloven § 13-21 enda tydeligere. Det såkalte «supplerende rettsgrunnlaget» vil da mer eksplisitt etablere rammene for hva som er tillatt.

[3] Se blant annet C-252/21 avsnitt 94.
[4] Guidelines 1/2024, blant annet på side 28.
[5] Fortalepunkt 47.

Prosjektgruppen har kommet til at både GDPR artikkel 6 nr. 1 bokstav e og f kan utgjøre behandlingsgrunnlag for delingen. I det videre skrives sluttrapporten med utgangspunkt i at det er GDPR 6 nr. 1 bokstav e som er behandlingsgrunnlaget.

5.3 GDPR artikkel 6 nr. 1 bokstav e

I dette punktet beskrives prosjektgruppens vurderinger, på bakgrunn av veiledning fra Datatilsynet, av om det er behandlingsgrunnlag for *deling,* i snever forstand. Hva gjelder lovligheten av *operasjonaliseringen/metoden*,[6] vil dette bli omtalt nærmere nedenfor.

GDPR artikkel 6 nr. 1 bokstav e tillater behandling av personopplysninger dersom og i den utstrekning det er «nødvendig for å utføre en oppgave i allmennhetens interesse». Grunnlaget for den oppgaven i allmenhetens interesse det er tale om å utføre, og nærmere regler om behandlingen som kan gjennomføres for å utføre oppgaven, må fastsettes i unionsretten eller den nasjonale rett, jf. GDPR artikkel 6 nr. 3. Lovgivningen skal fastsette formålet med behandlingen, «skal oppfylle et mål i allmennhetens interesse og stå i et rimelig forhold til det berettigede målet som søkes oppnådd» og kan inneholde særlige bestemmelser for å tilpasse anvendelsen av de generelle reglene i GDPR. Slik konkret og mer spesifikk regulering kan være nødvendig for å sikre nødvendige garantier mot misbruk og sørge for at inngrepet holdes til det som er strengt nødvendig (proporsjonalitetsprinsippet).

Finansforetaksloven § 13-21, som tillater blant annet utveksling av opplysninger mellom foretak som yter betalingstjenester for å sikre forebygging, etterforskning eller avsløring av betalingsbedrageri, er begrunnet i og søker å ivareta allmenne interesser knyttet til å motvirke og bekjempe betalingsbedragerier. Betalingsbedrageri, delvis som følge av digitaliseringen av betalingssystemer og tjenester, utgjør et stort samfunnsproblem.

På bakgrunn av veiledning fra tilsynene, har prosjektgruppen kommet til at Finansforetaksloven § 13-21 må forstås som et uttrykk for at foretak som yter betalingstjenester har en viktig oppgave i å bidra til at betalingsbedragerier kan begrenses. Selv om finansforetaksloven og dens forarbeider kunne vært klarere på dette punkt, må det kunne legges til grunn at § 13-21 innebærer at nevnte foretak er tillagt en oppgave i allmenhetens interesse knyttet til å kjempe betalingsbedragerier, og at bestemmelsen regulerer nærmere den behandling av opplysninger som foretakene skal ha tillatelse til å utføre.

Finansforetaksloven fastsetter i den forbindelse nærmere vilkår, herunder for hvilket formål opplysninger kan deles, hva slags type opplysninger som kan deles og mellom hvem.

I den utstrekning foretakene deler opplysninger som er innenfor rammene av finansforetakloven § 13-21 – og som da er *nødvendig* for å oppfylle formålet som er angitt i finansforetaksloven § 13-21 – må behandlingen, etter prosjektgruppens syn,

[6] Spørsmålene om lovlighet av deling og måten delingen skjer på er tett tilknyttet hverandre, men er allikevel to ulike vurderinger. Det er mulig at deling mellom to aktører er lovlig, men det er ikke gitt at enhver *form* for deling er dekket av behandlingsgrunnlaget (da særlig kravet til nødvendighet).

anses å være lovlig etter GDPR artikkel 6 nr. 1 bokstav e. Hva prosjektgruppen mener dette betyr i praksis er nærmere adressert nedenfor i punkt 7.

5.4 GDPR artikkel 10

I prosjektet ble det ikke tatt stilling til om det skal behandles personopplysninger om straffedommer og lovovertredelser eller tilknyttede sikkerhetstiltak, som er underlagt særlig beskyttelse etter GDPR artikkel 10. Prosjektet har likevel diskutert at hvis et finansforetak behandler slike opplysninger, krever GDPR artikkel 10 at behandlingen er *«tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som sikrer nødvendige garantier for de registrertes rettigheter og friheter»*.

At behandlingen er tillatt etter nasjonal rett er gjennomgått ovenfor i punkt 5.3. Prosjektgruppen mener også at det foreligger nødvendige garantier for å beskytte de registrertes rettigheter og friheter. For det første inneholder finansforetaksloven § 13-21 i seg selv visse garantier, ved at den setter klare rammer for delingen. Prosjektgruppen har videre diskutert hvordan det eksisterer et regulatorisk rammeverk som gir de registrerte et tilleggsvern. Blant annet eksisterer det en grunnleggende rett til kundeforhold (kontraheringsplikt for betalingstjenester), plikt til å gjennomføre godkjente betalinger og krav til saklig grunn for å si opp og/eller begrense kundeforholdet. Videre er det tale om utveksling mellom foretak underlagt lovbestemt taushetsplikt. Prosjektgruppen har også vektlagt at det tilhørende prosessuelle rammeverket (krav til klagebehandling i foretak, klagerett til finansklagenemnda m.m.) bidrar til å verne om de registrerte.

Dette har medført at prosjektgruppen har kommet til at så lenge foretakene opererer innenfor rammene av finansforetaksloven § 13-21, er det tillatt å dele opplysningene – dette også selv hvis det forutsettes at behandlingen rammes av GDPR artikkel 10.

5.5. Rolleallokering

I vurderingen av rolleallokering etter personopplysningsregelverket, har prosjektgruppen sammen med tilsynsmyndighetene sondret mellom de to alternative måtene som delingen kan bli operasjonalisert på, jf. beskrivelsen i punkt 3 ovenfor.

<u>Alternativ 1:</u>

Prosjektgruppen har landet på at deling mellom foretakene i Alternativ 1, utføres som selvstendig behandlingsansvarlige. Selv om foretakene deler et felles mål om å forhindre, forebygge, etterforske og avsløre betalingsbedrageri, er det flere forhold som tilsier at de må anses som selvstendig behandlingsansvarlige. Det finnes ingen felles beslutningsstruktur. Delingen iverksettes på foretakets eget initiativ og ansvar, utfra de konkrete omstendighetene som foreligger (selv om datadelingslisten ofte vil danne grunnlaget for når og hva som deles). Selv om det overordnede formålet er likt, vil operasjonaliseringen av formålet være ulikt – ved at foretakene selv vurderer risikoen for sine kunder, og tar egne beslutninger om tiltak basert på mottatt informasjon. Hvert foretak må på selvstendig grunnlag ta stilling til spørsmål som lagringstid m.m. Det er også naturlig at foretakene under Alternativ 1 har selvstendig ansvar for å ivareta den registrertes rettigheter, som innsyn, retting og sletting (i den utstrekning dette skulle bli aktuelt). Det fremstår ikke hensiktsmessig å etablere felles mekanisme for å håndtere slike henvendelser. Det benyttes heller ikke en felles

databehandler eller på andre måter felles infrastruktur. Prosjektgruppen kan heller ikke se hvordan å operere med selvstendig behandlingsansvar gir dårligere personvern enn ved alternative løsninger.[7]

Alternativ 2:

Prosjektgruppen mener at felles behandlingsansvar er en hensiktsmessig rolleallokering under Alternativ 2. Foretakene vil ikke kun ha et likt formål, men vil også velge å etablere en felles infrastruktur og hjelpemidler, ved at opplysningene lagres og behandles i en felles teknisk løsning, som foretakene har tilgang til. Det vil i denne forbindelse bli utpekt en databehandler som vil drifte systemet på vegne av foretakene. Foretakene vil i fellesskap bestemme tilgangsstyring, lagringstid og sikkerhetstiltak m.m. I (enda) større utstrekning enn ved Alternativ 1, blir det etablert formaliserte (og felles) kriterier for når opplysninger skal deles, og hvilke situasjoner som utløser deling.

Hva gjelder rekkevidden av det felles behandlingsansvaret, anser prosjektgruppen det mest riktig at det felles behandlingsansvaret ikke omfatter den forutgående behandlingen av personopplysninger før delingen inn i «hub-en». Videre omfatter ikke det felles behandlingsansvaret den etterfølgende behandlingen, etter at opplysningene blir innhentet fra et aktuelt foretak fra/via «hub-en».

5.7 Personvernrettslig vurdering av Alternativ 2

I den videre gjennomgangen skilles det mellom (i) lovligheten av «hub-en» og (ii) rammene som må etableres for «hub-en». De to spørsmålene henger tett sammen, blant annet fordi forutsetningene for lovligheten av «hub-en» er at det foreligger tilstrekkelige gode og lovlige rammer for delingen.

Det første spørsmålet er lovlighet i snever forstand: om det i utgangspunktet er akseptabelt å etablere en felles «hub» for deling.

Lovlighet av «hub-en»:

Som bemerket i punkt 5.3 mener prosjektgruppen at det i utgangspunktet er behandlingsgrunnlag for å dele mellom de aktuelle foretakene. Dette innebærer imidlertid ikke at det er grunnlag for enhver form for deling. Operasjonaliseringen må være i tråd med kravet til nødvendighet og ellers overholde personvernprinsippene m.m.

Etablering av en felles «hub» tilrettelegger for økt deling og vil medføre at dataen ikke kun lagres i hvert enkelt foretak, men medfører lagring i nytt medium. Det er påkrevd å begrunne/vurdere hvorfor lagringen er nødvendig, jf. GDPR artikkel 5 nr. 1 bokstav c og GDPR artikkel 6 nr. 1 bokstav e.

Som prosjektgruppen har påpekt og diskutert med tilsynsmyndighetene, vil etableringen av en felles «hub» effektivisere delingen. Det vil bli enklere for foretakene å få relevant informasjon om betalingsbedrageri som berører deres

[7] Et perspektiv som har blitt vektlagt av EU-domstolen, ved vurdering av rolleallokering (se for eksempel C-40/17, Fashion ID-avgjørelsen).

kunder. Ved individuell/bilateral deling (Alternativ 1) må istedenfor slike opplysninger utledes av for eksempel transaksjonshistorikk, for å identifisere hvor de andre involverte eventuelt har kundeforhold. Alternativt må informasjon deles med flere foretak som *kan* ha kundeforhold til de involverte. Videre vil deling via den sentraliserte «hub-en» bidra til at foretakene mottar sist tilgjengelig informasjon, uten forsinkelser. Delingen via en såkalt «hub» vil derfor være formålstjenlig, og bidra til en langt mer effektiv realisering av formålet med delingen.

Imidlertid forutsetter bruken av Alternativ 2 gode og etablerte rammer for delingen – som vil bli gjennomgått ytterligere i det følgende.

Overordnede rammer for deling:

Sandkasseprosjektet har ikke gått nærmere inn på detaljreguleringen av en slik felles «hub», men blitt enig om å fastslå noen overordnede rammer, som etter prosjektgruppens syn bør sikres før deling via en «hub»:

- **Ordning om felles behandlingsansvar.** Det må inngås en ordning mellom foretakene som regulerer hvem som har ansvar for hvilke deler av behandlingen, hvordan de registrertes rettigheter skal ivaretas, og hvordan informasjon om behandlingen skal gjøres tilgjengelig for de registrerte m.m.

- **Databehandleravtale.** Det må sikres at aktøren som drifter «hub-en» har inngått databehandleravtale med de aktuelle foretakene.

- **Sletteregler og lagringstid.** Det må etableres rutiner/regler for hvor lenge opplysninger kan lagres, når og hvordan opplysninger skal slettes m.m.

- **Informasjonssikkerhet og tilgangsstyring.** Det må implementeres tekniske og organisatoriske tiltak som sikrer for eksempel tilstrekkelig kryptering og logging, rollebasert tilgangsstyring, beskyttelse mot uautorisert innsyn og endring m.m.

- **Informasjon til registrerte.** De registrerte må få klar og forståelig informasjon (med visse begrensninger) om ordningen.

- **DPIA – Personvernkonsekvensvurdering.** Det må gjennomføres en DPIA.

I tillegg vil foretakene måtte overholde andre regulatoriske krav som blir aktualisert som følge av bruken av «hub-en», herunder reglene i DORA.

6 Forholdet til hvitvaskingsregelverket

Prosjektgruppen har diskutert forholdet til hvitvaskingsregelverket, herunder avsløringsforbudet i hvitvaskingsloven § 28. Avsløringsforbudet rammer i denne sammenheng den som *deler* opplysninger, altså avsenderen. Forbudet innebærer at avsender ikke skal avsløre overfor mottaker at det foretas nærmere undersøkelser

etter hvitvaskingsregelverket.[8] Forbudet omfatter ikke kun avsløring i form av deling av konkrete opplysninger om at det foretas nærmere undersøkelser, men også opplysninger som medfører at kunden eller tredjepersoner *indirekte* vil/må forstå at så er tilfelle. Vurderingen av hvorvidt den tiltenkte delingen rammes av avsløringsforbudet tar utgangspunkt i at avsender (gjennom delingen) gjør mottaker kjent med opplysninger som beskyttes av forbudet. Det er altså ikke relevant for vurderingen om mottaker, på bakgrunn av den mottatte informasjonen, selv igangsetter undersøkelser etter hvitvaskingsregelverket – så lenge denne informasjonen ikke deles videre.

Prosjektgruppen har ikke funnet unntaksbestemmelsene i hvitvaskingsloven § 28 anvendelige for den tiltenkte delingen.[9] Det avgjørende er derfor om informasjonen deles på en slik måte at den rammes av avsløringsforbudet – noe som vil omtales nærmere i det følgende.

Det er enighet om at foretakene ikke skal dele informasjon som anses å være *direkte* avsløring av etterfølgende undersøkelser etter hvitvaskingsregelverket. Delingen vil begrense seg til informasjon knyttet til antatte betalingsbedragerier (primærforbrytelsen), for å hindre eller avdekke ytterligere svindel. Konkret er det snakk om å dele opplysninger fra den såkalte Datadelingslisten, som omtales nærmere i punkt 7 nedenfor.

Prosjektgruppen har imidlertid diskutert hvorvidt finansforetaket som mottar opplysningene *indirekte* vil/må forstå at avsender foretar slike undersøkelser. Problemstillingen gjør seg særlig gjeldende ved deling av opplysninger om mulige muldyr, fordi disse kan besitte «utbytte av en straffbar handling»[10], som igjen kan utløse undersøkelsesplikt etter hvitvaskingsloven.

Prosjektgruppen har likevel kommet til at deling av opplysninger om mulige muldyr, i den form som planlegges etter Datadelingslisten, heller ikke anses å utgjøre indirekte brudd på avsløringsforbudet. Deling av opplysninger om potensielle muldyr er ikke synonymt med at avsender gjennomfører nærmere undersøkelser etter hvitvaskingsregelverket. Det er følgelig ikke grunnlag for mottaker, med tilstrekkelig grad av sikkerhet, å slutte at avsender gjennomfører undersøkelser etter hvitvaskingsregelverket.

Foruten de begrensede opplysningene som fremgår av Datadelingslisten, er det flere rettslige og faktiske forhold ved den tiltenkte informasjonsdelingen som vil hindre mottaker fra å forstå at avsender foretar undersøkelser – dersom det skulle være tilfelle:

---

[8] På delingstidspunktet vil det sjelden være risiko for avsløring av etterforskning eller rapportering av mistenkelige forhold til Økokrim, som er de to andre typetilfellene som dekkes av avsløringsforbudet, så dette omtales ikke nærmere. Forholdene som begrunner deling nedenfor, vil uansett gjøre seg gjeldende dersom det skulle være rapportert eller gjennomføres etterforskning.

[9] Umiddelbart fremstår det mest nærliggende unntaket å være hvitvaskingsloven § 28 (6). Imidlertid kommer ikke unntaket til anvendelse for den tiltenkte delingen. Årsaken er at informasjonsdelingen som regel vil angå langt flere mottakere enn de rapporteringspliktige som deltar i «en transaksjon» med «felles kunde». Unntaksbestemmelsen i hvitvaskingsloven § 28 (4), jf. § 31 (3) begrenser seg til *"nødvendige kundeopplysninger…når det anses nødvendig som ledd i nærmere undersøkelser etter § 25",* mens den tiltenkte delingen i medhold av finansforetaksloven § 13-21 gjelder primærforbrytelsen betalingsbedragerier – uavhengig av om det senere foretas nærmere undersøkelser etter hvitvaskingsloven eller ikke. Dessuten er det et vilkår at delingen er «nødvendig» for å gjennomføre nærmere undersøkelser, hvilket gjør at bestemmelsen forholdsvis sjeldent vil være anvendelig for betalingsbedragerier. Heller ikke de øvrige unntaksbestemmelsene anses anvendelige.

[10] Vilkåret i straffelovens heleri- og hvitvaskingsbestemmelser, jf. hvitvaskingsloven § 2 bokstav a

For det første begrenser definisjonen av sekundærforbrytelsen hvitvasking seg til forsettlige heleri- og hvitvaskingshandlinger, jf. hvitvaskingsloven § 2 bokstav a. Eksempelvis vil forsøk på bedrageri der det enda ikke er generert et økonomisk utbytte – typisk der banken stanser bedrageriet, men deler muldyrinformasjon – falle utenfor gjerningsbeskrivelsen i heleribestemmelsen i straffeloven § 332 («mottar»). Utenfor hvitvaskingslovens anvendelsesområde vil det ikke foreligge undersøkelsesplikt etter § 25, og følgelig rammes ikke deling av slik informasjon av avsløringsforbudet. Tilsvarende rammer heller ikke hvitvaskingslovens definisjon *uaktsomt* heleri (straffeloven § 335) eller faktisk villfarelse (straffeloven § 25). Med de begrensede opplysningene som fremgår av Datadelingslisten, vil mottaker derfor ikke ha forutsetninger for å forstå hvorvidt det deles informasjon om uaktsomt ID-misbrukte muldyr eller unnskyldelig uvitende muldyr, som ikke utløser undersøkelsesplikt, eller om det faktisk mistenkes en forsettlig helerihandling – som utløser plikten.

For det andre vil informasjonen som deles like gjerne kunne utløse plikt til løpende oppfølging av kundeforhold, fordi det er tvil om tidligere innhentede opplysninger er korrekte eller tilstrekkelige, jf. hvitvaskingsloven § 24 andre ledd, andre punktum, som undersøkelser etter § 25 andre ledd. Slik løpende oppfølging er ikke underlagt avsløringsforbud. Løpende oppfølging kan også gjennomføres parallelt med nærmere undersøkelser.

For det tredje vil miljøene for bedrageribekjempelse, blant annet av hensyn til avsløringsforbudet, gjerne arbeide adskilt fra miljøene som gjennomfører undersøkelser og rapportering etter hvitvaskingsregelverket. Mottaker av informasjon som deles fra et slikt miljø for bedrageribekjempelse, vil derfor ikke ha forutsetninger for å forstå om det foretas nærmere undersøkelser.

For det fjerde, kan opplysningene være delt med mottaker på et så tidlig tidspunkt at avsender selv ikke har avdekket forhold som «kan indikere» at midlene også har tilknytning til hvitvasking – i tillegg til primærforbrytelsen bedrageri. Undersøkelsesplikten etter § 25 første ledd oppstår først når avsender «avdekker» slike forhold.

Det må på denne bakgrunn antas at delingen normalt kan skje uten at den berøres av avsløringsforbudet, jf. også høringsnotatet om regulatoriske sandkasser, vedlegg 1 s. 3.

At deling i medhold av PSD2 artikkel 94 / finansforetaksloven § 13-21 normalt ikke rammes av avsløringsforbudet, harmonerer med ordlyden i hvitvaskingsloven § 28, som på delingstidspunktet altså begrenser seg til tilfeller der undersøkelsesplikten faktisk har inntrådt. En utvidende tolkning av avsløringsforbudet ville gjort finansforetaksloven § 13-21 ineffektiv ved at finansforetakene ikke får forebygget/avdekket flere bedragerier – og dermed heller ikke flere hvitvaskingshandlinger –, i strid med formålet bak begge bestemmelsene. Det har neppe vært lovgivers intensjon. Finansforetaksloven § 13-21 gjennomfører dessuten PSD2 i norsk rett, og en slik praktisering av bestemmelsen vil medføre brudd med både direktivet og de nye reglene som ventes i PSR. Også det har formodningen mot seg.

På denne bakgrunn, samt med veiledning fra Finanstilsynet, har prosjektgruppen kommet til at det må antas at den tiltenkte delingen normalt ikke vil berøres av avsløringsforbudet i hvitvaskingsloven.

7 Datadelingslisten

På bakgrunn av gjennomgangen ovenfor har prosjektgruppen utarbeidet en datadelingsliste. Listen gir oversikt over datafelter som prosjektgruppen mener at faller inn under finansforetaksloven § 13-21, samt tilhørende eksempelscenarioer.

Formålet med listen er å gi et praktisk verktøy for å identifisere hvilke data som kan deles lovlig i samsvar med gjeldende regelverk.

Datatilsynet har ikke vurdert alle behandlingene av personopplysninger knyttet til denne listen, men har veiledet om dataminimeringsprinsippet, nødvendighetsvilkåret og forholdsmessighetsprinsippet.

Dersom de foreslåtte endringene i finansforetaksloven § 16-2 blir vedtatt, vil datadelingslisten måtte oppdateres/endres i tråd med den utvidede delingsadgangen.

8 Veien videre

Målet til prosjektgruppen har vært at sandkasseprosjektet resulterer i mer utstrakt deling i bransjen, med det overordnede målet om å forebygge og redusere antall betalingsbedragerier.

Prosjektgruppens ambisjon er at vurderingene fra sandkasseprosjektet raskt skal kunne tas videre av bankene og andre relevante aktører - eksempelvis NFCERT og Finans Norge.

I første omgang, legger foretakene i prosjektet opp til å dele informasjon basert på vurderingene i sandkassen, gjennom manuell deling mellom aktører. På noe lengre sikt, er tanken at bankene vil dele data gjennom en sentral “hub”. Prosjektgruppen har vært i dialog med NFCERT med tanke på mulig operasjonalisering av dette etter prosjektets avslutning.

Prosjektgruppen vil jobbe for å videreføre arbeidet med å operasjonalisere delingen. I denne forbindelse vil det være behov for å avklare ytterligere juridiske spørsmål.

Prosjektgruppen antar at den tiltenkte delingen også vil etterleve EUs kommende AML-forordning, selv om det ventes ytterligere detaljering av regelverket i bebudete Regulatory Technical Standards og Guidelines frem mot sommeren 2027. Det vises her blant annet til at skillet mellom den særnorske undersøkelsesplikten og rapporteringsplikten hviskes ut i forordningen, at rapporteringsplikten utvides til å gjelde primærforbrytelser, og at delingsadgangen virker å bli utvidet for foretak som inngår i såkalte partnerskap for informasjonsutveksling, jf. AMLR artikkel 75 nr. 3 bokstav g.

I fremtiden kan det være aktuelt å se nærmere på muligheten til å bygge videre på «hub»-alternativet, for eksempel ved å utvide den med felles analyse- og deteksjonskapabiliteter. Her kan man tenke seg at data fra flere foretak analyseres samlet, enten gjennom automatiserte verktøy eller av en nøytral tredjepart. Formålet med dette er å identifisere mønstre og sammenhenger som ikke er synlige i enkeltaktørers data. En slik løsning kan bidra til å avdekke kriminelle nettverk og gjentakende modus på tvers av aktører, og gi raskere varsling. Løsningen fordrer imidlertid ytterligere rettslige avklaringer som ikke har vært vurdert innenfor dette sandkasseprosjektet, og heller ikke vært drøftet med tilsynsmyndighetene.

Erfaringene fra sandkassen og dialogen med både Finanstilsynet og Datatilsynet er positive, og det er ønskelig å fortsette den gode dialog med tilsynene på veien videre.

***