KPMG eika.

Sandkasserapport

Februar 2026

Sammendrag

Denne rapporten oppsummerer et regulatorisk sandkasseprosjekt gjennomført av Eika Gruppen og KPMG, i samarbeid med Finanstilsynet og Datatilsynet. Formålet har vært å utforske det juridiske handlingsrommet for økt og mer effektiv datadeling mellom banker i arbeidet mot økonomisk kriminalitet, herunder anti-hvitvasking. Formålet omfatter dermed også identifisering av eventuelt manglende rettslig mulighetsrom. I forbindelse med økt fokus på informasjonsdeling er det ved flere anledninger påpekt at det kan være bankene har større muligheter for deling enn det som skjer i praksis, slik at også identifisering av manglende hjemmelsgrunnlag for datadeling blir viktig.

Bakgrunnen for prosjektet er en observert økning i økonomisk kriminalitet knyttet til bedrageri og organisert kriminalitet. Utbytte fra primærforbrytelser må som regel hvitvaskes før det kan nyttiggjøres, noe som forutsetter bruk av finansielle tjenester og ofte involverer flere banker. Kriminelle aktører utnytter i dag fragmenterte datasett og manglende samhandling mellom banker, og prosjektet tar derfor utgangspunkt i at et mer helhetlig informasjonsgrunnlag kan styrke både treffsikkerhet og effektivitet i bankenes arbeid, samtidig som rettssikkerhet og personvern ivaretas.

Sandkassearbeidet har bestått av strukturerte arbeidsmøter der juridiske rammer for datadeling er vurdert med utgangspunkt i tre typiske faser av arbeidet med anti-hvitvasking:

1. Deteksjon/identifisering av mistanke
2. Utredning av mistenkelige forhold
3. Kundevurdering og «flaggede» kunder

Vurderingene er gjort med bakgrunn i finansforetaksloven, hvitvaskingsloven og personvernregelverket (GDPR).

Prosjektet konkluderer med at gjeldende regelverk gir et visst, men begrenset handlingsrom for datadeling. I utredningsfasen åpner hvitvaskingsloven for deling når dette er nødvendig som ledd i nærmere undersøkelser. Her vurderes det som juridisk mulig å etablere mer strukturerte, sikre og sporbare tekniske løsninger enn dagens praksis, forutsatt klare rutiner, dokumenterte nødvendighetsvurderinger og streng tilgangsstyring. I deteksjonsfasen er handlingsrommet derimot svært snevert. For kundevurderinger identifiseres kun et begrenset og regulatorisk risikofylt rom for systematisk deling etter dagens regler.

Rapporten viser samtidig at foreslåtte endringer i finansforetaksloven kan åpne et større mulighetsrom for mer systematisk og forebyggende datadeling i arbeidet mot økonomisk kriminalitet. Særlig vil fjerning av krav om styrevedtak og «særlige tilfeller» i finansforetaksloven, samt tydeligere hjemler for deling for forebyggende formål, kunne muliggjøre mer systematisk samarbeid i både deteksjon og kundevurdering. Dette vurderes som avgjørende for å kunne realisere ambisjoner om mer effektiv bekjempelse av økonomisk kriminalitet, slik også politiske ambisjoner legger opp til.

Avslutningsvis understrekes det at prosjektet gir prinsipielle vurderinger, men ikke godkjenning av konkrete løsninger. Eventuell implementering vil kreve ytterligere juridiske, tekniske og organisatoriske vurderinger, samt et robust avtaleverk. Rapportens appendiks inneholder prosjektets samlede innspill til foreslåtte lovendringer, og er ment som et supplement til hovedfunnene.

Innhold

Sammendrag 2
Innhold 3
Om prosjektet 4
Om Eika Gruppen og KPMG 4
Bakgrunn 4
Behovet for dette prosjektet 4
Prosjektets mål og avgrensninger 5
Hvilket regelverk er relevant? 7
Finansforetaksloven 7
Hvitvaskingsloven 8
Personvernregelverket 10
Behandlingsgrunnlag 10
Om automatiserte behandlinger 11
Dataminimeringstiltak 12
Tilgangsstyring 12
Juridiske vurderinger av fasene i anti-hvitvaskingsarbeidet 13
1. Deling innen deteksjon 13
Problemstilling 13
Drøfting av løsning 13
2. Deling innen utredning 14
Problemstilling 14
Drøfting av løsning 16
3. Deling innen kundevurdering 18
Problemstilling 18
Drøfting av løsning 18
Oppsummering og konsekvenser for videre arbeid 19
Hvilket økt mulighetsrom ser vi med eksisterende lovverk? 19
Hvilket økt mulighetsrom ser vi med nytt lovverk? 20
Refleksjoner rundt videre arbeid og lovutvikling 21
Appendiks – Innspill til lovendringer i Finansforetaksloven 22
Innledning 22
Utlevering av opplysninger i god tro 22
Strenger nødvendighetskrav 22
Presisering av formålsangivelsen 23
Presisering av anvendelsesområdet til GDPR art. 6 nr. 1 bokstav c 23
Presisering av trykkfeil 23

Om prosjektet

Datatilsynet og Finanstilsynet inviterte i november 2024 banker til å delta i etatenes regulatoriske sandkasse, med prosjekter som utforsker muligheten for bedre datadeling i bekjempelsen av økonomisk kriminalitet.

Et av prosjektene som ble tatt opp, var et samarbeid mellom Eika Gruppen og KPMG, med formål å utforske mulighetene for økt datadeling i Eika-bankenes arbeid mot økonomisk kriminalitet, herunder anti-hvitvasking.[1]

Sandkassearbeidet har bestått av møter mellom Eika, KPMG, Datatilsynet og Finanstilsynet, der juridiske rammer, handlingsrom og mulige løsninger for datadeling er vurdert.

Denne sluttrapporten – utarbeidet av Eika Gruppen og KPMG – oppsummerer vurderinger og funn, basert på den faglige støtten som er gitt fra Finanstilsynet og Datatilsynet gjennom det regulatoriske sandkassearbeidet.

Om Eika Gruppen og KPMG

Eika Gruppen AS[2] består av nærmere 50 lokale sparebanker av ulike størrelser i Norge. Gruppen er en allianse eid av bankene, som har flere fellestjenester for medlemsbankene.

KPMG AS er et globalt konsulentselskap med store engasjementer innen anti-hvitvasking i norske og nordiske banker. KPMG har vært prosjekt- og prosjektlederstøtte for Eika i forberedelser, gjennomføring og etterarbeid for arbeidsmøter med tilsynene. KPMG har ikke fått betalt av Eika eller andre for dette oppdraget. KPMG Law Advokatfirma AS har bistått prosjektet med juridiske vurderinger.

KPMG samarbeider med mange finansinstitusjoner i Norge og resten av Norden. I prosjektet har KPMG trukket fra totaliteten av sine erfaringer, ikke bare knyttet til Eika.

I tillegg til Eika og KPMG deltok også Nordea i arbeidsmøtet som diskuterte kundevurdering (fase 3).

Bakgrunn

Prosjektet har sin bakgrunn i Eikas ønske om mer samarbeid på tvers i alliansen, for å bedre levere på samfunnsoppdraget i bekjempelsen av økonomisk kriminalitet.

Selv om det er tatt utgangspunkt i tre ulike faser tilknyttet anti-hvitvaskarbeidet, har prosjektet hatt en bred tilnærming ved å se på flere juridiske innfallsvinkler for deling av informasjon.

Ambisjonene har vært høye: å utforske det juridiske mulighetsrommet for økt samarbeid og datadeling i alle definerte faser. Eikas organisering og etablerte samarbeid gjør alliansen godt egnet til å belyse problemstillinger og potensielle løsninger som også er relevante for flere aktører. Som allianse – og ikke et finanskonsern – opererer Eika også innenfor de samme rettslige rammene for datadeling som ellers uavhengige banker. Samtidig gir det tette samarbeidet gode forutsetninger for å omsette idéer til praktiske løsninger.

Behovet for dette prosjektet

Økonomisk kriminalitet fremheves som en betydelig og voksende utfordring, hvor samarbeid og informasjonsdeling ofte trekkes frem som avgjørende for å møte truslene. Vi ønsker derfor å gi et bakteppe til drøftingene om deling som vil følge under i denne rapporten.

Kriminalitetsbildet i Norge knyttet til organisert kriminalitet har blitt mer krevende. Bomben som detonerte i Drøbak for over to år siden rystet mer enn bare et nabolag. Den brakte et annet

[1] «AHV» og anti-hvitvask vil benyttes som en samlebetegnelse på anti-hvitvask og anti-terrorfinansiering
[2] Eika, Eika-gruppen og «alliansen» vil benyttes om hverandre i rapporten

kriminalitetsbilde i fokus for mange nordmenn. Siden denne hendelsen har det vært en rekke grove voldshendelser i Norge, som høsten 2025 inkluderte håndgranater i bybildet på Østlandet og barn som blir rekruttert til voldsoppdrag mot betaling. Disse hendelsene har gjerne bunnet i konflikter i organiserte kriminelle miljøer, og har vært knyttet til narkotikahandel. Økt narkotikaomsetning, som indikeres av Tolletatens trusselvurdering for 2025, øker også behovet for hvitvasking.

Samtidig har bedrageri blitt en viktigere inntektskilde for kriminelle. I Sverige anslås utbytte fra bedragerier å nå overstige narkotikautbytte. I 2022 dro svenske kriminelle inn anslagsvis 5,8 milliarder SEK fra bedragerier. Bedrageritrenden har vært stigende siden – også i Norge. Omfanget av bedrageri har ført til at Økokrim kaller dette for et «samfunnsproblem».[3]

For å unngå oppdagelse og kunne nyte av disse midlene, må de hvitvaskes. Dette henger nødvendigvis sammen med den forutgående primærforbrytelsen, særlig i forbindelse med digitale bedragerier. I motsetning til annen kriminalitet som benytter kontanter, er utbyttet fra bedrageri gjerne allerede i den digitale bankverdenen. Utbyttet må derfor flyttes raskt gjennom banksystemet, før bedrageriet blir oppdaget og midlene stanses.

Økonomisk kriminalitet, herunder bedrageri, har også sterke koblinger til fysisk vold. Oslo Politidistrikt har pekt på at bedrageri finansierer voldskriminalitet[4], og Svensk politi fant at nær halvparten av de som har vært mistenkt for voldskriminalitet, også har vært mistenkt for bedrageri.[5]

Som påpekt av Økokrim er kriminelle raskt ute med å ta i bruk ny teknologi og endre metoder.[6] De er ikke bundet av lovverk, regulativer, internrutiner eller taushetsplikt. Man må erkjenne at aktørene som står imot den økonomiske kriminaliteten, både myndigheter og finansbransjen, ikke har klart å være like smidige av praktiske og juridiske årsaker.

Eika og KPMG mener derfor at denne runden med sandkasseprosjekter kom på et godt tidspunkt. Det er nødvendig å fullt ut utnytte handlingsrommet for samarbeid og deling, om man skal demme opp for denne økningen i økonomisk kriminalitet. Der det identifiseres manglende mulighetsrom er det viktig at dette tydeliggjøres for næringen og myndighetene, slik at konsekvensene det har for deteksjonskapabilitet kommer tydelig frem.

Organisert kriminalitet er profittmotivert, og utbyttet må hvitvaskes. I et gjennomdigitalisert samfunn, med høy bruk av moderne banktjenester, finnes de sentrale sporene i bankenes datasystemer. Ved å bruke denne informasjonen bedre, og på tvers av foretak og myndigheter, kan innsatsen mot økonomisk kriminalitet styrkes betydelig. Det følgende er vårt bidrag til å nå denne ambisjonen.

Prosjektets mål og avgrensninger

Prosjektet har hatt som overordnet mål å utforske sikre og effektive løsninger for datadeling mellom banker i Eika Gruppen for å styrke og sentralisere arbeidet mot økonomisk kriminalitet. Kjernen i prosjektet har vært å undersøke hvordan dagens lovverk kan tolkes, anvendes og videreutvikles for å muliggjøre bedre datadeling i anti-hvitvaskingsarbeidet og arbeidet mot økonomisk kriminalitet generelt.

Den viktigste delen av prosjektet, og hovedfokus for sandkassearbeidet, har vært tre sentrale datadelingssituasjoner:

1. Datadeling for å identifisere mistanke

Prosjektets første delmål var å undersøke hvordan Eika-bankene kan benytte kunde- og transaksjonsdata på tvers av alliansen for å få mer presise og risikobaserte alarmer. Målet var å

[3] Økokrim, «Bedrageri - et samfunnsproblem»
[4] Dagens Næringsliv, «Tegner bildet av granatkrigens økonomiske bakteppe», 31.10.25
[5] Svenske Polisen, «De dödliga bedrägerierna», 2022
[6] Økokrim, «Trusselvurdering 2024 – Den kriminelle økonomien»

forstå om dagens regelverk ga rom for å se kunder og deres aktivitet i sammenheng på tvers av banker og dermed ha høyere presisjon i arbeidet mot økonomisk kriminalitet.

2. Datadeling i undersøkelser av mistenkelige forhold (utredning)

Prosjektets andre delmål var å vurdere om og hvordan Eika-bankene kan dele og innhente nødvendig informasjon sømløst og strukturert når en alarm krever nærmere undersøkelser. Prosjektet så på hvordan dagens manuelle praksis kan erstattes av mer sporbare, standardiserte og teknisk sikre løsninger. Videre tok prosjektet for seg hvordan nødvendighetskravet i hvitvaskingsloven og dataminimeringsprinsippet i GDPR må balanseres mot behovet for mer helhetlige og effektive løsninger. Denne fasen favner både forundersøkelser (før undersøkelsesplikten etter hvitvaskingsloven inntreffer) og «nærmere undersøkelser» etter hvitvaskingsloven.

3. Datadeling ved kunderisikovurdering

Prosjektets tredje delmål var å utforske om og hvordan Eika-bankene kan dele informasjon om kundeforhold der banken(e) har etablert en mistanke. Dette innebar å forstå handlingsrommet i delingsadgangen etter finansforetaksloven uten å komme på kant med kontraheringsplikten, bryte avsløringsforbudet eller personvernregler, og om slik deling kan redusere problemet med «bankshopping» blant kriminelle.

For leseren vil det være nyttig å se for seg at forslagene implementeres i et felles teknisk system, hvor hver banks data kan avgrenses i siloer som et utgangspunkt, men hvor det er mulig å legge inn åpninger/delingsadganger mellom siloene.

Samtidig er det viktig å påpeke at Eika og KPMG har ønsket å ta en maksimalistisk tilnærming i prosjektet. Det vil si at vi har diskutert med Datatilsynet og Finanstilsynet ulike alternative løsninger for å utforske hvor grensene for gjeldende regelverk går. Det er dermed ikke gitt at alt mulighetsrom som identifiseres vil benyttes av Eika. Våre endelige løsninger vil ikke bare ta utgangspunkt i det juridiske, men også i det teknologiske og forretningsmessige handlingsrommet. Vi håper at mulighetsrommet identifisert i denne rapporten uansett vil komme flere aktører til gode, og at andre kan nyttiggjøre seg av mulighetsrommet vi ikke selv benytter oss av, i tråd med sandkassenes formål som et felles gode.

Videre vil løsningene forutsette et forutgående og potensielt omfattende avtaleverk for å kunne settes ut i livet. Dette innebærer utkontrakteringsavtaler, rutiner for etterfølgende kontroller, sikkerhet/tilgangsstyring, ivaretakelse av kravene etter Digital Operational Resilience Act (DORA) med mer. Vi har ikke hatt muligheten til å gjennomføre omfattende vurderinger av alle disse rammene i sandkasseprosjektet med Datatilsynet og Finanstilsynet, men etterfølgelse av disse legges til grunn for løsningene selv om de ikke omtales.

I søken etter å bli bedre på bekjempelse av økonomisk kriminalitet kan det reises spørsmål ved hvor langt *plikten* strekker seg for bankene, og om prosjektet ser mot et ambisjonsnivå utover det lovgiver har forutsatt. Det skal være lav terskel for å rapportere til Økokrim, og banker skal ikke drive etterforskning. Vi mener likevel at det innenfor rammene av *plikten* er forbedringspotensialer, og at å bli mer effektiv og mer treffsikker i arbeidet med økonomisk kriminalitet vil komme både banker, kunder, politiinnsatsen, og samfunnet for øvrig, til gode.

Som nevnt over har prosjektets hovedformål vært å se på datadeling innen anti-hvitvaskarbeidet, som er underlagt et eget lovverk adskilt fra lovverk som regulerer datadeling innen annen økonomisk kriminalitet. I realiteten endte prosjektet med å inkludere også mulighetsrom for datadeling innen andre former for økonomisk kriminalitet enn anti-hvitvaskarbeidet. Dette var dels på grunn av et ønske om å benytte muligheten til å utforske så mye som mulig i sandkasseprosjektet, dels på grunn av forslaget til lovendring som kom i løpet av prosjektperioden

med nye muligheter og dels på grunn av hvordan disse kriminalitetsområdene henger så tett sammen i virkeligheten.

Underveis i prosjektperioden kom høringsnotatet for nytt lovforslag til finansforetaksloven, med høringsfrist 14. november 2025. Selv om fokus i prosjektet var å utforske mulighetsrommet i eksisterende lovverk, var det helt naturlig å diskutere hvordan dette ville kunne se ut i fremtiden når partene likevel var samlet. Vi har inkludert synspunkter på lovforslaget i denne rapporten, samt vår forståelse av de mulighetene som kan oppstå, der det har vært relevant å fremheve slike. I sluttrapportens appendiks er det lagt ved en oppsummering på prosjektets innspill til lovforslaget.

Hvilket regelverk er relevant?

I prosjektet har Eika og KPMG, i samråd med Datatilsynet og Finanstilsynet, begrenset seg til å se på skrankene og mulighetene for datadeling som ligger innenfor tilsynenes myndighetsområder. Dette inkluderer:

- Finansforetaksloven
- Hvitvaskingsloven
- Personvernregelverket

De tekniske løsningene som Eika og KPMG ønsker å realisere, aktualiserer en rekke juridiske problemstillinger som går på tvers av disse regelverkene. Det presiseres at mange av de juridiske vurderingene etter ulike lovverk har vært sammenfallende, og dermed diskutert felles, ikke isolert for den enkelte lovtekst. Dette gjelder blant annet kravet til nødvendighet, da vilkåret går igjen i samtlige lover.

Ettersom høringsnotatet for endringer i finansforetaksloven ble publisert i løpet av samarbeidsperioden til sandkasseprosjektet, har mulighetsrommet og nødvendige avklaringer rundt den foreslåtte lovteksten vært et sentralt tema for siste samling. Utkastet til ny finansforetakslov § 16-2, med tilhørende forskrifter, åpnet tilsynelatende for en adskillig videre delingsadgang enn etter regelverket som gjaldt i februar 2026, som var når denne rapporten for sandkasseprosjektet ble ferdigstilt. Det var dermed nødvendig å få klarhet i de rettslige rammene som ble presentert og intendert handlingsrom.

Finansforetaksloven

Et sentralt tema for sandkasseprosjektet har vært handlingsrommet som potensielt ligger i dagens ordlyd i finansforetaksloven § 16-2 tredje ledd. Det følger av denne bestemmelsen at

> *«Taushetsplikten etter første ledd er ikke til hinder for at et finansforetak i særlige tilfelle gir et annen finansforetak opplysninger som foretaket har mottatt under utøvelsen av virksomheten, dersom*
>
> *a. Formålet er å avdekke eller motvirke økonomisk kriminalitet eller annen alvorlig kriminalitet. […]»* (våre understrekninger)

Det følger videre av bestemmelsens fjerde ledd at

> *«Utlevering av opplysninger etter første punktum kan bare skje i henhold til styrevedtak.»*

Slik Eika og KPMG ser det, er bestemmelsen i utgangspunktet godt egnet til å åpne for en vid datadelingsadgang, ettersom bestemmelsen i liten grad begrenser hvilke opplysninger som kan deles, samt at det tilsynelatende er tilstrekkelig at formålet er å enten *«avdekke eller motvirke økonomisk kriminalitet eller annen alvorlig kriminalitet».* Isolert sett taler dette for en vid delingsadgang også til forebyggende formål, før en konkret mistanke mot den enkelte kunden har materialisert seg, jf. ordlyden av *«avdekke eller motvirke»*.

Bestemmelsen hjemler likevel ikke en generell adgang til datadeling, og terskelen fremstår ved videre tolkning som høy når man leser bestemmelsen i sammenheng, jf. blant annet henvisningen til gjennomført styrevedtak for å ha en slik delingsadgang. Forarbeidene presiserer at *«[d]et er ikke adgang for styret til å fastsette retningslinjer som gir en helt generell adgang til rutinemessig utveksling av opplysninger mellom finansforetak»*., jf. Prop.125 L (2013-2014) s. 206. I tillegg gjelder delingsadgangen kun i «*særlig tilfelle*» uten at terskelen for dette er direkte angitt. Ordlyden *«særlig»* gir her en anvisning på at bestemmelsen bare unntaksvis kan benyttes som hjemmel for delingsadgang. Disse momentene innskrenker finansforetakenes delingsadgang betydelig.

I arbeidsmøtene uttrykte Finanstilsynet enighet om at behandlingen av § 16-2 tredje ledd er utfordrende å anvende i praksis, og ikke rommer den delingsadgangen man har behov for i banker generelt. Særlig kravet om styrevedtak og den høye terskelen for anvendelsesområdet, jf. vilkåret om *«særlige tilfelle»*, sperrer for systematisk deling av kundeopplysninger. Dette er til hinder for effektiv avdekking og motvirkning av økonomisk og annen alvorlig kriminalitet. Det virker lite hensiktsmessig at banker som sitter på informasjon om at mulig økonomisk kriminalitet foregår, ikke kan dele dette med andre banker for å avdekke eller motvirke slik kriminalitet. Dette må ses i sammenheng med at den teknologiske utviklingen har gjort at særlig svindel og bedrageri forekommer og avdekkes hyppigere, men også kan fullbyrdes raskere. Det er dermed nødvendig med effektive mekanismer i arbeidet mot økonomisk kriminalitet.

I arbeidsmøtene med Finanstilsynet ble det presisert at dagens regelverk ikke åpner opp for rent rutinemessig deling for å oppdage og avverge økonomisk og annen alvorlig kriminalitet, slik det også følger av lovens forarbeider. De presiserte at det likevel var en viss adgang til deling av opplysninger på typetilfellenivå ved mistanke om eksempelvis svindel fra bankkontoer, og at det er tilstrekkelig med at styrevedtaket retter seg mot tilstrekkelig alvorlige og konkretiserte typetilfeller. Denne adgangen kan etter dagens regelverk ikke delegeres bort til andre enn styret. Likevel er det ikke nødvendigvis et krav om styrevedtak på den enkelte delingsforespørselen, men det forutsetter at kravet til *«særlige tilfelle»* er hensyntatt i styrevedtaket, og at tilfellet er tilstrekkelig konkretisert. Denne adgangen er dermed reelt sett snever, og det vil være utfordrende å manøvrere når man er innenfor og utenfor den høye terskelen loven legger opp til. Forslaget til endringer i finansforetaksloven skal dermed tjene til det formål å utvide delingsadgangen i betydelig grad, der Eika og KPMGs bekymringer rundt dagens regelverk har bidratt til en ny og mer velegnet lovhjemmel for datadeling. Dette inkluderer å fjerne kravet til styrevedtak og ordlyden om å kun gjelde ved *«særlige tilfelle».*

Når det gjelder utveksling av transaksjonsopplysninger og annen betalingsinformasjon, gir finansforetaksloven § 13-21 første ledd en særlig adgang til å dele slike opplysninger. Anvendelsesområdet til bestemmelsen omfatter imidlertid kun *«betalingsbedrageri»*, og avgrenser dermed mot andre former for økonomisk kriminalitet eller annen alvorlig kriminalitet. Forslaget til endringer i ffl. innebærer å fjerne denne for å så inkorporere den i en videre § 16-2. Totalt sett har Eika og KPMG derfor vurdert det som mest hensiktsmessig å heller prioritere diskusjoner rundt foreslått regelverk fremfor eksisterende § 13-21. Denne er imidlertid grundig behandlet i utvalgte andre sandkasseprosjekter, og det vises derfor til disse for en nærmere vurdering av ffl. § 13-21.

Hvitvaskingsloven

Et av temaene i arbeidsmøtene med Finanstilsynet og Datatilsynet var særlig hvilket handlingsrom man finner i den spesielle delingsadgangen som følger av hvitvaskingsloven (hvvl.) § 31. Det følger av bestemmelsens tredje ledd at

> *«Rapporteringspliktige som nevnt i § 4 første ledd bokstav a til c og j, kan uten hinder av taushetsplikt utveksle nødvendige kundeopplysninger seg imellom når det anses nødvendig som ledd i nærmere undersøkelser etter § 25»* (vår understrekning)

Det er bare utvalgte «*rapporteringspliktige*» som har mulighet til å utveksle opplysninger i henhold til bestemmelsen, ettersom ordlyden kun viser til hvvl. § 4 fjerde ledd bokstav a til c og j. Banker omfattes av bestemmelsen, jf. § 4 første ledd bokstav a.

For å kunne *«utveksle nødvendige kundeopplysninger»* må det anses *«nødvendig»* som *«ledd i nærmere undersøkelser etter § 25»*. Undersøkelsesplikten etter denne bestemmelsen anses utløst dersom

(1) «Den rapporteringspliktige avdekker forhold som kan indikere at midler har tilknytning til hvitvasking eller terrorfinansiering
(2) Dersom det avdekkes forhold som avviker fra den rapporteringspliktiges kjennskap til kunden, kundeforholdets formål og tilsiktede art, eller dersom en transaksjon

a) Synes å mangle et legitimt formål
b) Er usedvanlig stor eller kompleks
c) Er uvanlig ut fra kundens kjente forretningsmessige eller personlige mønster av transaksjoner
d) Foretas til eller fra personer i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking og terrorfinansiering
e) På en annen måte har uvanlig karakter»

Lest i sammenheng vurderer Eika og KPMG at bankene i Eika Gruppen har anledning til å utveksle slike *nødvendige* kundeopplysninger når det anses *nødvendig* etter at en bank har avdekket forhold som kan indikere at midler har tilknytning til hvitvasking eller terrorfinansiering, det er avdekket forhold som avviker fra bankens kjennskap til kunden, eller en transaksjon anses å falle inn under de ulike alternativene i § 25 (2) bokstav a til e.

Det foreligger imidlertid ingen plikt til å dele opplysninger når kriteriene som sådan er oppfylt. Den rapporteringspliktige velger selv hvorvidt de ønsker å dele eller å avstå fra å dele *kundeopplysninger* i tråd med bestemmelsen.

Spørsmålet er dermed når undersøkelsesplikten er utløst. En begrensende faktor i dette, og dermed til delingsadgangen, vil være den doble nødvendighetsvurderingen som ligger i hvitvaskingsloven § 31 tredje ledd. Gitt at undersøkelsesplikten er utløst har bankene som redegjort for over anledning til å dele *«nødvendige kundeopplysninger»* seg imellom når det anses *«nødvendig»*.

At de rapporteringspliktige kan dele *«nødvendige kundeopplysninger»* avgrenser mot kundeopplysninger som det ikke er behov for som ledd i de nærmere undersøkelsene. Bestemmelsen gir derfor ikke adgang til å dele informasjon om en kunde ukritisk, selv om undersøkelsesplikten er utløst. Det må foretas en vurdering av hvilke opplysninger som faktisk er *nødvendige* å dele for å oppnå formålet.

Videre følger det av bestemmelsen at delingen må *«anses nødvendig»* som ledd i de nærmere undersøkelsene. Dette innebærer at det må foretas en konkret vurdering i hvert enkelt tilfelle, hvor bankene vurderer om nødvendighetskriteriet er oppfylt. Det er altså ikke tilstrekkelig med en generell henvisning til undersøkelsesplikt – det må kunne begrunnes at delingen av de aktuelle opplysningene er nødvendig for den pågående undersøkelsen.

Forarbeidene gir begrenset med videre veiledning for hva som ligger bak den doble nødvendighetsvurderingen, og det gis ingen videre anføring på hva som skal til for at opplysninger er nødvendige å dele, eller nødvendige som ledd i de videre undersøkelsene.

Samtidig som delingsadgangen etter § 31 tredje ledd er frivillig og etter sin ordlyd begrenset av det doble nødvendighetskravet, oppstiller loven strenge regler mot å dele opplysninger som omfattes av avsløringsforbudet.

Avsløringsforbudet er inntatt i hvvl. § 28 med følgende ordlyd:

«Rapporteringspliktige, herunder styremedlemmer, ledere, ansatte og andre som utfører oppdrag på vegne av rapporteringspliktige, skal ikke gjøre kunden eller tredjepersoner kjent med undersøkelser, oversendelse av opplysninger til Økokrim eller etterforskning.»

Av Finanstilsynets veileder til hvitvaskingsloven fremgår det at med «tredjepersoner» menes alle som ikke har tjenstlig behov for opplysningene. Videre fremgår det at også opplysninger om at det vurderes å gjennomføre nærmere undersøkelser, samt opplysninger som gjør at personen må forstå at det vil iverksettes nærmere undersøkelser, er ment omfattet av forbudet. Avsløringsforbudet i norsk rett favner altså svært bredt, både i anvendelse og i rekkevidde, selv om enkelte unntak fra forbudet gir en viss delingsadgang i noen tilfeller.

Gitt at hvvl. § 51 tredje ledd åpner for å straffe ansatte med bøter og, i særlige omstendigheter, fengsel i inntil ett år for grovt uaktsomme overtredelser av avsløringsforbudet, er det å forvente at enkelte rapporteringspliktige er tilbakeholdne med å benytte delingsadgangen etter § 31 tredje ledd.

Personvernregelverket

Den skisserte løsningen til Eika og KPMG involverer behandling av personopplysninger, og utfordringene ved disse vil følgelig reguleres av personvernregelverket. Det var derfor en stor fordel å ha Datatilsynet som aktiv deltager. I arbeidsmøtene kom det tydelig frem fra Datatilsynet at Eika og KPMGs løsning vil involvere behandling av personopplysninger, og derfor være regulert av personvernregelverket.

I utgangspunktet er det to typer data som er aktuelt å behandle i de ulike løsningene som Eika og KPMG presenterer. Dette inkluderer:

- **Kundedata**: Dette kan knytte seg til bankkundens personalia, kontaktinformasjon, ID-papirer, informasjon om kundens risikoklasse eller kundetiltak fra tidligere eller annen bank eller informasjon om avvikling av kunden som helhet.
- **Opplysninger knyttet til kundens aktivitet**: Dette kan innebære informasjon om transaksjoner, innlogginger eller andre tekniske indikatorer som kundens IP-adresse.

Kategoriene kan justeres ved behov, slik at det ikke trenger å være alt-eller-ingenting. Transaksjoner kan for visse formål aggregeres opp (eksempelvis totale utenlandsoverføringer gjennom en måned fremfor én og én overføring), og kundeinformasjon kan begrenses (eksempelvis å bruke fylke fremfor postnummer) eller pseudonymiseres. Når man fastsetter innholdet av kategoriene, samt grad av spesifisitet, er det vesentlig at man må foreta en kontinuerlig og faglig begrunnet vurdering av om behandlingen av opplysninger oppfyller det tilsiktede formålet samt i hvilken grad behandlingen av dem har den ønskede effekten.

Det presiseres at selv om dette er aktuelle kategorier av personopplysninger, er listen ikke uttømmende, og de konkrete personopplysningene som skal deles vil måtte spesifiseres. Felles for personopplysningene er at man må ha behandlingsgrunnlag i ett av alternativene i GDPR art. 6 nr. 1. Nødvendigheten av å behandle den enkelte kategori av personopplysninger vil måtte defineres på typetilfellenivå.

Transaksjonshistorikk kan innebære enten direkte eller indirekte behandling av sensitive personopplysninger. Dersom opplysningene omfattes av forordningens definisjon av «særlige kategorier» kreves det behandlingsgrunnlag i GDPR art. 9 nr. 2. Krav til behandlingsgrunnlag er gjennomgått under.

Behandlingsgrunnlag

I prosjektet har vi vurdert hva som kan være rettslig grunnlag for datadeling mellom banker etter personvernregelverket. Personvernforordningen (GDPR) krever at all behandling av personopplysninger har hjemmel i ett av alternativene som følger av GDPR art. 6 nr. 1 bokstav a til f.

Det følger av høringsnotatet til Finanstilsynet at

> *«Etter personvernforordningen artikkel 6 nr. 1 er behandling av personopplysninger bare lovlig når behandlingen kan forankres i ett av behandlingsgrunnlagene angitt i bokstav a til f. Ved deling av personopplysninger mellom finansforetak for formål knyttet til bekjempelse av økonomisk kriminalitet er det særlig aktuelt å vurdere artikkel 6 nr. 1 bokstav c, e og f.»*

Prosjektet er enig i denne uttalelsen fra høringsnotatet. De aktuelle behandlingsgrunnlagene er dermed de som er nevnt i høringsnotatet, bokstav c, e og f som gjelder henholdsvis der den behandlingsansvarlige har en «rettslig forpliktelse», «en oppgave i allmennhetens interesse» eller «berettiget interesse» i behandlingen av personopplysninger.

Etter dagens regelverk foreligger det ikke en «rettslig forpliktelse» til utlevering eller deling av kundeopplysninger i ffl. § 16-2, selv om det foreligger en adgang til deling. Dermed kan dette behandlingsgrunnlaget ikke benyttes.

En må dermed vurdere om det foreligger en «oppgave i allmennhetens interesse» eller en «berettiget interesse» som gir grunnlag for behandling av personopplysninger for å forhindre økonomisk eller annen alvorlig kriminalitet i medhold av GDPR art. 6 nr. 1 bokstav e eller f. Behandling av personopplysninger for å utføre en oppgave i allmennhetens interesse krever at det foreligger et supplerende rettsgrunnlag, jf. art. 6 nr. 3. Datatilsynet har gitt uttrykk for at dette er de to mest relevante rettslige grunnlagene å vurdere i denne sammenhengen.

For særlige kategorier av personopplysninger må det i tillegg foreligge et supplerende behandlingsgrunnlag i art. 9 nr. 2. I utgangspunktet forespeiles det at bankene i begrenset grad vil behandle slike kategorier av personopplysninger, men transaksjonsinformasjon kan eksempelvis avsløre fagforeningsmedlemskap eller helseopplysninger dersom det gis betalinger til en spesifikk fagforening eller transaksjonshistorikken viser legebesøk eller kjøp av apotekvarer. Det kan også forekomme tilfeller der opplysningene er direkte relevante for mistanken, eksempelvis betalinger som viser medlemskap eller donasjon til religiøse organisasjoner eller ekstremistiske foreninger.

Et aktuelt behandlingsgrunnlag etter GDPR art. 9 nr. 2 er alternativ g. Det følger av bestemmelsen at

> *«Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser»* (våre understrekninger)

I forslaget til revidert ffl. § 16-2 og ny § 16-17 i finansforetaksforskriften er det foreslått en uttrykkelig hjemmel for å dele særlige kategorier av personopplysninger når dette er nødvendig for å forebygge eller avdekke økonomisk kriminalitet og annen alvorlig kriminalitet.

Om automatiserte behandlinger

Under sandkasseprosjektet uttrykte tilsynsmyndighetene bekymring for at behandlingen av personopplysninger i denne sammenheng vil være i strid med GDPR art. 22 om automatiserte behandling og profilering. Det følger av artikkelens første ledd at

> *«den registrerte skal ha rett til å ikke være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende»* (våre understrekninger).

Det ble avklart i møtene med Finanstilsynet og Datatilsynet at artikkel 22 ikke vil utgjøre en skranke for datadelingen omtalt her, ettersom behandlingen ikke vil innebære en «*rettsvirkning»* for den registrerte eller *«på tilsvarende måte i betydelig grad påvirker vedkommende»* uten at bankene vil implementere en høy grad av menneskelig involvering ved saksbehandlingen, innrapportering til

Økokrim eller vurdering av avvikling av kundeforhold. Det er dermed kun datadeling for økt informasjonsgrunnlag som automatiseres i de aktuelle scenarioene som sandkasseprosjektet beskriver.

Dataminimeringstiltak

Det følger av GDPR art. 5 nr. 1 bokstav c at man skal sikre ivaretakelse av dataminimering ved behandling av personopplysninger. Som ledd i dette er den pågående nødvendighetsvurderingen som må foretas av bankene.

Datatilsynet presiserte under sandkasseprosjektet at dette må være en kontinuerlig prosess dersom det åpnes for datadeling mellom banker, da en må vurdere hvilke personopplysninger som faktisk er nødvendig for å løse opp i den konkrete mistanken. Rent praktisk kan dette bli løst med å starte opp med ett regelsett for bankene basert på en utfyllende og dokumentert vurdering av nødvendighet for å oppfylle formålet (i personvernrettslig forstand) med delingen, der treffsikkerheten følges opp og evalueres kontinuerlig. Dersom man reelt sett, sitter på eller utveksler unødvendige mengder informasjon må regelen innskrenkes. Dersom man motsetningsvis ser at regelen treffer dårlig fordi man ikke sitter på tilstrekkelig med opplysninger til å oppklare mistanken, kan regelgrunnlaget utvides.

Tilgangsstyring

Et annet risikoreduserende tiltak som ble drøftet i arbeidsmøtene var behovet for tilgangsstyring, slik at det kun var personer i banken med tjenstlig behov for kundeopplysningene som ville ha tilgang til dette. Dette vil ikke være utfordrende å løse på et teknisk eller praktisk plan.

Juridiske vurderinger av fasene i anti-hvitvaskingsarbeidet

De følgende underkapitlene vil etter tur presentere de tre funksjonelle fasene – deteksjon, utredning og kundevurdering – som deler av AHV-arbeidet normalt deles inn i, og mer konkrete juridiske drøftinger opp mot disse.

Første del vil omhandle deteksjon. Dette er prosessene som medfører at det genereres en alarm eller varsling i bankens systemer med en mistanke på en kunde, og vi er derfor forut for fasen hvor undersøkelsesplikten etter hvitvaskingsloven inntrer. Mistanken som avdekkes i fasen kan også gjelde andre former for kriminalitet enn hvitvasking og terrorfinansiering. I fokus her er den elektroniske transaksjonsovervåkningen, hvor et regelsett avgjør når en kunde «alarmeres», altså blir gjenstand for en alarm i systemet. Dette kan være enkle regler som kontantinnskudd over visse grenser, eller smartere regler som ser på avvik fra en forventning basert på statistiske modeller.

Andre del vil omhandle utredning. Dette er prosessene som skjer etter at det er generert en alarm på en kunde. Det vil her gjennomføres en utredning for å vurdere om mistanken som er flagget av deteksjonssystemet er reell. Ofte er utredninger delt inn i faser, med en forundersøkelse som en innledende «triage» og eventuelt videre undersøkelser etter dette. Denne delen vil således inkludere både forundersøkelser hvor man er forut for «nærmere undersøkelser» etter hvvl., og perioden etter dette hvor man er i neste nivå av utredning og følgelig er i «nærmere undersøkelser».

Tredje del vil omhandle kunderisikovurdering. Dette handler om hvordan man totalt sett vurderer risikoen fra en kunde, ofte som resultat av en utredning som i foregående del.

1. Deling innen deteksjon

Problemstilling

Som nevnt i innledningen kan deteksjonsregler være mer eller mindre «smarte». Uansett hvordan reglene designes, er det ønskelig med et mest mulig komplett datagrunnlag å kjøre reglene på. Det er kundens totale finansielle adferd som best indikerer hvorvidt kunden er involvert i økonomisk kriminalitet som bedrageri, hvitvasking eller terrorfinansiering. Samtidig er det en kjensgjerning at kriminelle gjerne har flere bankforhold nettopp for å gjøre det vanskelig å oppdage deres totale aktivitet og se den i riktig sammenheng.

Utfordringen oppstår nettopp når aktivitet som samlet sett ville blitt alarmert i en bank, ikke blir alarmert fordi aktiviteten er fordelt på flere banker – og dermed på flere datasett.

De kriminelle har altså en asymmetri til sin fordel. De har adgang til å spre sin aktivitet uten at bankenes deteksjon har anledning til å spre seg tilsvarende og følge aktiviteten. Prosjektet har derfor ønsket å utforske mulighetene for å se på hvilke datapunkter, og under hvilke omstendigheter, man kan samle på tvers.

Dette er kanskje det mest ambisiøse området i dette sandkasseprosjektet, ettersom det fordrer deling av data *før* mistanke er etablert. Vi har likevel ment det er viktig å ta dette opp med tilsynene i rammene av Meld. St. 15 (2023-2024), «Felles Verdier – Felles Ansvar», hvor det fremgår en ambisjon om å drive felles transaksjonsovervåkning. Å utforske hvordan dette faktisk kunne sett ut i nåværende eller fremtidig lovverk er etter vårt syn viktig for å oppnå målet om en bedre og mer effektiv bekjempelse av økonomisk kriminalitet.

Drøfting av løsning

Et kjennetegn ved denne fasen i arbeidet er at dataene det er snakk om å dele ofte ikke er forbundet med mistanke hos den enkelte bank. Det ligger i sakens natur at deteksjonsfasen handler om å gå fra datapunkter uten mistanke, til å identifisere mistanke basert på ett eller flere datapunkter.

Et tema for samarbeidsmøtene med Finanstilsynet og Datatilsynet var om dagens regelverk åpnet opp for at man kunne dele spesifikke datapunkter til en sentral løsning i deteksjonsfasen, altså før man reelt sett har en mistanke. To relevante eksempler er deling av opplysninger om alle påbegynte kundeonboardinger og enkelte datapunkter knyttet til dette for å avdekke mistenkelig mange samtidige onboardingsforsøk fra samme person; og deling av utvalgte kategorier transaksjonsopplysninger for å se mistenkelige mønstre i disse hos kunder på tvers av banker.

Det ble tidlig etablert at dagens regelverk ikke gir adgang til en «pooling» av eksempelvis transaksjonsdata for felles transaksjonsovervåking for anti-hvitvaskingsformål. All den tid man etter gjeldende praksis ikke vil evne å avdekke den mistenkelige adferden, vil bankene ikke ha hjemmel i ffl. § 13-21 som følge av bedrageribekjempelse eller hjemmel i hvvl. § 31 tredje ledd til å dele kundeinformasjon. Dette forutsetter at ikke noen av kundens enkeltaktiviteter i seg selv utløser alarm og undersøkelsesplikt.

Tilsvarende vil heller ikke dagens hjemmel i ffl. § 16-2 gi en legitim adgang, ettersom en slik deling ville falt utenfor lovens krav til å kun dele ved «særlige tilfeller» og ved fattede styrevedtak. Slike vedtak måtte uansett vært konkretiserte nok, og kan dermed ikke hjemle en helt generell datadelingsadgang etter dagens regelverk. Man kan i teorien se for seg en adgang etter dagens ffl. § 16-2 hvor man angir et meget snevert typetilfelle, godkjent gjennom styrevedtak. Finanstilsynet anså imidlertid dette å tøye intensjonen i gjeldende regelverk. Her vil det til gjengjeld åpne seg muligheter i det foreslåtte lovverket, omtalt avslutningsvis i rapporten.

Datatilsynet anså at en form for teknisk deling med samling av data mellom alliansebankene i deteksjonsfasen på enkelte, forhåndsdefinerte datapunkter knyttet til eksempelet med et mistenkelig stort antall samtidige onboardinger potensielt kunne være lovlig etter personvernlovgivningen under gitte forutsetninger. Én forutsetning er at det i tilfellet må være begrenset til det absolutt nødvendige av personopplysninger for å detektere mulig kriminalitet. Videre er det av betydning at formålet om å motvirke eller forhindre økonomisk eller annen alvorlig kriminalitet er et formål av betydelig allmenn interesse, samtidig som personverninngrepet presumtivt vil være av en mindre inngripende karakter for de registrerte forutsatt at delingen begrenses til det som er absolutt nødvendig. Slik teknisk deling av opplysninger i deteksjonsfasen vil imidlertid først være aktuelt etter at de foreslåtte lovendringer i finansforetaksloven eventuelt trer i kraft. Det ble presisert av Datatilsynet at vurderingen knyttet seg til deling av grunnleggende kundeinformasjon. Deling av eksempelvis transaksjonsdata vil derimot anses mye mer inngripende, men dette ble ikke drøftet nærmere i sandkassen.

Datatilsynet fremhevet også andre forutsetninger, som at det etter GDPR og personopplysningsloven kreves gode rutiner for lagringstid, sletting og tilgangsstyring for at samling av data på tvers av juridiske entiteter kan være lovlig etter dette regelverket. Videre kreves det kontinuerlige nødvendighetsvurderinger av delingen, omfanget og behandlingen av personopplysninger, inkludert hvor lenge opplysninger måtte behandles for å faktisk kunne identifisere mistenkelig adferd i kundeforhold. Dette innebærer eksempelvis å lage rutiner for hvilket avgrenset tidsrom man skal behandle opplysninger i, samt en vurdering av hvilke datapunkter som må benyttes i deteksjonsfasen. Behandling av unødvendige mengder data må unngås, samtidig som datapunktene må være tilstrekkelig til å faktisk gi en tilstrekkelig klar output. Videre er det viktig å ha på plass mekanismer for å ivareta de registrertes rettigheter.

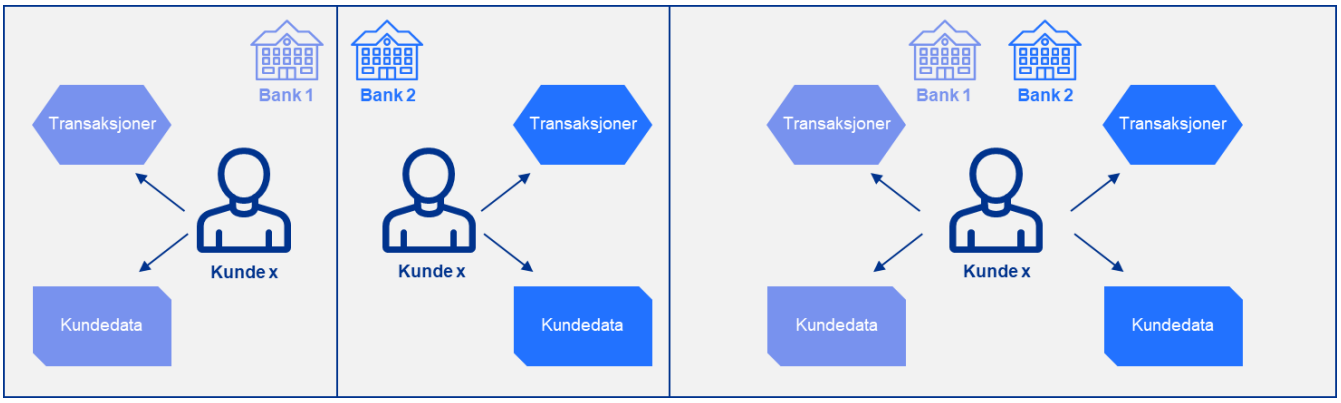
2. Deling innen utredning

Problemstilling

Når en transaksjonsalarm er utløst, starter en utredningsfase i banken hvor alarmen har gått. Vi bruker her bevisst ikke «nærmere undersøkelser» som begrep for å beskrive fasen som helhet. «Nærmere undersøkelser» er, som nevnt over, et begrep i hvitvaskingsloven som hjemler deling.

Som oftest vil banker operere med en innledende undersøkelse/forundersøkelse hvor man luker ut alarmer som åpenbart ikke når terskelen for undersøkelsesplikten, før saker «eskaleres» til full utredning. Vi ønsker her å inkludere både fasen før og etter utløsning av undersøkelsesplikten i det vi kaller «utredning» nettopp for å kunne inkludere denne overgangen i eksempler og løsningsforslag under.

En utredning inneholder gjerne analyser og vurderinger av kunden, transaksjonshistorikk og kundens formål og tilsiktede art ved kundeforholdet. I motsetning til i del 1 ser vi her på et tilfelle hvor en viss mistanke allerede er identifisert, typisk gjennom en alarm fra transaksjonsovervåkningen. Denne delen vil fokusere på adganger etter hvitvaskingsloven, ettersom det her finnes en eksplisitt adgang til deling.



Figur 1: Kundeaktivitet spredd over flere banker slik det ser ut for utredere i dag (venstre) og ønsket situasjon (høyre)

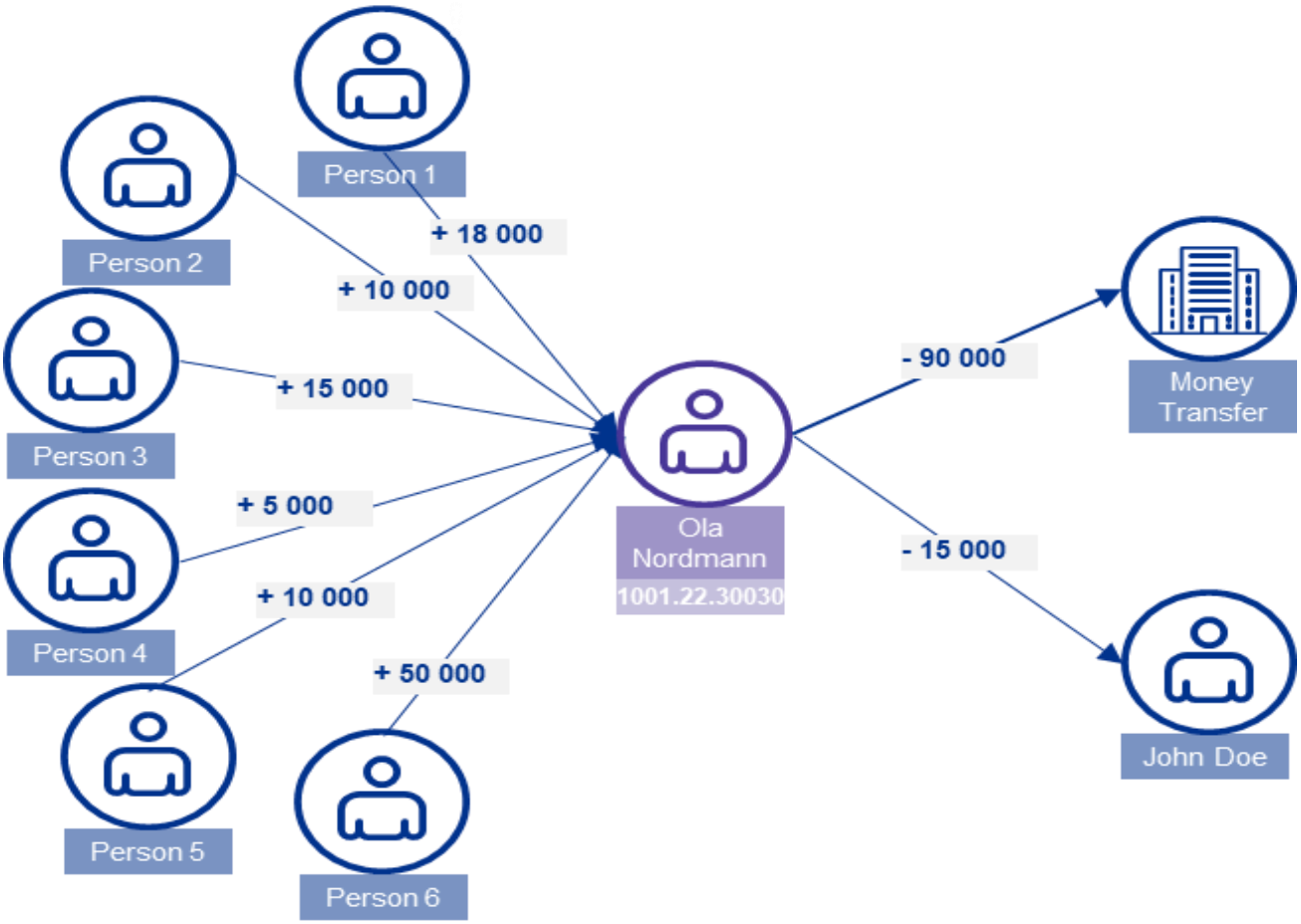
Utfordringen er her at alarmer kan feilvurderes dersom man har ufullstendige opplysninger. Legitime transaksjoner kan ende opp med å rapporteres til Økokrim dersom man ser et for smalt bilde og ikke en helhet hvor transaksjonene hadde fremstått mindre mistenkelige. På den annen side vil man også kunne unnlate å rapportere reelle kriminelle forhold, der hvor en helhet hadde bidratt til å kaste lys over et større mønster. Vi har en hypotese om at disse svakhetene særlig kommer de avanserte og profesjonelle hvitvaskerne til gode, en kategori hvitvaskere som varsles om fra både norske myndigheter og Europol. I tillegg vanskeliggjør det Økokrim sitt arbeid ved at de får flere mindre og fragmenterte rapporteringer.

Prosjektet har derfor ønsket å utforske hvorvidt man kan etablere en løsning hvor utredere i Eika Gruppen eller -banker kan trekke inn data fra andre banker i alliansen der det er relevant for nærmere undersøkelser i deres egen bank.

Drøfting av løsning

Startpunktet for eksempelet og prosessen er at en utreder åpner en alarm til forundersøkelse. I dette steget ser utreder kun data fra banken hvor alarmen er generert i utgangspunktet.

Utreder gjør så en vurdering av om mistanken er åpenbart grunnløs, eller om alarmen bør gå til nærmere undersøkelser. Dersom alarmen eskaleres videre fra forundersøkelser, får utreder muligheten til å hente ytterligere opplysninger på kunden eller motparter fra andre banker i Eika Gruppen.

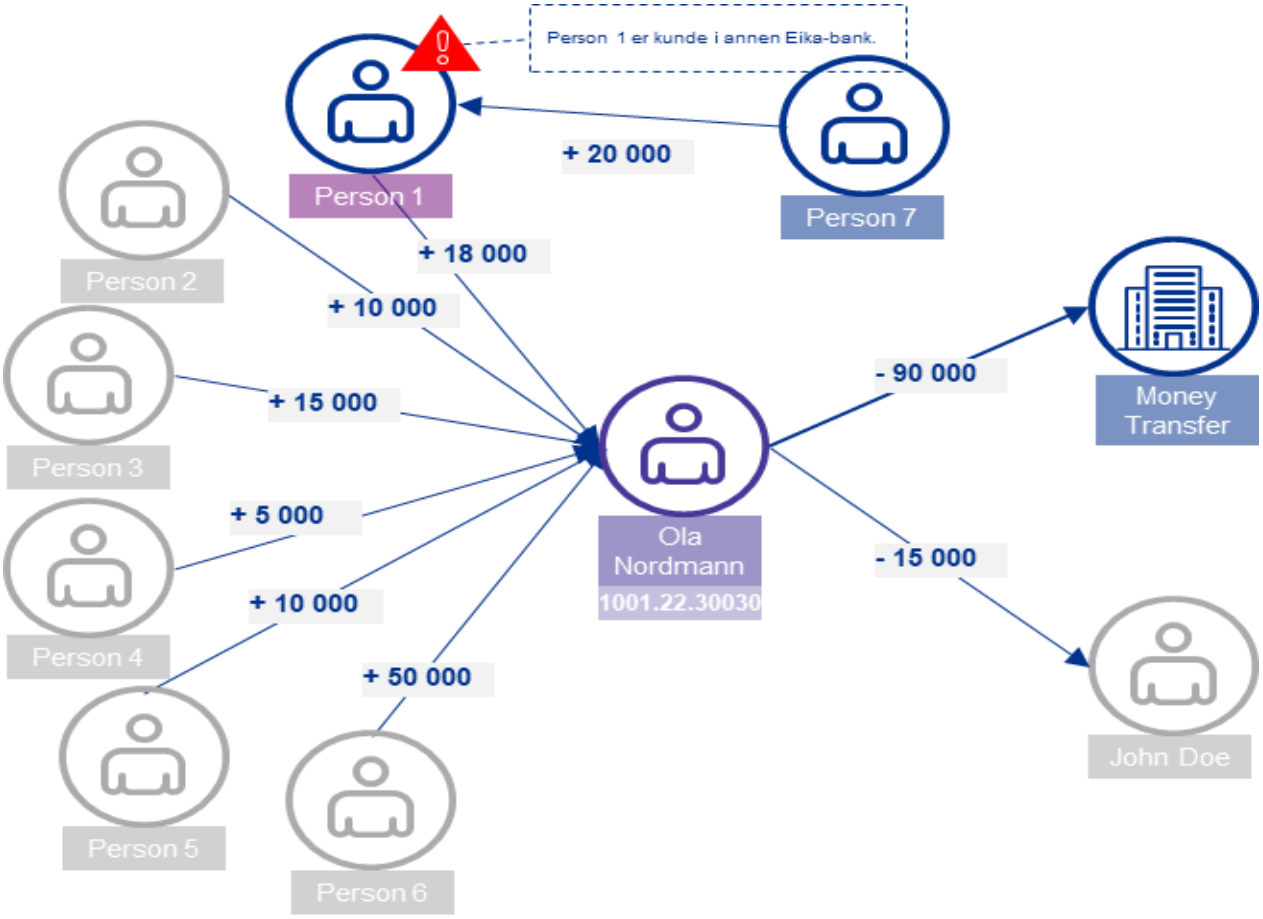


Figur 2: Transaksjonsoversikt i utredning, kun egne data

Ved å beholde dette forundersøkelsessteget før man får mulighet til å utveksle opplysninger, sikrer man å bare utveksle opplysninger der man er i en kvalifisert fase av nærmere undersøkelser i henhold til hvitvaskingsloven § 31 tredje ledd.

Etter at en utreder har eskalert saken, får vedkommende se hvilke av nodene i transaksjonsoversikten det finnes data på i andre banker i Eika. Deretter kan utreder velge å innhente data på disse fra de aktuelle bankene. Utreder må også spesifisere hvilke typer opplysninger man ønsker utlevert, fra en standardisert liste med kategorier av opplysninger. Ved å både måtte aktivt velge *å utveksle* opplysninger, og velge *hvilke sett med opplysninger* som utveksles, vurderer KPMG og Eika at det doble nødvendighetskravet i hvitvaskingsloven ivaretas.

Samtidig foreligger det et juridisk krav om at løsningen overholder dataminimeringsprinsippet. Datatilsynet anbefalte at man ber om data inkrementelt, fremfor en alt-eller-ingenting-løsning. Oppsettet med å be om enkeltkategorier av data gjør at dette naturlig ivaretas.



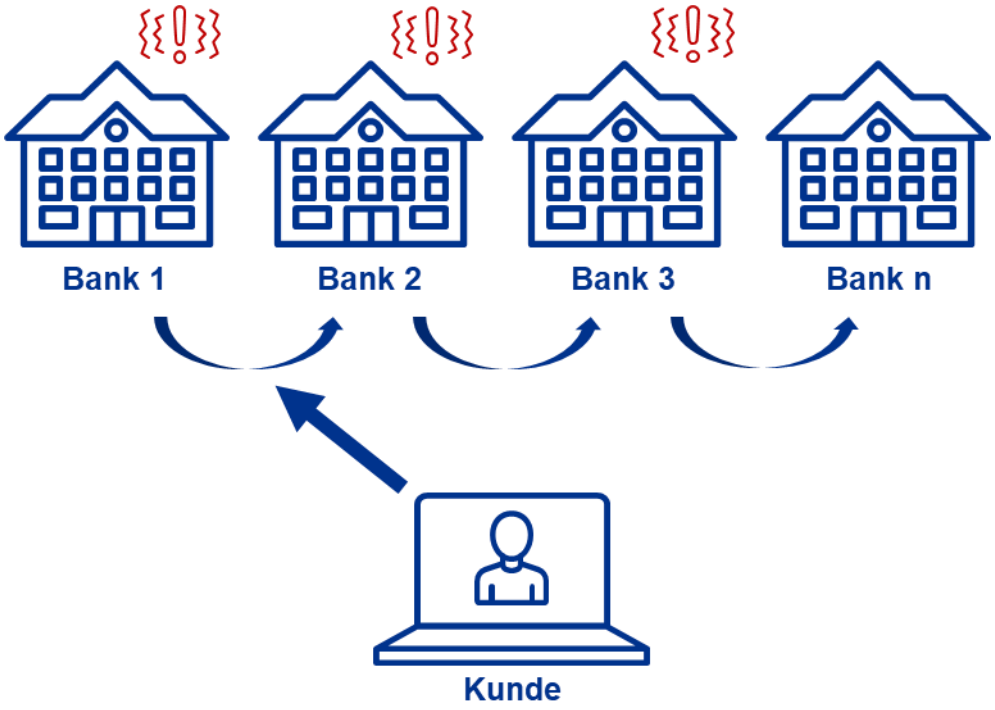
Figur 3: Transaksjonsoversikt med deling

Opplysningene utveksles så umiddelbart, uten godkjenning i hvert enkelt tilfelle av avsenderbank. Dette muliggjøres gjennom et felles avtaleverk som gir forutgående godkjenning til dette. Finanstilsynet kunne ikke se noe hinder for å ha et slikt avtaleverk.

3. Deling innen kundevurdering

Problemstilling

Som nevnt over er det velkjent at kriminelle drar på «bankshopping» med mange parallelle kundeforhold for å spre aktivitet. Tilsvarende er vi kjent med at kriminelle hopper fra bank til bank over tid, ettersom banker fatter mistanke ved deres aktivitet og begynner å stille nærgående spørsmål. I både samtidig og suksessiv «bankshopping» vil det være avgjørende om en bank kan få raskt tilgang på røde flagg eller vurderinger fra andre banker på samme kunde.



Figur 4: "Bankshopping" over tid

Et eksempel vil være at en bank oppdager at en kunde er involvert i bedrageri. I slike tilfeller vil det være rimelig å anta at denne kunden også har kundeforhold i andre banker, ettersom kunden er forberedt på at banken fatter mistanke eller avslutter kundeforholdet etter kort tid. Minst like aktuelt er når banken oppdager et bedrageri*offer*. Ved sosial manipulasjon vil svindlere kunne overbevise ofrene sine i stor nok grad til at ofrene selv ønsker å omgå bankenes svindeldeteksjon, eksempelvis ved å overføre midler til en annen bank, og så betale bedragerne derfra.

Drøfting av løsning

En løsning er å sørge for utveksling av informasjon av kunder som er flaggede. Merk at dette skiller seg fra løsningsforslaget i del 1. Der var temaet deling av ikke-mistenkte kunders informasjon for å komme til mistanke. Her er temaet deling av en allerede identifisert og utredet/etablert mistanke, enten innen hvitvasking eller annen økonomisk kriminalitet. Dette kan være rutinemessig like mye som hendelsesutløst.

Vi ser for oss en løsning hvor en bank som får en tilstrekkelig sterk mistanke til en kunde, flagger denne i et sentralt register. Når en kunde starter et kundeetableringsløp i en annen bank, eller kunden skal revurderes av en annen bank, gjøres det oppslag mot det sentrale registeret. Dersom det er treff på den aktuelle kunden, hentes relevante data fra banken eller bankene som har den

konkrete informasjonen. Dette vil typisk handle om mistankegrunnlag, kategori av mistanke/rolle og grunnleggende informasjon om kundeforholdet.

Det er her verdt å påpeke at løsningen ikke handler om å nekte kunder bankforbindelser, men å sørge for at utvalgte kunder ikke nødvendigvis får starte med «blanke ark» i gjentatte bankforhold og slik utnytte dette til å begå kriminalitet over tid.

Grunnet de begrensede hjemlene for deling av informasjon i hvitvaskingsloven, herunder unntakene fra avsløringsforbudet i hvitvaskingsloven § 28, vil det som hovedregel ikke være anledning til å dele informasjon om at kunder er MT-rapporterte på måten som skisseres i løsningen. Eika og KPMG mener dette er en svakhet som ikke fremmer formålet i hvitvaskingsloven, dersom det er en høyere terskel for å utveksle opplysninger om kunder som er flagget for mulig hvitvasking enn kunder som er flagget for annen økonomisk kriminalitet.

Avhengig av typetilfellet, kan det være en begrenset adgang til å dele informasjon i denne løsningen etter dagens ffl. § 16-2, forutsatt blant annet at man har et styrevedtak på deling, og at det er snakk om et klart avgrenset typetilfelle. Det ble imidlertid bemerket at dette ville være en bruk av bestemmelsen som ikke er tilsiktet av lovgiver, og det vil dermed være en regulatorisk risiko involvert i å forsøke å benytte bestemmelsen på denne måten. Med de foreslåtte endringene til § 16-2 vil dette mulighetsrommet bli betydelig større. Ved å fjerne kravet om styrevedtak og særlige tilfeller legger man opp til en mer systematisk og skalerbar deling enn hva dagens bestemmelse åpner for. Vi vurderer at løsningen slik vi har skissert den her vil bli tillatt dersom endringene innføres som foreslått.

Det bør også nevnes at det allerede i dag kan være en begrenset anledning til å utveksle informasjon etter § 13-21 for å forebygge, etterforske eller avsløre *betalingsbedragerier*. Deling begrenser seg dermed til betalingsbedragerier og ikke alle typer økonomisk kriminalitet.

Oppsummering og konsekvenser for videre arbeid

Basert på de ovenstående vurderingene som Eika og KPMG har gjort med veiledning fra Datatilsynet og Finanstilsynet, ser vi et utvidet handlingsrom etter eksisterende lovverk, samtidig som ytterligere muligheter tydelig åpner seg med foreslåtte endringer i finansforetaksloven.

Under vil vi først oppsummere hvilke muligheter vi ser i dagens lovverk, da dette er primærformålet med sandkasseprosjektene. Like fullt er de foreslåtte endringene i finansforetaksloven i så stor grad i kjernen av de diskuterte problemstillingene at disse også må adresseres.

Vurderingene under er gjengitt slik de fremstod etter diskusjon i arbeidsmøtene med tilsynene. Slik sett kan de sies å reflektere en felles enighet om hvor handlingsrommet ligger prinsipielt sett. Like fullt kan ikke vurderingene tas som et endelig godkjentstempel fra tilsynene for fremtidige tekniske innretninger. Eksemplene som er diskutert over er skjematiske og forenklede. En praktisk, teknisk løsning ville nødvendigvis innebåret en rekke nyanser og problemstillinger som ikke har blitt diskutert eller er løftet her. En fremtidig løsning vil derfor kreve mer inngående vurderinger som følgelig tilsynene ikke har tatt stilling til her.

Hvilket økt mulighetsrom ser vi med eksisterende lovverk?

Innen **deteksjon** har prosjektet vurdert at det er svært begrenset adgang til å dele data *før* mistanke er etablert, i den hensikt å avdekke mistanke (fase 1). Dette er fordi dette ofte ikke tilfredsstiller nødvendighetskravene slik de står i lovverket.

Personvernregelverket er i utgangspunktet ikke til hinder for at det innføres en nasjonal hjemmel som innenfor visse rammer gir adgang til å dele opplysninger før mistanken er konkretisert, sett opp mot den allmenne interessen man har i å motvirke økonomisk eller annen alvorlig kriminalitet. Sett opp mot formålet kan dermed behandlingen legitimeres under forutsetning av at man ikke går utover rammene til personvernlovgivningen når det kommer til for eksempel prinsipper om

forholdsmessighet, dataminimering og formålsbegrensning. En forutsetning er altså at en eventuell hjemmel må være tilstrekkelig begrunnet, klar og ledsaget av nødvendige rettssikkerhetsgarantier for de registrerte.

Etter gjeldende rett setter imidlertid finansforetaksloven og hvitvaskingsloven begrensinger i delingsadgangen, da de krever en konkretisert mistanke før deling kan skje. Dette gjør at dagens regelverk ikke åpner for å drive felles deteksjon innenfor AHV-arbeid eller på andre former for økonomisk kriminalitet.

Det er imidlertid funnet et handlingsrom i **utredningsfasen** av en AHV-utredning (fase 2). Det er anledning i hvitvaskingsloven til å utveksle nødvendige opplysninger når det er nødvendig for å avklare mistanke i nærmere undersøkelser. Under forutsetning av at man har hjemmel til datadeling etter hvitvaskingsloven, vil ikke GDPR være en begrensende faktor for behandlingen, så lenge man har behandlingsgrunnlag og oppfyller de andre pliktene i GDPR ellers. Eika Gruppen kan etablere et system hvor utreder i én bank kan trekke inn data fra andre banker i alliansen som deltar i systemet. Eika og KPMG anser at lovkravene for deling av kundeinformasjon etter hvitvaskingsloven ivaretas ved at deling kun gjøres i tilfeller hvor man tenker at ytterligere data vil være nødvendig for å vurdere mistanken, og man velger kun å utveksle relevante opplysninger. Rettidighet forbedres vesentlig ved at utredere kan innhente opplysninger uten forsinkelse basert på en forutgående generell godkjenning fra avsenderbankene i et felles avtaleverk.

Avslutningsvis er det identifisert et knapt handlingsrom i **kunderisikovurderinger** (fase 3) etter dagens regelverk basert på typetilfelleadgang i finansforetakslovens §16-2 og § 13-21. Løsningen vil her være at Eika ivaretar et sentralt register over kunder med identifisert mistenkelig aktivitet. Dette vil fortrinnsvis være bedragerimistanke, ettersom hvitvaskingsloven setter begrensninger for deling av etablert mistanke om hvitvasking (hvilket gjerne er synonymt med innrapportering omfattet av avsløringsforbudet).

Hvilket økt mulighetsrom ser vi med nytt lovverk?

I det nye regelverket ser vi et betydelig forbedret spillerom i **deteksjonsfasen**. Eksempelet over med «pooling» av informasjon om kundeetableringer på tvers av Eika-bankene for å identifisere åpenbare bedrageriintensjoner vil bli tillatt etter de foreslåtte endringene i ffl § 16-2. Dette vil forbedre Eika-bankenes evne til å hindre misbruk av alliansen til kriminelle forhold.

Et steg videre ser vi også for oss at en variant av vårt andre eksempel med «pooling» av visse transaksjonsopplysninger vil bli tillatt med nevnte lovendringer, om de innføres som foreslått. Det er her viktig å presisere at det ikke er snakk om å samle alle transaksjoner ukritisk, men å gjøre en faglig vurdering av hvilke konkrete transaksjonstyper som er nødvendig for å avdekke definerte kriminalitetsformer/typologier. Dette vil være mer inngripende deling av personopplysninger enn ren kundeinformasjon, som også vil fordre ytterligere personvernvurderinger. Dette er en ambisiøs løsning som ikke ble diskutert med Datatilsynet, men samtidig tar vi til etterretning de ambisjonene regjeringen selv legger for bekjempelsen av økonomisk kriminalitet med ønsket om felles transaksjonsovervåkning i st. mld. 15 av 2023-2024. Vi legger også til grunn at Finanstilsynet i sitt forslag til lovendring i ffl. har ønsket å følge opp signalene fra stortingsmeldingen.

I en **utredningsfase** på AHV-området eksisterer det som nevnt over allerede i dag et uutnyttet handlingsrom innenfor hvitvaskingsloven. Prosjektet har derfor i mindre grad fokusert på konsekvensene av de foreslåtte regelverksendringene på denne fasen. Vi ser likevel for oss at regelverket slik det er foreslått potensielt vil gi noen ytterligere adganger. For det første er det relevant å vurdere om det vil bli anledning til en grad av informasjonsdeling også i fasen før man er definert innenfor hvitvaskingslovens «nærmere undersøkelser». I forlengelsen av dette kan det vurderes om løsningsforslaget vi har presentert for utredningsfasen innen AHV også kunne vært utvidet til å gjelde utredning av annen økonomisk kriminalitet, og om det foreslåtte regelverket vil gi

en adgang for annen økonomisk kriminalitet likere den som eksisterer for deling av informasjon i «nærmere undersøkelser» på AHV i dag.

For **kundevurderinger** åpnes mulighetsrommet tydeligere for deling av etablerte mistanker mot kunder. Løsningen skissert i del 3, med et sentralt register for å dele etablerte mistanker eller røde flagg på kunder mellom banker, blir tydeligere tillatt. Med også GDPR-vurderingene positive vil dette være en nyttig løsning for Eika Gruppen i å sørge for at man ikke uten videre får starte på «ny frisk» ved hver nye bank man etablerer seg i dersom man driver med økonomisk kriminalitet.

Refleksjoner rundt videre arbeid og lovutvikling

Dersom de foreslåtte endringene til finansforetaksloven blir implementert slik de nå foreligger, vil det åpne for at finansforetak i større grad enn i dag kan dele data for å bekjempe økonomisk kriminalitet. Samtidig vil avsløringsforbudet i hvitvaskingsloven fortsatt være en begrensende faktor ved deling av data i situasjoner som omfattes av avsløringsforbudet. Til tross for at hvitvaskingsområdet har hatt betydelig politisk og samfunnsøkonomisk oppmerksomhet det siste tiåret, vil resultatet her slik vi ser det bli at datadeling med hjemmel i hvitvaskingsloven blir mer begrenset enn datadeling knyttet til annen økonomisk kriminalitet, hvor deling kan skje etter ny § 16-2 i finansforetaksloven. Vi har vanskelig for å se at dette er en tilsiktet eller ønskelig utvikling, og vi håper at den norske implementeringen av den nye «AML-pakken» vil bidra til å løse, i alle fall deler av, denne utfordringen.

Vi ble imidlertid tidlig informert om at endringer i datadelingsadgang etter hvitvaskingsloven skulle holdes utenfor prosjektet, nettopp på grunn av den kommende «AML-pakken». Vi har derfor ikke vurdert denne problemstillingen nærmere. KPMG mener likevel det er viktig å påpeke at dagens regulering av deling av data mellom banker etter hvitvaskingsloven i praksis kan hindre en effektiv bekjempelse av hvitvasking, sammenlignet med andre former for økonomisk kriminalitet som vil omfattes av ny § 16-2.

Det er videre vår oppfatning at det i et større bilde vil være nødvendig å bevege seg mot en tilstand med mer integrerte samarbeid mellom foretak (og myndighetene) for å effektivt avdekke økonomisk kriminalitet. Den silobaserte tilnærmingen som er praksis i dag, skaper ineffektive systemer og smutthull for kriminelle. Vi ser på ambisjonen om felles transaksjonsovervåkning fra ovennevnte stortingsmelding som positivt og et sentralt punkt å utvikle videre i lovarbeid. Dette ville i våre øyne skapt bedre kriminalitetsbekjempelse, bedre sporbarhet i prosesser og beslutninger, et mer effektivt bankvesen og i realiteten bedre personvern og informasjonssikkerhet. Dette er en diskusjon vi gjerne fortsetter med tilsynene.

Vi vil også trekke frem at vi opplevde meget gode diskusjoner rundt det nye foreslåtte regelverket i ffl. med tilsynene, og at Finanstilsynet har tatt til seg samfunnsproblemet og ambisjonene lagt frem av regjeringen i arbeidet med lovendringene. Vi ønsker å oppfordre Finanstilsynet til å sørge for god kommunikasjon til finansforetakene rundt hva som har vært den intenderte utviklingen med det foreslåtte regelverket. Innenfor dette regelverket må man regne med at usikkerhet rundt tolkning vil føre til tilbakeholdenhet og følgelig risikere at ikke handlingsrommet blir utnyttet maksimalt. Det vil særlig innledningsvis, før praksis etableres, være verdifullt med tydelighet fra Finanstilsynet på dette.

Appendiks – Innspill til lovendringer i Finansforetaksloven

Innledning

Mellom andre og tredje workshop kom Finanstilsynet med et høringsnotat som presenterte forslag til ny hjemmel i finansforetaksloven § 16-2 med tilhørende forskriftsendringer for å utvide rammene for datadeling i arbeidet mot økonomisk og annen alvorlig kriminalitet. Den tredje workshopen med begge tilsynene bestod dermed i stor grad med å etterspørre avklaringer som høringsnotatet reiste, samt å fremme praktiske innspill. Under følger innspill og avklaringer som fremkom av møtet. Formålet med å trekke dem frem er å synliggjøre vurderinger som er gjennomført samt bekrefte Finanstilsynets hensikt med høringsuttalelsen, og å presisere enkelte momenter som ikke var påtenkt ved publiseringen av høringsuttalelsen. Høringsfristen var 14. november 2025, men vi ønsker om komme med noen av betraktningene som ble presentert i siste workshop, som også kan tjene til avklaringer i det videre arbeidet med utarbeidelsen av lovforslaget.

Utlevering av opplysninger i god tro

Til tredje workshop reiste KPMG spørsmålet om hva som ville kunne være konsekvensene av at det deles opplysninger som i etterkant viser seg at ikke var «*nødvendig for å forebygge eller avdekke økonomisk kriminalitet og annen alvorlig kriminalitet*» slik ordlyden i foreslått ny § 16-2 fjerde ledd legger opp til. Dersom slik deling kan anses å utgjøre brudd på personvernregler er det risiko for at finansforetakene vil vise tilbakeholdenhet mot å dele informasjon med mindre det foreligger en kvalifisert mistanke om at delingen vil være «nødvendig». Da ordlyden i forslaget er utformet svært likt som den lite benyttede delingsadgangen i hvvl. § 31 tredje ledd, anser KPMG det som mulig at den foreslåtte nye § 16-2 fjerde ledd kan bli tilsvarende lite benyttet.

Datatilsynet forklarte i den anledning at det ikke alltid vil være i strid med dataminimeringsprinsippet å behandle personopplysninger som det i etterkant viser seg at likevel ikke var nødvendige for formålet. I denne sammenhengen er det relevant å se hen til om utvalget av opplysningstyper er tilfeldig eller om opplysningstypen ble valgt ut på bakgrunn av en saklig og legitim antagelse om opplysningenes relevans for formålet. Det er også relevant å se hen til hvilke systemer som er satt opp for å kontrollere effekt og avdekke opplysningstyper som ikke har den tilsiktede effekten. KPMG vurderer det likevel som positivt om det inntas en eksplisitt ordlyd om at deling i god tro ikke innebærer brudd på taushetsplikten, slik det er i hvvl. § 26 fjerde ledd.

Det følger av hvvl. § 26 fjerde ledd at

> *«Oversendelse av opplysninger til Økokrim i god tro medfører ikke brudd på taushetsplikt og gir ikke grunnlag for erstatningsansvar eller straffansvar, med mindre det foreligger grov uaktsomhet.» (vår understrekning)*

En lignende ordlyd vil kunne trygge finansforetakene og dermed tilrettelegge for en mer utstrakt bruk av en delingsadgang som myndighetene mener skal benyttes.

Strenger nødvendighetskrav

Det følger av punkt 4.5 i høringsnotatet til Finanstilsynet at

> *«Bokstav f åpner for å behandle personopplysninger når behandlingen er nødvendig for formål knyttet til de berettigede interessene hos den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn. Fortalepunkt 47 i personvernforordningen sier at behandling av personopplysninger som er strengt nødvendige for å forebygge bedrageri utgjør en berettiget interesse for den berørte behandlingsansvarlige.» (vår understrekning)*

Det ble bemerket at ordlyden til fortalepunktet legger opp til en strengere nødvendighetsvurdering enn som følger av henholdsvis hvvl. § 31 tredje ledd, ffl. § 16-2 og GDPR art. 5 bokstav c jf. ordlyden av strengt nødvendig.

Det ble presisert av både Datatilsynet og Finanstilsynet at henvisningen til fortalepunktet ikke skal forstås som en strengere anvendelse av nødvendighetskravet der berettiget interesse benyttes som behandlingsgrunnlag. Det vil alltid være tale om det alminnelige nødvendighetsvilkåret som følger av de omtalte lovene og reguleringene.

Presisering av formålsangivelsen

Videre følger det av punkt 5.2 i høringsnotatet til Finanstilsynet at

> *«Formålsangivelsen skal både sikre at det ikke utleveres taushetsbelagte opplysninger og personopplysninger for andre formål enn det hjemmelsgrunnlaget åpner for, og at det ikke utleveres andre eller et større omfang av opplysninger enn det som er nødvendig for å oppnå formålet. I dette ligger det først og fremst at opplysningene kun skal brukes til, og skal være relevante, for dette formålet. Men like viktig er det at den som mottar opplysningene i medhold av denne utleveringsadgangen, ikke bruker opplysningene til andre formål enn det de er utlevert for.» (vår understrekning)*

I den tredje workshopen ble det stilt spørsmål om hvor spesifikke Finanstilsynet hadde til hensikt å være når det kom til formålsangivelsen for det opplysningene var utlevert for. Dette ble eksemplifisert om det var tilstrekkelig å henvise til økonomisk kriminalitet generelt, eller om primærforbrytelsen måtte spesifiseres, herunder om formålet med utleveringen konkret var å forhindre svindel, bedrageri eller hvitvasking. Finanstilsynet oppklarte i møtet at det kan gis som en generell formålsangivelse. Det er ikke nødvendig å presisere primærforbrytelsen som danner grunnlaget for den enkelte mistanken om økonomisk eller annen alvorlig kriminalitet. Finanstilsynet ga videre klart uttrykk for at foreslått ny § 16-2 ikke skal innebære noe krav om å vurdere om deling av opplysninger gjøres for å «forebygge *eller* avdekke» (vår understrekning) den økonomiske kriminaliteten, som sådan. Dette kan imidlertid stille seg annerledes dersom avsenderen har ment å begrense bruken til forebygging eller avdekking, men det er altså ikke et krav.

Presisering av anvendelsesområdet til GDPR art. 6 nr. 1 bokstav c

Høringsnotatet presenterer en rekke aktuelle behandlingsgrunnlag, herunder GDPR art. 6 nr. 1 bokstav c. Det er fastsatt i bestemmelsen at behandling av personopplysninger er lovlig når *«behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige»* (vår understrekning). Henvisningen til «*rettslig forpliktelse*» tilsier at det må foreligge et supplerende rettsgrunnlag i enten nasjonal eller unionens rett, som pålegger den behandlingsansvarlige å behandle personopplysningene.

I høringsnotatet side 28 beskrives forslaget om en ny ffl. § 16-2 slik

> *«Forslaget vil medføre adgang, men ikke plikt, til økt informasjonsdeling som igjen vil kunne medføre at alvorlige bedragerier og annen økonomisk kriminalitet avdekkes og forhindres i større grad enn i dag, noe som vil redusere både finansforetakenes og kundenes økonomiske tap og innebære besparelser for samfunnet.» (vår understrekning)*

Det ble avklart at i lys av dette at GDPR art. 6 nr. 1 bokstav c ikke vil utgjøre et lovlig behandlingsgrunnlag for informasjonsdeling.

Presisering av trykkfeil

Ved inkurie har det kommet en trykkfeil i forslaget til ny forskrift. I forslaget til endringer i finansforetaksforskriften § 16-17 første ledd er det foreslått følgende

«*Opplysninger som kan utleveres i medhold av finansforetaksloven § 16-2 fjerde ledd, og bestemmelser gitt i medhold av denne, kan også omfatte opplysninger innhentet gjennom kundetiltak etter hvitvaskingsloven og personopplysninger nevnt i personvernforordningen §§ 9 og 10.»* (våre understrekninger)

Forslaget bes rettet til

«*Opplysninger som kan utleveres i medhold av finansforetaksloven § 16-2 fjerde ledd, og bestemmelser gitt i medhold av denne, kan også omfatte opplysninger innhentet gjennom kundetiltak etter hvitvaskingsloven og personopplysninger nevnt i personvernforordningen artikkel 9 og 10.*» (våre understrekninger)