FNH

Sparebankforeningen
The Norwegian Savings Banks Association

Justis- og politidepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref.	Deres brev	Vår ref.	Dato
200904400 ES HAJ/mk	03.07.2009	09-500 FNH 200000331 Spf	28.10.2009

Høring - etterkontroll av personopplysningsloven

Finansnæringens Hovedorganisasjon (FNH) og Sparebankforeningen i Norge viser til Justisdepartementets høringsbrev 3. juli 2009 om etterkontroll av personopplysningsloven av 14. april 2000 nr. 31 (POL). Loven gjennomførte i sin tid EUs personverndirektiv (95/46/EF).

Det er et meget omfattende materiale som er sendt på høring. Problemstillingene er av prinsipiell karakter som griper inn i både strukturmessige, materielle og prosessuelle forhold i loven og personopplysningsforskriften (POF). Av kapasitetsmessige grunner har vi i høringsuttalelsen nedenfor måttet gjøre et utplukk av de mest aktuelle problemstillinger for finansbedriftene.

FNH og Sparebankforeningens hovedsynspunkter kan sammenfattes i følgende punkter:

- Vi fraråder radikale endringer i personopplysningsloven med bl.a. oppdeling i primære og sekundære behandlingsgrunnlag, men kan støtte enkeltelementer fra Schartum/Bygrave (2006) som omtalt nedenfor.
- POL §§ 8-11 med krav til behandlingsgrunnlag, formål og relevans bør etter vår mening opprettholdes og videreføres som i dag.
- Det bør presiseres i POL § 8 at ikke-sensitive personopplysninger også kan behandles dersom det er nødvendig for at behandlingsansvarlig skal kunne fastsette, gjøre gjeldende eller forsvare et rettskrav eller oppfylle en rettslig forpliktelse.
- Vi støtter forslaget om at det i POL inntas en presiserende bestemmelse om at personopplysninger kan behandles dersom etterlevelse av lovgivning gjør det nødvendig at opplysningene blir behandlet.

Postboks 2473 Solli
0202 Oslo
Tlf. 23 28 42 00
Fax. 23 28 42 01
Finansnæringens Hovedorganisasjon: NO 981 423 682
Finansnæringens Servicekontor: NO 969 000 938

Postboks 6772 St. Olavs plass
0130 Oslo
Tlf. 22 11 00 75
Fax. 22 36 25 33
Sparebankforeningen i Norge: NO 971 531 045
Sparebankforeningens Servicekontor: NO 971 526 610

- De særlige konsesjonsreglene for forsikringsselskaper, banker og finansinstitusjoner etter POF §§ 7-2 og 7-3 bør etter vår mening endres for å klargjøre konsesjonsområdet, herunder hvilke behandlinger som er konsesjonspliktige.
- Ordningen med standardkonsesjoner for finansbedrifter bør videreføres for de vanligste behandlingsformene.

I. Generelle kommentarer

FNH og Sparebankforeningen vil sterkt anbefale Justisdepartementet å beholde gjeldene struktur i personopplysningsloven og bare foreta de justeringer det materielt sett er behov for. Vi vil fraråde lovendringer som er begrunnet i mer filosofisk disponering av lovbestemmelsene, og kan således ikke støtte det radikale forslaget fra Schartum/Bygrave. Etter vår vurdering vil en oppdeling av grunnkravene basert på primære og sekundære rettslige grunnlag ikke lette tilnærmingen og forståelsen av bestemmelsene. Videre vil en slik oppdeling også bidra til å utviske skillet mellom ikke-sensitive og sensitive personopplysninger, noe som etter vår mening vil være uheldig.

Vårt hovedinntrykk er at lovsystematikken har satt seg så godt hos saksbehandlere og andre brukere av loven, at forbedringene bør være betydelige for å veie opp mot de ulemper som brukerne av loven får ved å måtte forholde seg til en ny systematikk. Eventuelle lovendringer bør således bare gjennomføres dersom regelverket blir klarere og enklere å forholde seg til enn det som er tilfellet i dag.

Vi er videre av den oppfatning at myndighetene må vurdere den ønskede personvernmessige effekt av de forslag som fremmes opp mot de økonomiske konsekvensene endringene vil få for de behandlingsansvarlige, ikke minst for banker, forsikringsselskaper og finansinstitusjoner som behandler store mengde personopplysninger på grunnlag av lovpålagte behandlingsregler og rapporteringskrav. Dersom det kun oppnås mindre endringer i personvernet må myndighetene vurdere om de skal gjennomføres hvis det innebærer store økonomiske konsekvenser for aktørene, for eksempel som følge av endringer i systemer, dokumentasjon, retningslinjer og prosesser. Disse kostnadene vil til slutt ende opp hos kundene i form av økte priser på produkter og tjenester.

FNH og Sparebankforeningen er ellers opptatt av at de reglene som foreslås ikke medfører noen konkurransemessige ulemper for visse typer behandlingsansvarlige ut fra hvordan man har organisert virksomheten. Det er i denne forbindelse også viktig å ta hensyn til at mange av aktørene på markedet i dag er utenlandske, og myndighetene må sørge for at regelverket i Norge ikke blir en hindring for at utenlandske aktører kan drive virksomhet i Norge på lik linje med norske konkurrenter. Det er selvsagt også viktig ved slike regelendringsprosesser å ta hensyn til at norske virksomheter ikke får en konkurranseulempe i forhold til virksomheter etablert i utlandet, særlig innenfor EØS.

II. Kommentarer til enkeltforslag

Nedenfor følger FNH og Sparebankforeningens kommentarer til de enkelte temaer og forslag som Justisdepartementet presenterer i sitt høringsnotat fra juni 2009. Forslag fra Schartum/ Bygrave (2006) som departementet ikke har drøftet spesielt, blir kommentert fortløpende der de tematisk hører hjemme i departementets fremstilling i høringsnotatet.

Ad 1. Definisjonene i personopplysningsloven (§ 2)

Generelt mener vi det er fornuftig av tilgjengelighets- og kontinuitetshensyn å beholde definisjonsreglene i POL § 2.

1.1 Begrepet "personopplysning"

FNH og Sparebankforeningen mener det radikale forslaget til Schartum/Bygrave (2006, pkt 13.2) vedrørende begrepet "personopplysning" skaper flere spørsmål enn det avklarer. Vi er på den annen side enig i at det kan være hensiktsmessig med en viss klargjøring av dagens begrep, da vi har sett flere eksempler på usikkerhet hvorvidt man står overfor en personopplysning eller ikke.

Vi mener videre at dagens skille i POL mellom "ordinære" personopplysninger og sensitive opplysninger er hensiktmessig og bør opprettholdes. Dette gir god oversikt over de ulike krav til behandlingsgrunnlag, konsesjonsplikt mv.

1.1.3.2 Levende personer

FNH og Sparebankforeningen støtter departementets forslag (jfr. departementets lovforslag i pkt. 1.1.3.9) om å presisere i POL § 2 nr. 1 at begrepet "personopplysning" i utgangspunktet omfatter opplysninger og vurderinger som kan knyttes til en levende fysisk person.

Vi vil videre foretrekke departementets presisering om at opplysninger om en død person er "en personopplysning dersom den samtidig er informasjon om en levende person", fremfor Schartum/Bygrave (2006) sitt radikale lovforslag under pkt. 13.2 (§ 2 fjerde ledd). Mens departementets forslag i hovedsak er en kodifisering av gjeldende rett, frykter vi at formuleringen "levende personers familiemessige relasjoner" i det radikale forslaget vil skape usikkerhet om avgrensing av den relaterte personkretsen.

1.1.3.4 "Opplysninger og vurderinger"

Etter vår oppfatning bør definisjonen av personopplysning i POL § 2 nr. 1 videreføres. Begrepet "informasjon" vil etter vår mening gjøre det vanskeligere å se av lovteksten at en personopplysning også omfatter vurderinger som kan knyttes til en identifiserbar person. Så lenge det ikke skjer en realitetsendring, vil vi foretrekke at lovteksten forblir uendret fremfor at brukerne må søke i lovens forarbeider for å finne ut at "informasjon" både dekker (fakta)opplysninger og vurderinger.

1.1.3.6 Kravet til identifikasjon

FNH og Sparebankforeningen støtter departementets vurdering (jfr. departementets lovforslag i pkt. 1.1.3.9) om ikke å følge opp det radikale lovforslaget fra Schartum/Bygrave (2006, pkt

13.2) hvor det presiseres at det foreligger tilstrekkelig identifikasjon av personen så lenge opplysningene kan knyttes til ett medlem av en husstand. I dette radikale lovforslaget § 2 femte ledd heter det:

> *"Opplysninger som kan knyttes til ett eller flere medlemmer av samme husstand regnes alltid som personopplysninger".*

Livsforsikringsselskapene spør i dag om foreldre eller søsken av en forsikringssøker har hatt visse sykdommer, for eksempel kreft, og i tilfelle hvor mange det er, og hvor gamle de var da de fikk sykdommen. Selskapene identifiserer ikke hvem det er som har hatt sykdommen. Spørsmålet er helt avgjørende for at selskapene skal kunne håndtere risikoen for visse arvelige sykdommer forsvarlig, og dermed om selskapene fortsatt kan tilby forsikringer av typen alvorlige sykdommer. Dersom lovforslaget i § 2 femte ledd fra Schartum/Bygrave (2006) er slik å forstå at forsikringssøker ikke vil kunne svare på spørsmålet fra selskapet uten samtykke fra hver enkelt i den kretsen spørsmålet omfatter i "samme husstand", finner FNH og Sparebankforeningen det radikale forslaget helt uakseptabelt.

Videre blir det en vanskelig avgrensning mot hvem som hører til "samme husstand" og hvem ikke. Så lenge barna bor hjemme, regnes de i hvert fall som "samme husstand". Da kan opplysninger om disse, ikke behandles uten samtykke. Så snart barna flytter ut, regnes foreldre og søsken neppe som "samme husstand" og spørsmålet kan stilles uten at samtykke er innhentet.

1.1.3.7 Pseudonymisering

Vi er enig i det radikale forslaget fra Schartum/Bygrave (2006, pkt 13.2) som i § 3d foreslår en bestemmelse som unntar deler av POL for personopplysninger som er pseudonymisert.

1.1.3.8 Sensitive personopplysninger

I det radikale lovforslaget fra Schartum/Bygrave (2006, pkt 13.2) åpnes det for at definisjonen av sensitive personopplysninger gis følgende tilføyelse: "opplysningstyper som er egnet til å åpenbare" .... <for eksempel> " c) helseforhold".

Under pkt. 1.1.3.8 i høringsnotatet skriver departementet at det kan være hensiktsmessig å vise at opplysninger som røper sensitive forhold kan være sensitive, selv om opplysningen i seg selv kan virke harmløs. Departementet viser til at alternative formuleringer kan være "opplysninger som åpenbarer" eller "opplysninger som sier noe om ...", og foreslår selv sistnevnte formulering i sitt forslag til lovtekst i ny § 2 nr. 8. Et slikt krav til en konkret sensitivitetsvurdering før behandlingen iverksettes, er i tråd med personverndirektivet art 8 nr. 1.

Det nevnes som eksempel i høringsnotatet en person som har adresse Ila landsfengsel. Det kan her opplyses at forsikringsselskaper, banker og andre finansinstitusjoner er forpliktet til å registrere kundenes faste (folkeregistrerte) adresse etter hvitvaskingsloven § 8 første ledd nr. 3. Finansbedrifters behandling av slik sensitiv (adresse)informasjon vil således ha tilstrekkelig lovgrunnlag, jf. POL § 9 første ledd litra b), med mindre Folkeregisteret har vedtatt at kundens adresse skal være "fortrolig eller strengt fortrolig" etter hvitvaskingsloven § 8 annet ledd.

Vi vil generelt advare mot at man lar enhver "ordinær" personopplysning der det er mulig å "spekulere seg til" forhold som nevnt i definisjonen av sensitive personopplysninger, skal være omfattet av definisjonen av sensitive personopplysninger. Som eksempel nevner vi at et passbilde (ansiktsfotografi) alltid vil gi en viss informasjon om rase. Videre vil et personnavn i seg selv normalt sannsynliggjøre etnisk opphav. Et fotografi eller levende bilder kan vise sykdom eller helsemessige svakheter – for eksempel en person som halter eller har skadet en arm. Tittel/yrke som prest, kateket, rabbiner, imam eller mulla kan vise religiøs tilhørighet. Eksemplene foran mener vi bør kunne behandles som "ordinære" personopplysninger og ikke som sensitive. Vi er også skeptiske til at informasjon om at noen er "trygdet", at noen har adresse sykehjem/omsorgsbolig, har fått oppnevnt hjelpeverge og så videre, i seg selv skal anses som sensitive personopplysninger.

I definisjonen av sensitive personopplysninger har departementet i forslaget til alternativ lovtekst i pkt. 1.1.3.9 tilføyd følgende formulering: "informasjon som sier noe om". Etter vår vurdering er formuleringen altfor upresis og for lite kvalifiserende til at behandlingsansvarlig skal kunne få gjennomført en forsvarlig sensitivitetsvurdering.

Schartum/Bygrave (2006) uttaler på side 16 og 17 i utredningen følgende om selve behovet for en presisering av lovteksten:

> *"Spennet mellom tilfeller der det er nødvendig å skjelne mellom opplysningstype og opplysningsverdi, og de tilfeller der skillet er unaturlig, er utfordrende i forhold til en hensiktsmessig definisjon av "personopplysning". Spørsmålet kan begrunne at en i visse bestemmelser understreker at det er personopplysningstype det siktes til. Dette er gjort fire steder i den gjeldende lovteksten. Vi mener en tilsvarende presisering bør skje i forhold til definisjonen av sensitive personopplysninger. Slik denne er definert, etterlater den en usikkerhet mht. om bestemmelsen sikter til opplysningstype eller -verdi eller begge deler. I først nevnte tilfelle er det kun slike opplysninger som er klassifisert/tydeliggjort som opplysning om helseforhold mv. som skal anses som sensitive. I andre nevnte tilfelle er det opplysninger som kan ses som opplysninger med slikt sensitivt innhold som loven angir som sensitiv. "NN, Ila fengsel, forvarings- og sikringsanstalt Jøssingveien 33, 1359 Eiksmarka" hører til opplysningstypen "adresse", men sier samtidig, med stor grad av sannsynlighet, at NN har ufrivillig opphold på anstalten. I så fall er adressen en opplysning "om at en person er [...] dømt for en straffbar handling", og dermed sensitiv, se § 2 nr. 8 bokstav b. Sensitivitet skal imidlertid vurderes før behandling av opplysninger starter. Dette tilsier at "sensitive personopplysninger" må forstås som opplysningstyper, jf. § 9 og § 33 der sensitivitet har særlig betydning.*
>
> *På denne bakgrunn forslår vi følgende presisering av § 2 nr. 8 (i kursiv):*
>
> > *8) sensitive personopplysninger: opplysningstyper som er egnet til å åpenbare*
> > *a) rasemessige eller etnisk bakgrunn, eller politisk eller religiøs oppfatning,*
> > *b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,*
> > *c) helseforhold,*
> > *d) seksuelle forhold,*
> > *e) medlemskap i fagforeninger.*

Vi mener en slik endring av definisjonen klargjør innholdet, samtidig som den norske definisjonen blir bedre i samsvar med direktivets bestemmelse, jf. artikkel 8 nr. 1. I direktivet er sensitive opplysningstyper benevnt "special categories of data" (vår kursiv), dvs. det er understreket at det siktes til kategorier av opplysninger. Samtidig er en del av disse opplysningskategoriene beskrevet som "personal data revealing racial or ethnic origin" osv., jf. også Europarådskonvensjon artikkel 6."

FNH og Sparebankforeningen kan prinsipalt ikke se behovet for tilføyelser i dagens definisjon. Dersom departementet likevel kommer til at det skal gjøres tilføyelser så bør slike bidra til å fjerne uklarhetene i dagens formulering, jfr. Schartum/Bygraves vurdering ovenfor. Det vil følgelig være hensiktsmessig å innføre begrepet "opplysningstyper" i definisjonen. Dette vil også være i tråd med direktivets artikkel 8 nr.1 hvor sensitive opplysningstyper er benevnt "special categories of data".

FNH og Sparebankforeningen vil på denne bakgrunn alternativt foreslå formuleringen; "opplysningstyper som åpenbarer". Dette vil både gi den nødvendige avklaring, samtidig som formuleringen oppfattes som tilstrekkelig konkret.

1.3 Begrepet "personregister"

Vi støtter departementets forslag til alternativ definisjon av "personregister" i POL § 2 nr. 3 (inntatt nederst på side 17 i høringsnotatet).

1.4 Begrepet "behandlingsansvarlig"

Vi kan videre gi vår tilslutning til departementets forslag til ny § 2 nr. 4 med en alternativ definisjon av "behandlingsansvarlig" (inntatt på side 20 i høringsnotatet).

Ad 4. Krav til rettslig grunnlag for behandling av personopplysninger (§§ 8-11)

4.3.1 Primære og sekundære rettslige grunnlag
I det radikale lovforslaget fra Schartum/Bygrave (2006, pkt 13.2) foreslås det en rekke materielle og strukturelle endringer i §§ 8 til 8d.

Vi er uenig i dette forslaget fra Schartum/Bygrave. En oppdeling av grunnkravene i generelle krav til rettslig grunnlag (§ 8), primære rettlige grunnlag (§ 8a), sekundære rettslige grunnlag (§ 8b), behandling på grunnlag av skjønnsmessige avveininger og endelig en adgang for Datatilsynet til å tillate behandling der det foreligger samfunnsmessige interesser (§ 8d), fraviker så vidt mye fra gjeldende systematikk i POL at tilgjengeligheten blir klart svekket. Videre utviskes skillet mellom "ordinære" og sensitive personopplysninger i grunnvilkårene, noe vi i utgangspunktet stiller oss skeptiske til. Vi synes også at Schartum/Bygrave beveger seg for mye bort fra personverndirektivets regeloppbygging i artiklene 7 og 8. Materielt sett innebærer forslagene også innstramninger på flere punkter i forhold til gjeldende rett, jfr. departementets vurderinger i høringsnotatets pkt. 4.3.3.

I det moderate lovforslaget fra Schartum/Bygrave (2006, pkt 13.3) er det som nytt annet ledd i § 8 inntatt et krav til behandlingsansvarlig om å kunne dokumentere at "interesseavveiningsgrunnlaget" er benyttet på en legitim måte. Vi har ingen innvendinger til en slik presisering.

Vi kan også slutte oss til Schartum/Bygrave (2006, pkt 13.3) som i det moderate lovforslaget § 11 første ledd litra c) foreslår en presisering om at lovhjemmel kan gi grunnlag for å fravike det opprinnelige formålet med behandlingen.

4.3.2 Nærmere om utredernes forslag til primære rettslige grunnlag
I det radikale lovforslaget fra Schartum/Bygrave (2006, pkt 13.2) foreslås i § 8a en bestemmelse som inneholder krav til primære rettsgrunnlag for behandling av personopplysninger.

Etter forslaget *§ 8a bokstav a)* videreføres *lovhjemmel* som et primært rettsgrunnlag. I forslagets *§ 8a bokstav b)* presiseres det at også "etterlevelse av lovgivning" som "gjør det nødvendig at opplysningene blir behandlet", vil utgjøre et primært behandlingsgrunnlag. Vi støtter dette forslaget. Etter vår vurdering er det en klar fordel med en presisering i lovteksten om at kravet til lovhjemmel anses oppfylt både i tilfeller der det er klart fastsatt i lov at behandling kan skje, samt i de tilfellene der etterlevelse av lovgivning gjør behandling nødvendig.

Etter forslagets § *8a bokstav d)* vil hovedregelen om (frivillig, uttrykkelig og informert) *samtykke* fra den registrerte videreføres som et primært behandlingsgrunnlag.

Det er imidlertid i dette radikale forslaget tilføyd et vilkår om at samtykket ikke må være trukket tilbake. Schartum/Bygrave (2006, pkt. 13.2) har samtidig i § 6 tredje ledd fremmet forslag til regler om retten til tilbaketrekning og virkningen av slik tilbaketrekning. Bestemmelsen lyder:

> *"Et samtykke kan alltid trekkes tilbake. Er samtykket trukket tilbake og det ikke foreligger annet rettslig grunnlag (jf. §§ 8 - 8d), opphører retten til å behandle opplysningene videre, og disse skal slettes, jf. § 9b".*

Etter denne bestemmelsen kan kunden trekke tilbake et gitt samtykke med den konsekvens at personopplysningene skal slettes. Isolert sett kan et automatisk slettingspåbud synes greit så fremt det foreligger et annet uomtvistelig behandlingsgrunnlag (etter forslagets §§ 8 – 8d), for eksempel der behandlingsansvarlig skal oppfylle en avtale med den registerte (§ 8b bokstav a) eller der den behandlingsansvarlige skal fastsette, gjøre gjeldende eller forsvare et gyldig rettskrav (§ 8b bokstav d).

Et vilkår om automatisk sletting av opplysningene ved tilbaketrekning av samtykket, vil etter vår vurdering likevel skape mange (nye) problemstillinger, ikke minst i forhold til handlinger utført av den registrerte før tilbaketrekningen fant sted. Utgangspunktet må - uten hensyn til hjemmel for ulike behandlinger - være at sletting skal skje når det ut fra behandlingsformålet ikke lenger er nødvendig i inneha opplysningene, jfr. POL § 28 første ledd. Å gi den registrerte rett til å kreve sletting i de tilfeller der fortsatt oppbevaring av opplysningene er nødvendig, bare fordi behandlingen har vært basert på samtykke, fremstår som et alvorlig

brudd med lovens system. En slik vilkårlig sletteplikt er etter vårt syn uforenlig med behandlingsansvarliges selvstendige ansvar for sine behandlinger og kan reise uoverskuelige problemer i forhold til legitime behov for å ivareta ulike interesser knyttet til den behandling som har funnet sted, herunder bevisføring ved klager og tvister. Vi viser i den forbindelse til vurderingene som fremkommer i kommentarene til POL § 28 tredje ledd i Ot.prp. nr. 92 (1998-99) side 125.

Som et eksempel på problemstillingen knyttet til å gi den registrerte et rettslig krav på sletting kan nevnes at vedkommende får avslag på en søknad på for eksempel en forsikringsavtale eller vedkommende blir tatt for svik eller forsikringsbedrageri.

En tilbaketrekning som innebærer at forsikringsselskapet må slette alle oppgitte personopplysninger i søknaden og andre lovlig innsamlede opplysninger, gjør selskapet ikke i stand til å kunne forklare og begrunne avslaget på søknaden eller stå i mot et eventuelt erstatningskrav. Opplysninger som gir grunnlag for avvising av kundeforholdet må selskapet således kunne oppbevare så lenge dette er nødvendig, jfr. POL § 28. Selskapet må videre kunne forhindre forsikringsbedragerier eller andre kriminell handlinger mot eget eller andre selskaper basert på allerede registerte opplysninger. Kunder som har fått avslag i et selskap skal etter vår mening ikke kunne løpe til neste selskap og lyve for deretter å få en forsikring han ikke skulle hatt. Tilsvarende eksempler har vi ved lånebedragerier mot bankene.

4.3.3 Nærmere om utredernes forslag til sekundære rettslige grunnlag
Vilkårene i det radikale forslaget fra Schartum/Bygrave (2006) til *ny § 8b* om sekundære rettsgrunnlag synes å innbære en innstramning i forhold til POL § 8 som hjemmel for behandling av ikke-sensitive opplysninger. Inngangskriteriene for å benytte § 8b i det radikale forslaget er at et samtykke er " umulig eller uforholdsmessig vanskelig eller ressurskrevende å legge til grunn for behandlingen", som er vesentlig strengere enn etter gjeldende lovgivning. Vi finner et slikt vilkår uakseptabelt. Vilkårene i POL § 8 er etter vår mening strenge nok som de er i dag.

Det sekundære behandlingsgrunnlaget i *§ 8b bokstav a)* hos Schartum/Bygrave (2006) tilsvarer ordlyden i POL § 8 bokstav a). Vi legger til grunn at vilkåret ikke innebærer materielle endringer og at den praksis som er etablert etter dette grunnlaget eventuelt kan videreføres.

Etter det radikale forslaget i *§ 8b bokstav d)* vil et sekundært rettslig grunnlag for behandling av også ikke-sensitive personopplysninger være der den behandlingsansvarlige skal fastsette, gjøre gjeldende eller forsvare et rettskrav. Dette grunnlaget følger i dag av POL § 9 bokstav e) for sensitive personopplysninger og vil ut i fra mer til mindre -betraktninger også gjelde for behandling av ikke-sensitive personopplysninger. Etter vår vurdering er dette et så sentralt rettslig grunnlag at det også bør inntas som ny bokstav i POL § 8 slik at det direkte gir grunnlag for behandling av ikke-sensitive personopplysninger.

Etter gjeldende rett er det ikke et grunnlag for å behandle sensitive opplysninger at dette er nødvendig for å oppfylle en avtale med den registrerte. Dette vil derimot være et grunnlag for å behandle ikke-sensitive opplysninger. Schartum/Bygrave (2006) går i det radikale forslaget inn for en materiell endring på dette punkt, slik at oppfyllelsen av en avtale med den

registrerte vil gi rettslig grunnlag for behandling av sensitive opplysninger. Vi støtter dette forslaget slik at POL § 9 første ledd tilføres dette behandlingsgrunnlaget.

4.3.5 Sammenslåing av §§ 8 og 9

FNH og Sparebankforeningen mener at gjeldene struktur i personopplysningsloven i utgangspunktet bør videreføres. Dette gjelder også for POL §§ 8 og 9. Etter det vi har erfart har lovsystematikken nå blitt godt kjent og innarbeidet hos finansbedriftene samtidig som den er i overensstemmelse med strukturen i personverndirektivet artikkel 7 og 8.

Vi mener som utgangspunkt at gjeldende lovs system med et skille mellom grunnvilkårene for "ordinære" personopplysninger (§ 8) og sensitive personopplysninger (§ 9) er fornuftig og bør beholdes. På den måten får man fremhevet at sensitive personopplysninger skal behandles med særlig aktsomhet. Ved å endre systemet til primære og sekundære behandlingsgrunnlag slik som hos Schartum/Bygrave (2006, pkt 13.2), mister man lett dette viktige perspektivet.

4.3.6 Grunnkrav til behandling av personopplysninger

Eventuelle endringer i §§ 8-11 med hensyn til krav til behandlingsgrunnlag, formål og relevans bør etter vår mening gi vesentlige forbedringer for å veie opp mot de ulemper som brukerne av loven får ved å måtte forholde seg til en ny systematikk. Vi kan bl.a. ikke se at man oppnår noe nevneverdig ved å forandre rekkefølgen på §§ 8-11.

Ad 5. Overføring av personopplysninger til utlandet (§§ 29-30)

FNH og Sparebankforeningen vil innledningsvis understreke viktigheten av at Norge ikke innfører strengere regler for overføring av personopplysninger til utlandet, enn det som gjelder for andre stater innenfor EØS-området. Våre medlemmer med virksomhet i EØS har erfart at det er forholdsvis stor forskjell i reglene for utenlandsoverføringer som kan være konkurransemessig uheldig, særlig hvis det er ønskelig at flere utenlandske aktører skal etablere seg i Norge.

Vi stiller oss positive til en klargjøring av begrepet "overføring" av personopplysninger til utlandet, herunder opplysninger som gjøres tilgjengelig via Internett eller innenfor en lukket brukerkrets via den behandlingsansvarliges intranett. En slik klargjøring bør imidlertid ikke gjøres i POL, men i forskrifts form. Etter vår vurdering bør bestemmelsene i POL §§ 29 og 30 beholdes teknologinøytrale.

Vi er derimot skeptiske til en utvidet ordning med meldeplikt til Datatilsynet ved overføringer til tredjeland. Dette vil bare medføre økte kostnader hos de behandlingsansvarlige. Vi deler betraktningene til Schartum/Bygrave (2006) om at Datatilsynet neppe vil ha kapasitet til å ta aktivt stilling til innkomne meldinger. Etter vår oppfatning må den enkelte behandlingsansvarlige være bevisste på at det skal foreligge et overføringssamtykke fra den registrerte eller et annet rettslig grunnlag for overføringen etter reglene i POL § 30.

Ad 6. Melde- og konsesjonsplikten (§§ 31-35)

6.3.1 Generelt

Personverndirektivet fastsetter ikke krav om nasjonale konsesjonsordninger, men bestemmer i artikkel 20 nr. 1 at det skal gjennomføres en strengere forhåndskontroll ("prior checking") ved behandlinger av personopplysninger som kan innebære særlige farer for de registrertes friheter og rettigheter. Slik forhåndskontroll kan etter artikkel 20 nr. 2 utøves av både den nasjonale tilsynsmyndighet (her: Datatilsynet) eller av behandlingsansvarliges utpekte personvernombud i samråd med tilsynsmyndigheten.

Forsikringsselskaper, banker og finansinstitusjoner behandler som kjent store mengder personopplysninger. Konsesjonsplikten for disse finansbedriftene inntrer i hovedsak på følgende rettsgrunnlag:

1) Etter POF §§ 7-2 og 7-3 inntrer en alminnelig konsesjonsplikt for forsikringsselskaper, banker og finansinstitusjoners behandling av personopplysninger for kundeadministrasjon, fakturering og gjennomføring av forsikringsavtaler/banktjenester.
2) Etter POL § 33 første ledd ved behandling av sensitive personopplysninger, så som helseopplysninger og opplysninger om straffbare forhold.
3) Etter POL § 33 annet ledd dersom behandlingen åpenbart vil krenke tungtveiende personverninteresser.

Schartum/Bygrave (2006) har i sitt radikale forslag §§ 31-35 tatt til orde for at det etableres en generell ordning med meldeplikt kombinert med en rett for Datatilsynet om å kreve konsesjon der det er fare for at behandlingen kan krenke tungtveiende personverninteresser. Utover dette inneholder det radikale forslaget i § 33b en forskriftshjemmel slik at det kan innføres konsesjonsplikt for å behandle personopplysninger innen bestemte næringer, for bestemte formål, eller på bestemte måter. Etter vår vurdering tilsvarer disse forslagene i hovedsak det som allerede gjelder for finansbedriftene i dag.

Det er for øvrig etter vår mening ikke uproblematisk at banker, forsikringsselskaper og finansinstitusjoner som driver sin virksomhet og behandler personopplysninger i henhold krav fastsatt i forsikrings- og finanslovgivningen mv samt i konsesjon fra Finansdepartementet, Kredittilsynet og Norges Bank, vil kunne risikere at Datatilsynet nekter konsesjon eller krever et konsesjonsvilkår i strid med de nevnte lovbestemte, offentligrettslige krav. Denne problemstillingen har noen ganger gjort seg gjeldende i de drøftelser som FNH og Sparebankforeningen har hatt med Datatilsynet opp gjennom årene ved utarbeidelse av standardkonsesjoner til finansbedriftene etter POF §§ 7-2 og 7-3. Gjennom smidighet og god dialog mellom partene har vi klart å unngå en slik konflikt, men optimalt burde ulike tilsynsmyndigheter selv finne sammen for å unngå motstridende konsesjonsregulering.

6.3.2 Nærmere om meldeplikten

Meldepliktsreglene i POL §§ 31 og 32 samt de omfattende unntaksreglene i POF er generelt vanskelig tilgjengelig og bør forenkles for å få et mer hensiktsmessig system.

I finansbedriftene oppleves det som vanskelig å avgjøre hvilke behandlinger som er meldepliktige (utenfor det konsesjonsbelagte området) og hvilke som ikke er det. På

bankområdet kan dette illustreres ved at bankene har vektlagt ulikt hvilke behandlinger som krever melding, selv om det antas at behandlingen, i alle fall i de større bankene, langt på vei er sammenfallende. Forholdet mellom hva som omfattes av konsesjonsplikt og hva som er gjenstand for selvstendig meldeplikt, oppleves også som uklart. Som et utgangspunkt mener vi at standardkonsesjonen bør dekke alle vanlige behandlingsformer for hhv forsikringsselskaper og banker slik at meldeplikt bare inntrer for behandling som ligger utenfor de behandlingsformer som er alminnelige for angjeldende bransje.

Departementets uttalelser om at selve innsendingsprosessen bør rasjonaliseres slik at meldingene blir færre og mer konsentrerte (jfr. pkt. 6.3.2), støttes av FNH og Sparebankforeningen. Det antydes fra departementets side en ordning der den meldepliktige benytter samme skjema når nye typer behandlinger skal påbegynnes. Vi støtter dette forslaget.

I høringsnotatets pkt. 6.2.2.4.1 siste avsnitt reises det spørsmål om POL § 32 bør suppleres med et krav om at meldingen skal inneholde opplysninger om hvem de registrerte er. I forhold til finansbedriftene må dette kravet eventuelt kunne oppfylles med en generell henvisning til kundemassen, eventuelt fordelt på sektorer. Noe annet vil bli uhåndterbart og anses heller ikke formålstjenlig.

6.3.3 Nærmere om konsesjonsplikten

FNH og Sparebankforeningen har siden innføringen av POL 1. januar 2001 hatt jevnlige drøftelser med Datatilsynet om avgrensning og utforming av standardiserte konsesjonsvilkår for forsikringsselskapene og bankene. Vår erfaring er at konsesjonsinstituttet er fleksibelt for fastsetting av bransjeindividuelle vilkår, som igjen danner et godt grunnlag for etterfølgende kontroll og tilsyn samt internkontroll initiert av den behandlingsansvarlig selv. Den direkte kontakten og dialogen mellom Datatilsynet som konsesjonsgiver og de behandlingsansvarlige og deres næringsorganisasjoner, gir videre et godt grunnlag for forhåndskontroll og at det blir fastsatt konsesjonsvilkår som rent faktisk lar seg etterleve i praksis. At konsesjonsvilkårene formelt sett er å anses som enkeltvedtak, gjør det også mulig å klage vedtaket inn for Personvernnemnda for en fornyet behandling og eventuell omgjøring.

På den annens side har vi som næringsorganisasjoner erfart at Datatilsynet til tider mangler kapasitet og ressurser for en rask gjennomføring og vedtagelse av nye konsesjonsvilkår. Dette skaper frustrasjon hos medlemsbedriftene som ofte innretter seg etter varslede nye konsesjonsvilkår, med planlegging av nødvendige rutineendringer, dokumentasjonsutarbeidelse og IT-investeringer. En konsesjonsprosess som strekker seg langt utover normal saksbehandlingstid er etter vår mening et klart skår i finansbedriftenes forventninger til offentlig regulering og tilsynspraksis.

Det anføres av departementet at konsesjonsplikten skal sikre en forhåndskontroll av behandlingen slik som nedfelt i personverndirektivet artikkel 20 nr. 1. Vi er langt på vei enig i at konsesjonsordningen dekker et slikt formål såfremt tilsynsmyndigheten etter mottak av konsesjonssøknaden faktisk gjennomfører adekvate kontrolltiltak hos de behandlingsansvarlige før konsesjonsvilkårene fastsettes. Ved bruk av standardkonsesjoner innenfor bransjer hvis selskaper driver samme type virksomhet (typisk finansbedrifter), vil slike forhåndskontrolltiltak av ressursmessige grunner måtte begrenses til noen få utvalgte behandlingsansvarlige av ulik størrelse. Resultatet av kontrollen vil så danne grunnlag for fastsetting av standardvilkårene.

6.3.3.1 Kan eller bør konsesjonsordningen fjernes?
Datatilsynets reiser spørsmålet om konsesjonsordningen kan fjernes og erstattes av en annen form for forhåndskontroll ("prior checking") ved behandling av personopplysninger. FNH og Sparebankforeningen vil her avgrense problemstillingen til å gjelde finansbedrifter. I utgangspunktet er vi usikre på om andre kontrollmetoder vil kunne fungere like tilfredsstillende og med samme gjennomslagskraft hos finansbedriftene som Datatilsynets konsesjonsvilkår og tilsynsvirksomhet. Departementet viser til at den svenske personuppgiftslagen har en ordning med meldeplikt med etterfølgende forhåndskontroll. Dette vil nok også kunne fungere i Norge, men det krever at Datatilsynet har tilstrekkelige ressurser til å kunne "rykke ut" og eventuelt fastsette tilpassede konsesjonsvilkår.
FNH og Sparebankforeningen har etter en helhetsvurdering kommet til at dagens ordning med standardkonsesjoner for finansbedriftene bør videreføres. Som omtalt nedenfor under pkt. 6.3.3.2 bør POF §§ 7-2 og 7-3 endres for å klargjøre konsesjonsområdet og hvilke behandlinger som er konsesjonspliktige.

6.3.3.2 Hvilke behandlinger bør underlegges konsesjonsplikt eller annen forhåndskontroll?
På finansområdet legger vi for den videre drøftelse til grunn at forhåndskontrollen også i årene fremover vil bli foretatt av Datatilsynet og at en konsesjonsordning for forsikringsselskaper, banker og finansinstitusjoner vil bli videreført, jfr. den store mengden av personopplysninger, også av sensitiv karakter, som finansbedriftene håndterer.

Departementet viser under pkt. 6.3.3.2 i høringsnotatet til POF kapittel 7 pkt. I som setter rammer for hva som skal konsesjonsreguleres for ulike bransjer, herunder for finansbedriftene. For forsikringsselskaper, banker og finansinstitusjoner omfatter konsesjonsplikten behandling av personopplysninger for kundeadministrasjon, fakturering og gjennomføring av forsikringsavtaler/banktjenester. Annen behandling er enten meldepliktig etter POL § 31 eller konsesjonspliktig etter POL § 33.

Det har vært, og det er vel til dels fortsatt, usikkerhet både hos Datatilsynet og i finansbedriftene om hva som er rammene eller behandlingsformålet etter bestemmelsene i POF §§ 7-2 og 7-3. Konsesjonspraksis har vist at i de tilfeller det har oppstått tvil om forskriftsbestemmelsene gir hjemmel for konsesjonsregulering av en bestemt behandling, for eksempel bankenes bruk av kundeopplysninger i markedsføringsøyemed, har Datatilsynet i stedet anvendt POL § 33 annet ledd direkte. Dette er etter vår mening utilfredsstillende både for tilsynet og finansbedriftene.

Vi har ovenfor tatt til orde for at ordningen med standardkonsesjoner for finansbedrifter etter POF §§ 7-2 og 7-3 bør videreføres for de vanligste behandlingsformene. Etter vår mening bør departementet klargjøre bestemmelsene i POF slik at man konkret kan se hvilke behandlinger og opplysningstyper som er underlagt konsesjonsplikt.

Ad 7. Fjernsynsovervåking (§§ 36-41)

Departementet ber om høringsinstansenes syn på den lovstruktur som er valgt for reglene om fjernsynsovervåking i POL §§ 36-41 samt POF kapittel 8. Det samlede regelverket oppleves av brukerne i dag som lite oversiktelig. Etter vår vurdering bør POL kun inneholde noen få hovedregler om fjernsynsovervåking inklusiv en forskriftshjemmel mens POF bør inneholde alle materielle behandlingsregler.

Vi støtter ellers forslaget fra Datatilsynet om at begrepet fjernsynsovervåking erstattes av et mer teknologinøytralt begrep, for eksempel kameraovervåking. Videre bør det i POL § 36 presiseres nærmere hvilke typer overvåkningsutstyr som vil omfattes av begrepet. Etter vår mening bør håndholdt utstyr holdes utenfor begrepet slik som i dag (jfr. kriteriene " ... fjernbetjent og automatisk virkende ...").

Departementet omtaler under pkt. 7.4.2.1 i høringsnotatet et forslag fra Datatilsynet om å lage en bestemmelse som fastsetter krav til behandlingsgrunnlag for fjernsynsovervåking. Hensikten er å fjerne tvil om interesseavveiningsbestemmelsen i POL § 8 bokstav f) gir et tilstrekkelig behandlingsgrunnlag. Departementet viser til at en slik bestemmelse for eksempel kan lyde:

> *"Ved vurderingen av hva som er en berettiget interesse etter personopplysningsloven § 8 bokstav f skal det for fjernsynsovervåking legges vesentlig vekt på om overvåkingen verner om liv eller helse, eller forebygger kriminalitet".*

Vi støtter forslaget om en slik presisering av behandlingsgrunnlaget for fjernsynsovervåking. Bankenes overvåking av ekspedisjonslokaler, betalingsterminaler og minibanker mv er for eksempel begrunnet i disse hensynene.

Når det gjelder spørsmålet om hvorvidt det bør fastslås hvilke steder det ikke er anledning til å foreta overvåking, jfr. høringsnotatet pkt. 7.5, vil det etter vår vurdering være mest hensiktsmessig å definere hvilke steder det er anledning til å foreta overvåking. En motsatt avgrensning som innebærer definering av steder som skal være overvåkingsfrie (for eksempel friluftsområder, parkanlegg, offentlige badestrender og lignende) vil etter vår vurdering raskt lede til mange vanskelige avveininger av kryssende hensyn.

Ad 8. Mindreåriges personvern

Etter vår oppfatning er redegjørelsen i høringsnotatet uklar når det gjelder i hvilken grad foreldre og andre (herunder myndigheter) kan handle på vegne av mindreårige for å ivareta barns personverninteresser. Vi mener prinsipielt at disse spørsmålene bedre hører hjemme i vergemålsloven (se nedenfor) og barneloven. Det fremstår ikke hensiktsmessig at personopplysningsloven skal ha sin egen regulering av disse spørsmålene som egentlig handler om deling av kompetanse mellom foreldre og barn.

Av drøftelsen synes det som om departementet hovedsakelig har vært opptatt av finne mekanismer for å beskytte barn mot foreldre som, uten hensyn til barnet, velger å

offentliggjøre opplysninger på internett og andre steder. Dette er en viktig problemstilling som vi har stor forståelse for blir reist. Vi frykter imidlertid at de nye reglene som er fremmet av Schartum/Bygrave (2006) § 6a om barns adgang til å opptre som registrert person, vil kunne gå utover helt vanlige og legale avtaleslutninger som foreldrene foretar for ivareta foreldreansvaret på en forsvarlig måte, som for eksempel forvaltning/disponering av barns formuesmidler og tegning av barneforsikringer som innebærer avgivelse og behandling av sensitive personopplysninger om barnet. Det kan synes som om reglene legger opp til at alle barn over 12 år skal være aktivt med for at personopplysninger om dem skal kunne registreres.

Vi vil i denne sammenheng vise til Ot. prp. nr. 110 (2008-09) om ny vergemålslov som i lovutkastet § 9 regulerer den mindreåriges rettslige handleevne. Lovutkastet lyder: "*En mindreårig kan ikke selv foreta rettslige handlinger eller råde over sine midler, med mindre noe annet er særlig bestemt.*"

I proposisjonen kapittel 13 har Justisdepartementet kommenterer lovutkastet § 9. Her står bl.a.:

> "*Den manglende evnen til å foreta rettslig handlinger omfatter i utgangspunktet både gjensidige og ensidige handlinger og evnen til å motta påbud som krav og oppsigelser. Eksempler på disposisjoner som omfattes av forbudet, er kjøp, salg, gaveløfter, pantsettelse, bytte, utlån og utleie. Forbudet omfatter både aktive handlinger og unnlatelseshandlinger. Den mindreårige har heller ikke kompetanse til å samtykke til behandling av personopplysninger. Dette er også en «rettslig handling» som omfattes av forbudet. Det følger også av bestemmelsen at barn ikke kan representere seg selv i forvaltningssaker eller i saker for domstolene om ikke noe annet er særlig bestemt. Det er gitt egne regler om at vergen representerer den mindreårige i ulike rettslige prosesser, jf. forvaltningsloven, tvisteloven og straffeprosessloven.*" (vår understrekning)

Ad 9. Personvernombud

En del av finansbedriftene, både banker og forsikringsselskaper, har internt utpekte personvernombud. Erfaringene er gjennomgående gode, men vi er i utgangspunktet skeptiske til å gi personvernombudet for stor innflytelse i den forstand at man reduserer den behandlingsansvarlige forpliktelser i form av redusert meldingsplikt eller for ivaretagelse av internkontrollen.

Vi har liten tro på at et internt utpekt personvernombud som selv er ansatt i den bedriften som skal kontrolleres, vil kunne har tilstrekkelig distanse, kompetanse og gjennomslagskraft til å fylle Datatilsynets tilsynsrolle. Etter vår vurdering bør personvernombudet som i dag har en viktig og nyttig funksjon som "vaktbikkje" og pådriver i bedriftenes personvernarbeid, forbli et supplement til Datatilsynets virksomhet.

Etter vår mening bør ikke personvernombudet være ansvarlig for internkontrollen eller ha andre oppgaver som innebærer ansvar for at personvernet etterleves i praksis. Dette må ligge

hos daglig behandlingsansvarlig og de ressurser denne disponerer uavhengig av om man oppretter personvernombud eller ikke.

Vi støtter forslaget om at det i POL bør inntas en bestemmelse om personvernombudets gjøremål, jfr. høringsnotatet 9.3.4, men ombudets rolle bør begrense seg til å ha kontakt mot Datatilsynet og bistå som ressursperson ved internkontroll, avviksrapportering, sikkerhetsrevisjon m.v. Videre bør det tydeliggjøres hvilke plikter ombudet har ved avdekking av svikt i virksomhetens evne til å etterleve regelverket og sine egne internkontrollprosedyrer, så som intern rapportering til den daglige behandlingsansvarlige. Ombudet må også kunne være en person å henvende seg til for kunder, brukere og andre som har spørsmål eller klager vedrørende virksomhetens ivaretakelse av personvern, men ombudet bør ikke selv være klagebehandler.

Det er i høringsnotatet pkt 9.3.2 bedt om innspill vedrørende bruk av begrepet "personvernombud". Vi er enige i at begrepet kan assosieres i retning av de offentlig oppnevnte ombudene. Det vil være uheldig. På den annen side er etter hvert personvernombud blitt et innarbeidet begrep som mange forbinder med noe positivt, og dette taler etter vår vurdering for at man bør beholde dagens betegnelse. En endring av betegnelsen vil kunne skape unødig forvirring.

Ad 10. Andre problemstillinger

10.1 Personopplysningsloven og særlovgivningen

Personopplysningslovens forhold til andre lover er i dag regulert i POL § 5. Her fremgår det at POL ved lovkonflikt viker for "særskilt lov som regulerer behandlingsmåten". Selv om det kan hevdes at § 5 kun gjentar en opplagt tolkningsløsning, er § 5 og andre regler av denne karakter svært nyttige for brukerne av POL.

I det radikale forslaget fra Schartum/Bygrave (2006) er det i *§ 33c inntatt en bestemmelse som gir unntak fra konsesjonsplikt når behandlingen har hjemmel i lov*. Etter dette forslaget kan Datatilsynet ikke nekte behandling av personopplysninger eller stille vilkår for slik behandling dersom dette vil stride mot bestemmelser i lov eller forskrift. FNH og Sparebankforeningen støtter som nevnt foran under pkt. 6.3.1 Generelt, forslaget om at en slik unntaksbestemmelse inntas i POL.

I Schartum/Bygrave (2006) kapittel 12 tas det også til orde for at forholdet mellom personopplysningslovens behandlingsregler og regler om taushetsplikt i annen lovgivning må klargjøres. Konkret foreslår de i det radikale lovforslaget *§ 8 bokstav a)* en helt ny bestemmelse om at behandlingen skal skje innenfor rammene av lovbestemt taushetsplikt. Banker, forsikringsselskaper og finansinstitusjoner må etter gjeldende taushetsregler i forsikrings- og finanslovgivningen ta hensyn til sin taushetsplikt i tillegg til grunnkravene og behandlingsreglene i POL. For finansbedriftene vil forslaget § 8 bokstav a) således ikke innebære ny materiell rett, men det kan av pedagogiske og tolkningsmessige grunner være hensiktsmessig å innta en slik bestemmelse i POL. FNH og Sparebankforeningen støtter derfor forslaget om at forholdet mellom POL og lovbestemt taushetsplikt klargjøres nærmere med en egen bestemmelse i POL.

10.4 Informasjonssikkerhet og internkontroll
Departementet har i høringsnotatet pkt. 10.4 noen betraktninger om behovet for presisering og utdyping av reglene i POL § 13 (informasjonssikkerhet) og § 14 (internkontroll). Vi gir vår tilslutning til at det gjennomføres tiltak som kan forbedre forståelsen og praktiseringen av disse reglene i POL og i POF kapitlene 2 og 3.

POF § 2-15 regulerer sikkerhetsspørsmål i forholdet mellom behandlingsansvarlig og underleverandører. Når behandlingsansvarlig utpeker en underleverandør inngås det en tjenesteavtale mellom partene. Etter POF § 2-15 fjerde ledd er behandlingsansvarlig forpliktet til å etablere klare ansvars- og myndighetsforhold som skal beskrives i "særskilt avtale". Vi legger til grunn at partene ikke må lage et eget avtaledokument for å regulere vilkår om ansvars- og myndighetsforhold, men at slik "særskilt avtale" kan inngås som en del av den ordinære tjenesteavtalen. Vi ber departementet vurdere en klargjøring av dette punktet i POF § 2-15 fjerde ledd.

10.5 Databehandlerens rådighet over personopplysninger
Vi støtter også forslaget om en klargjøring av POL § 15 slik at det mer detaljert fremgår hvilke elementer som skal inngå i avtalen mellom en databehandler og behandlingsansvarlig. Videre bør databehandlerens plikter fremgå mer detaljert enten i POL eller i forskrifts form. Ofte vil databehandleren være den mest profesjonelle og dominerende part i et slikt avtaleforhold, jfr. bl.a. de store datasentralene på bankområdet.

10.9 Bruk av fødselsnummer, fingeravtrykk og annen biometri
Bruk av fødselsnummer og andre entydige identifikasjonsmidler er i dag regulert i POL § 12. Her oppstilles to hovedkriterier for bruk: 1) Det skal være saklig behov for sikker identifisering og 2) metoden skal være nødvendig for å oppnå slik bruk.

Schartum/Bygrave (2008) foreslår at bestemmelsen deles i to slik at § 12 bare regulerer bruk av fødselsnummer mens det lages en ny bestemmelse om biometriske kontrollmetoder. Vi støtter en slik oppsplitting, men er uenig med utrederne i at bruk av fingeravtrykk og andre biometriske metoder skal være forbudt uten lovhjemmel. Sikre metoder for entydig identifisering bør etter vår oppfatning kunne utvikles kommersielt og tas i bruk med samtykke fra borgerne, uten at det nødvendigvis foreligger lovhjemmel for anvendelsen. En annen sak er at dersom det ikke foreligger lovhjemmel for biometrisk identifikasjon, bør det være en reell valgfrihet for borgerne om de heller ønsker at identifikasjonen skal kunne foretas ved bruk av andre metoder.

I ny bestemmelse fra Schartum/Bygrave (2008) om fødselsnummer oppstilles fortsatt nødvendighetskravet, men bestemmelsen foreslås utvidet slik at den behandlingsansvarlige må ha gjennomført en risikovurdering som klart viser at fødselsnummer er nødvendig for å oppnå sikker identifisering. Bestemmelsen vil opplagt snevre inn adgangen til å benytte fødselsnummer samtidig som en dokumentert risikovurdering vil være svært ressurskrevende og ha store praktiske konsekvenser for behandlingsansvarlige. Risikovurdering etter forskriften hvor en tilkjennegir ulike uønskede hendelser med sannsynlighet og konsekvens synes dessuten uegnet for å vurdere/dokumentere nødvendigheten av å benytte fødselsnummer. Etter vår vurdering bør en ordinær vurdering av nødvendigheten for å benytte fødselsnummer som i dag må være tilstrekkelig.

I tilegg foreslås et generelt forbud mot at fødselsnummer *alene* benyttes til verifisering (bekreftelse) av en persons identitet. Vi har stor forståelse for at forslaget fremmes. Altfor mange (også offentlige myndigheter) tror eller legger til grunn at fødselsnummeret er en hemmelig opplysning som bare personen selv kjenner til. Fødselsnummer anvendes derfor ikke sjelden som en selvstendig identifikasjonsmetode, dvs. uten bruk av andre sikkerhetsanordninger i tillegg som for eksempel en eID eller et passord ved mildere sikkerhetsbehov. Et forbud mot bruk av fødselsnummer alene til verifikasjonsformål, vil derfor kunne være et godt bidrag til å redusere risikoen for at borgere blir utsatt for kriminelle handlinger ved identitetstyveri, for eksempel der noen misbruker et fødselsnummer for å utgi seg for være en annen.

Med vennlig hilsen

for Finansnæringens Hovedorganisasjon

Tore A. Hauglie
fagdirektør

for Sparebankforeningen i Norge

Gunnar Harstad
advokat