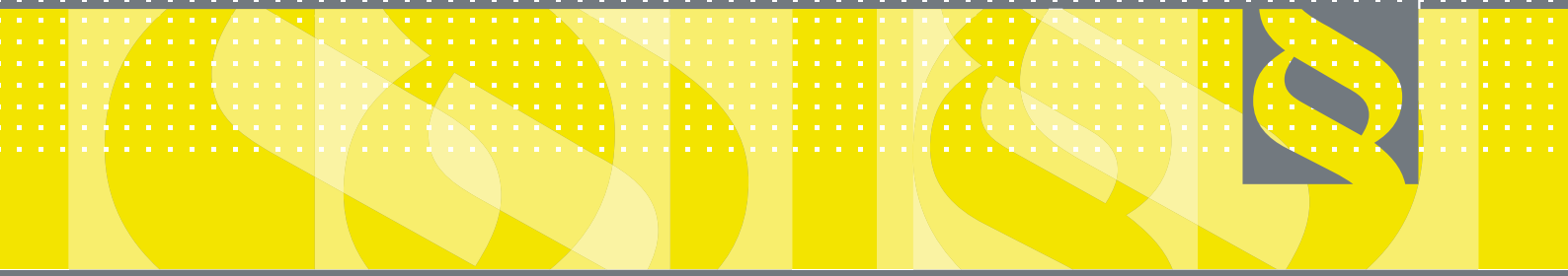
Rapport 2006

# Utredning av behov for endringer i personopplysningsloven

Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet

Professor dr. juris Dag Wiese Schartum
Førsteamanuensis dr. juris Lee A. Bygrave



JUSTIS- OG POLITIDEPARTEMENTET

Rapport 2006

# Utredning av behov for endringer i personopplysningsloven

Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet

Professor dr. juris Dag Wiese Schartum
Førsteamanuensis dr. juris Lee A. Bygrave

JUSTIS- OG POLITIDEPARTEMENTET

# Sammendrag

Rapporten inneholder redegjørelser, diskusjoner og forslag med utgangspunkt i 11 mandatpunkter som gjelder mulige behov for å endre personopplysningsloven:

- Lovens definisjoner – begrepene ”behandling av personopplysninger” og ”behandlingsansvarlig” (§ 2);
- Lovens saklige virkeområde (§ 3);
- Lovens geografiske virkeområde (§ 4);
- Ytringsfrihet og personvern (§ 7);
- Rettslig grunnlag for å behandle personopplysninger (§§ 8 og 9);
- Elektroniske spor;
- Overføring av personopplysninger til utlandet (§§ 29 og 30);
- Melde- og konsesjonsplikten (§§ 31 – 35);
- Frivillige ordninger – personvernombud, bransjevise atferdsnormer;
- Mindreåriges personvern;
- Strukturen i personopplysningsloven og forholdet mellom personopplysningsloven, særlovgivningen og personopplysningsforskriften.

Flere av mandatpunktene ovenfor som er uten henvisning til konkrete bestemmelser, reiser spørsmål om endring også av andre paragrafer enn de som er angitt ovenfor (i parentes).

Hovedkonklusjonen i evalueringen av loven er at det er mange behov for endringer i någjeldende bestemmelser. Det foreslås bl.a. å tydeliggjøre lovforståelser der en i dag må benytte forarbeider, forvaltningspraksis og litteratur for å få nødvendig kunnskap. Andre forslag tar utgangspunkt i behovet for å samle og tydeliggjøre bestemmelser som gjelder den enkeltes rettigheter mv. I tråd med mandatet fremmes det også forslag om å redusere og klart avgrense lovens saklige virkeområde, samt redusere konsesjons- og meldeplikten. I rapporten fremkommer det dessuten forslag til en ny og forbedret ordning med personvernombud.

Endringsbehovene er etter forfatternes mening så omfattende at det ideelt sett bør gjøres større endringer i flere av lovens kapitler. Disse endringsbehovene er samlet sett så radikale at forfatterene har valgt å fremme to parallelle forslag til lovendring: Et ”radikalt” og et ”moderat” forslag.

Det radikale lovforslaget har følgende hovedelementer:

- Nye, og langt mer utfyllende bestemmelser som klargjør lovens grunnbegreper;
- Bestemmelser som klargjør ulike aktører og roller, jf. både lov og forskrift;
- Bestemmelse som klargjør mindreåriges rett til å opptre som registrert person;
- Revisjon og endring av kravene til rettslig grunnlag (nåværende §§ 8 og 9);
- Ny bestemmelse om nye, ”uforenlige formål” (jf. nåværende § 11 første ledd bokstav c);
- Krav om sletting, retting mv. formulert som en rettighet for registerte personer;
- Nye lovbestemmelser om en utbygget ordning med personvernombud;
- Reduksjon av meldepliktordningen med nærmere tilknytning til ordningen med konsesjonsplikt;
- Reduksjon og omlegging av konsesjonsplikten, herunder med forslag til en ”demokratisert” konsesjonsordning.

I tillegg er det flere mindre endringer.

Det moderate lovforslaget inneholder også et forholdsvis stort antall forslag til endringer, men disse har mer beskjedne virkninger, og representerer således en klart mer forsiktig linje enn det radikale forslaget gjør:

- Presisering av definisjonene av ”personopplysning”, ”personregister” og ”sensitiv personopplysning” (§ 2);
- Ny bestemmelse som klargjør mindreåriges rett til å opptre som registrert person;
- Presisering av unntaket vedrørende rent personlige og private formål (§ 3);
- Innskjerping av alternativet i § 8 første ledd bokstav f om ”nødvendig grunn” til å behandle personopplysninger i henhold til en interesseavveining;
- Ny bestemmelse om nye, ”forenlige formål”(jf. nåværende § 11 første ledd bokstav c);
- Flytting av bestemmelsen i personvernforskriften vedrørende fødselsnummer opp i lovens § 12;
- Omformulering av § 18 om innsyn som to separate bestemmelser;
- Skjerping av krav til samtykke i tilknytning til overføring til utlandet (§ 30 første ledd bokstav a);
- Reduksjon av meldeplikten (§ 31);
- Reduksjon av konsesjonsplikten (§ 33);
- Ny bestemmelse om Datatilsynets rolle vedrørende internasjonale forhold (§ 42 a);
- Samlet regulering av Personvernnemndas kompetanse ved at kompetansen etter forskriften settes inn i lovens § 43 første ledd.

Denne listen over moderate forslag er uttømmende.

Til slutt i rapporten behandles administrative og økonomiske konsekvenser og forutsetninger, se kapittel 14.

# Innholdsfortegnelse

# Kapittel 1

## Om mandat, rammer, underlag og arbeidsmåte

Denne utredningen er skrevet på oppdrag av Justisdepartementet og Moderniseringsdepartementet som del av en større evaluering (etterkontroll) av personopplysningsloven.[1] Oppdraget går ut på å utrede 11 mandatpunkter. Hvert punkt er gjengitt i innledningen til hvert kapittel nedenfor. Oppdraget omfatter mange viktige og til dels vanskelige problemstillinger – bl.a. definisjoner av personopplysningslovens sentrale begreper, avgrensninger på lovens saklige og geografiske virkeområde, lovens forhold til ytringsfrihet og lovens konsesjons- og meldepliktsordningen.

Formålet med utredningen er primært å opplyse problemstillingene i mandatet og fremme konkrete forslag til løsninger. Ambisjonen har vært å fremme forslag der dette er mulig og fruktbart. De mandatpunktene vi har forholdt oss til, speiler en arbeidsdeling mellom oss og Justisdepartementet. Deler av loven som ikke inngår i vårt mandat, er omfattet av departementets arbeid med etterkontroll av loven.

I noen grad ligner vårt arbeid litt på de oppgaver utredningsutvalg utfører i tilknytning til utarbeidelse av nye lover og vesentlige endringer av eksisterende lover. En åpenbar forskjell er imidlertid at vi kun har vært to personer til å vurdere de aktuelle spørsmålene. Vi er begge jurister med bakgrunn fra Universitetet i Oslo, med spesialisering innen personopplysnings-rett. Slik spesialisering er delvis en klar fordel. På den annen side er det også en ulempe at bidraget til utredningen kun har kommet fra ett miljø og ett ståsted. Vi har forsøkt å kompensere for denne "ensidigheten" på to måter. Dette gjorde vi for det første ved å starte opp utredningsarbeidet med et åpent seminar der mandat og opplegget for utredningen ble diskutert.[2] Seminaret resulterte i justeringer av undersøkelsesopplegget, samt flere interessante innspill til de konkrete problemstillingene.

For det andre inviterte vi ulike eksperter til møter for problemkartlegging. Ett møte ble holdt med "personvernadvokater", dvs. advokater med praksis som i stor grad omfatter problemstillinger i tilknytning til personopplysningsloven.[3] Et annet møte hadde fokus på offentlig forvaltning. Vi var i denne sammenheng spesielt opptatt av nye samarbeidsmønstre knyttet til elektronisk forvaltning.[4] Begge møtene ga betydelige innspill til vår problemforståelse og til mulige løsninger. I utredningen er imidlertid ikke disse innspillene eksplisitt referert til, men inngår i det generelle grunnlaget for utredningen.

Det hadde åpenbart vært ønskelig med et mye bredere inntak av erfaringsmateriale i form av spørreundersøkelser, møter mv., men tidsramme og budsjett ga ikke mulighet for et bredere opplegg. Vi har imidlertid også hatt tilgang til viktig materiale som har blitt til bl.a. med henblikk på etterkontrollen av loven. Dette gjelder særlig to undersøkelser som Transportøkonomisk institutt gjennomførte i 2005 vedrørende erfaringer med, kunnskaper om og holdninger til personvern og personopplysningsloven. Den ene undersøkelsen,

---

1 Lov om behandling av personopplysninger 14. april 2000 nr. 31 (heretter også "pol").

2 Seminaret ble avholdt 14. september 2005, kl. 09.15 – 15.15 med ca. 30 deltakere.

3 Møtet ble holdt 14. november 2005 med representanter fra advokatfirmaene Føyen, Kluge, Hjort, Steenstrup Stordrange, og Wiersholm, Mellbye & Bech. En advokat fra Wikborg Rein var også invitert, men måtte melde frafall.

4 Møtet ble holdt den 12. desember 2005 med representanter fra Skattedirektoratet og Statskonsult. Rikstrygdeverket skulle ha deltatt på møtet, men hadde frafall.

”Befolkningsundersøkelsen”,[5] gjelder et utvalg av enkeltpersoner, dvs. av slike ”registrerte personer” som personopplysningsloven skal beskytte. Den andre undersøkelsen, ”Virksomhetsundersøkelsen”,[6] tar tak i et utvalg av juridiske personer i privat og offentlig virksomhet, og representerer virksomheter som er ”behandlingsansvarlige”, dvs. som primært har plikter i henhold til loven. Disse to undersøkelsene har først og fremst vært av verdi ved at de har formidlet et generelt bilde av kunnskaper og praksis vedrørende loven. Det har imidlertid ikke vært direkte koplinger mellom punktene i vårt utredningsmandat og spørsmålene i undersøkelsene. Derfor har resultatene ikke påvirket våre vurderinger på direkte måter. Som generelt bakgrunnsstoff er det særlig kombinasjonen av Befolknings- og Virksomhetsundersøkelsen som har vært av interesse. Grovt gjengitt viser svarene at befolkningen har stor tillit til at regler for behandling av personopplysninger blir etterlevet. På den annen side gir svarene fra virksomhetene et bilde av ”behandlingsansvarlige” som riktignok er positive til personvern, men på den annen side har begrensede kunnskaper om personopplysningsloven mv., og som i til dels skremmende liten grad ser ut til å etterleve lovens bestemmelser. Undersøkelsene sier lite om hvorfor etterlevelsen av loven er så slett. På spørsmål om kjennskap til personopplysningsloven, svarte hele 82% av virksomhetene enten ”lite kjennskap” eller ”verken eller”.[7] Samtidig svarte bare 5% at loven var vanskelig å forstå, mens hele 52% svarte ”verken eller” og 28% svarte ”vet ikke” på dette spørsmålet.[8] Virksomhetsundersøkelsen var generelt preget av mange svar av kategoriene ”verken eller” og ”vet ikke”, og gir klart inntrykk av lavt kunnskapsnivå blant de virksomheter som har plikt til å etterleve loven. Derfor er det lite grunn til å legge særlig vekt på at kun et lite antall respondenter mente loven er vanskelig å forstå. Fra vår egen erfaring med loven, som forfattere og undervisere, vet vi at folk ofte har problemer med å fortolke og anvende loven på akseptabel måte. Slike utfordringer gjenspeiles for øvrig i mandatet og har blitt grundig bekreftet i de forberedende møtene vi har avholdt.

Som del av forarbeidet i forbindelse med evaluering av loven, ble det også bestilt en utredning fra Norsk Regnesentral vedrørende ”elektroniske spor”.[9] I anledning fremleggelse av rapporten og Befolkningsundersøkelsen, ble det den 14. juni 2006 arrangert en konferanse i regi av Justisdepartementet.[10] Rapporten og konferansen har inngått som bakgrunnsmateriale for drøftelsene i kapittel 7 om elektroniske spor. Det samme gjelder en rapport skrevet av Teknologirådet om samme tema.[11]

I tillegg til ekspertmøtene, seminarene, de refererte undersøkelsene og rapportene, har vi hatt tre møter med de sentrale myndighetene på området. Således ble det avholdt separate møter med Datatilsynet, Justisdepartementet og Moderniseringsdepartementet (nå Fornyings- og administrasjonsdepartementet, FAD). Møtene tok primært sikte på å gjennomgå punktene i mandatet med vekt på supplerende problemkartlegging og identifisering av aktuelle dokumenter. Heller ikke innholdet av disse samtalene er direkte referert i utredningen, men inngår i vårt generelle kunnskapsgrunnlag. Disse samtalene ga imidlertid ikke noen vesentlige, konkrete resultater ut over de som allerede forelå i og i tilknytning til mandatet. Vi har herunder heller ikke blitt presentert konkrete løsningsforslag.

---

5 Se Ravlum 2005a.

6 Se Ravlum 2005b.

7 Se Ravlum 2005a tabell 4.4.

8 Se Ravlum 2005b tabell 4.5.

9 Se Danielson m.fl. 2005.

10 Justisdepartementets konferanse om elektroniske spor og personvern som menneskerettighet.

11 Jf. Teknologirådet 2005.

I tillegg til utredningsmandatet er vi anmodet om å forholde oss aktivt til Norges folkerettslige forpliktelser, særlig EUs direktiv av 1995 om personopplysningsvern.[12] Den EU-rettslige rammen har vært en vesentlig utfordring i dette arbeidet. Personverndirektivet, som Norge har plikt til å implementere, ble vedtatt for 11 år siden. Siden vedtakelsen har det vært betydelige juridiske, teknologiske og samfunnsmessige endringer som gjør at det ikke sjelden er utfordrende å finne ut av hva som er gjeldende EU-rett på området. Det hefter derfor usikkerhet ved flere av våre konklusjoner vedrørende EU-retten, men slik usikkerhet er åpent gjort rede for underveis i rapporten. Vi har valgt å ta utgangspunkt i engelskspråklige versjoner av aktuelle dokumenter. Dette skyldes dels usikkerheter som er knyttet til den norske oversettelsen av personverndirektivet, og dels det forhold at den engelske språkversjonen av direktivet er blant de versjoner som de fleste internasjonale diskusjoner tar utgangspunkt i. Uansett trekker vi også inn norske, danske, svenske, tyske og franske språkversjoner på utvalgte punkter.

Mandatet inneholder en anmodning om å utarbeide endringsforslag. Etter hvert som arbeidet skred frem, ble det stadig tydeligere at det etter vår mening er gode grunner til å gjøre betydelige endringer i gjeldende lovtekst. Det ble videre klart at én endring lett kunne forplante seg og begrunne ytterligere endringer, herunder endringer som pekte ut over punktene i mandatet. Vi stod derfor overfor valget mellom å ta konsekvensen av de innsikter arbeidet ga og foreslå forholdsvis omfattende endringer, eller å prøve å moderere diskusjonene slik at forslagene ble mindre "dramatiske". Dilemmaet er i rapporten løst ved at vi fremmer to sett av forslag til endringer; et "moderat" og et "radikalt" forslag. Det moderate forslaget inneholder endringer vi mener representerer et minimumsnivå, dvs. endringer som er nødvendige og – trolig – lite kontroversielle. Det radikale forslaget representerer det vi mener vil være det beste utgangspunkt for det videre arbeidet med evaluering av loven. Vi hevder ikke at disse forslagene er "vedtaksklare", men mener at de er hensiktsmessige og tilstrekkelige som basis for departementets nærmere analyse.

Valg av overordnet lovgivningsstrategi har ikke direkte vært en del av vårt mandat, noe som gjør en tosporet tilnærming nødvendig. Vi vil imidlertid ikke unnlate å peke på at resultatene fra Virksomhetsundersøkelsen er så nedslående at det kan danne grunnlag for å velge å gjøre radikale grep som en ellers ikke ville ha valgt. Uansett er det mulig å benytte de fleste enkeltelementer i vårt radikale forslag i ulike mellomløsninger. Vi har imidlertid ikke gitt anvisning på slike mulige modulariseringer, men vil minne om at flere endringsforslag har slik sammenheng at de vanskelig kan gjennomføres alene.

Vi har ikke skrevet særlige motiver til hvert av lovforslagene. Hovedresonnementer og -begrunnelser finnes i den løpende rapportteksten. I rapporten konkluderer vi i stor grad i form av forslag til enkeltbestemmelser som inngår i vårt radikale forslag. Her finnes imidlertid også begrunnelser for våre moderate forslag. Moderate forslag er imidlertid ikke begrunnet direkte men er knyttet til en moderert konklusjon på grunnlag av den samme rapportteksten. Når forslag til lovtekster formuleres som konklusjoner på delproblemstillinger, innebærer dette ikke sjelden at teksten får et noe annet innhold og en noe avvikende form sammenlignet med det samlede lovforslaget i kapittel 13. Dette skyldes bl.a. at kapitler som etterfølger delforslagene begrunner endringer/justeringer. For endelig vurdering av lovforslagene, viser vi derfor til utkastene til lovtekst i kapittel 13.

[12] Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger (heretter også "personverndirektiv").

I arbeidet med radikalt lovforslag, ble mandatets punkter til hinder for å behandle sammenhenger til de deler av loven som Justisdepartementet skal arbeide med, men som det ut i fra den saklige sammenhengen hadde vært naturlig for oss å se nærmere på. Dette gjelder særlig spørsmål vedrørende arbeidsdelingen mellom ulike myndigheter, både mht. tilsyns- og forskriftskompetanse. Uansett ville tids- og budsjettrammer gjort det umulig å utarbeide et fullstendig dekkende lovutkast. Dette er imidlertid snarere en påminnelse om begrensinger i vårt arbeid enn en kritikk av de rammene vi har måttet forholde oss til.

Ved utforming av lovtekstene har vi så langt som mulig tatt hensyn til retningslinjene i Justisdepartementets hefte om lovteknikk. Vi har imidlertid også måttet ta hensyn til den foreliggende lovteksten som endringene skal redigeres inn i. På planet over "teknikk" ligger betraktninger vedrørende hva som kan sies å være "enkle" og "gode" rettsregler. Her vil vi ikke gå inn i denne diskusjonen. Etter vår mening bør imidlertid en lov som henvender seg til hele befolkningen i størst mulig grad gi full informasjon. Det betyr bl.a. at en ikke kan forutsette at rettsanvenderene gjør bred og kvalifisert bruk av rettskildene for å løse tolkningsspørsmål eller for å få oversikt over aktuelle momenter i skjønnsmessige avveininger. Vår holdning har derfor vært at lovteksten skal gi så klar, presis og uttømmende uttrykk for rettsreglene som mulig. Vi kommer ikke her inn på hva som har vært avgjørende for hvor godt en slik målsetting er realisert, men gjør oppmerksom på at det radikale lovforslaget av den grunn er noe mer omfangsrikt enn gjeldende lov. En noe større tekstmengde, skyldes også at vi har valgt å flytte flere bestemmelser opp fra forskrifts- til lovnivå. Dette gjør imidlertid at forskriften vil bli vesentlig redusert. Dessuten er omfanget av forskriften redusert som resultat av materielle endringer i loven. Den samlede tekstmengden i lov og forskrift vil derfor ikke øke. Uansett mener vi det er god grunn til å anta at lesing av en utfyllende tekst gir sikrere og raskere resultater enn en komprimert tekst som krever spesialkunnskaper og/eller videre arbeid med rettskildene.

Mandatet viser dessuten til Utredningsinstruksen og til vurdering av administrative og økonomiske konsekvenser av forslagene. Vi har forsøkt å gjøre slike vurderinger på samvittighetsfull måte, men minner om at vi ikke har hatt tid eller tilgang til særlig kompetanse som har gjort det mulig å samle inn særskilt materiale, eller på annen måte gå i dybden på slike spørsmål. Hensynet til administrative konsekvenser er imidlertid på ett sentralt punkt innarbeidet i det radikale lovforslaget, se forslaget til § 33a annet ledd (vedrørende konsesjonsordning).

# Kapittel 2

## Definisjonene i personopplysningsloven § 2

### 2.1 Om mandatet

I rammen gjengir vi mandatets punkt 1 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Personopplysningslovens definisjoner – begrepene "behandling av personopplysninger" og "behandlingsansvarlig"*

I personopplysningsloven § 2 nr. 2 er "behandling av personopplysninger" definert som "enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter". Definisjonen er vid, noe som medfører at personopplysningsloven muligens får et bredere nedslagsfelt enn det som strengt tatt er nødvendig av hensyn til personvernet. **Utrederne bes også vurdere begrepene "personopplysning" og "personregister", i det minste i den utstrekning det er nødvendig for vurderingen av definisjonen i § 2 nr. 2.**

Departementet ber **utrederne vurdere endringer av definisjonen for å oppnå en viss innsnevring av det saklige virkeområdet for loven**. Eventuelle forslag til endringer må være i samsvar med EU-direktivet.

Begrepet "behandlingsansvarlig" er definert i personopplysningsloven § 2 nr. 4 som "den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes". Den behandlingsansvarlige er lovens pliktsubjekt, og vil også være den ansvarlige dersom pliktene ikke overholdes.

**Utrederne bes vurdere om definisjonen er tilfredsstillende utformet, blant annet tatt i betraktning den behandlingsansvarliges behov for å kunne forutsi sin rettsstilling**. Det er i denne forbindelse ønskelig å få vurdert om det kan være hensiktsmessig at loven eller forskriften utpeker hvem som er behandlingsansvarlig, eventuelt ved en generell karakteristikk av vedkommende, hos de største og mest vanlige aktørene som for eksempel allmennaksjeselskaper, kommuner, departementer, direktorater og tilsyn. Det bør i denne forbindelse ses hen til andre regler, herunder prosessregler, som knytter seg til slike aktører, og hvor ansvaret for andre generelle krav er plassert. Det skal fortsatt legges til grunn at det formelle ansvaret skal plasseres hos den eller de som har partsevne på vegne av selskapet, organisasjonen mv.

Vi forstår første del av dette mandatpunktet som anmodning om en diskusjon av de legaldefinisjoner som har betydning for lovens saklige virkeområde ("personopplysning", "behandling av personopplysninger" og "personregister"). Vårt underlagsmateriale viser at flere av disse begrepene kan være vanskelig å forstå. Det kan derfor også være grunn til å vurdere endringer i definisjonene for å oppnå større grad av klarhet.

Andre del av mandatpunktet ovenfor gjelder presisering av hvem som er "behandlingsansvarlig" og dermed det primære pliktsubjektet i loven. Dette har generell betydning for etterlevelse av lovens bestemmelser, og har dessuten særlig betydning fordi

straffeansvar og økonomisk ansvar er knyttet opp til denne definisjonen, se §§ 48 og 49. I et annet perspektiv er "behandlingsansvarlig" betegnelsen på én av de roller som loven forutsetter. Ytterligere en rolle – "databehandler" – er definert i § 2 nr. 5. Dessuten nevner eller beskriver loven og personopplysningsforskriften flere andre roller, men uten at disse relateres klart til hverandre. I vårt forarbeid til denne utredningen har det fremkommet et stort behov for både å klargjøre rollen som behandlingsansvarlig og denne rollens forhold til andre roller. Vi mener det uansett er lettest å klargjøre "behandlingsansvarlig" dersom en samtidig klargjør de andre roller som inngår i lovens systematikk, og som i stor grad må relateres til rollen som behandlingsansvarlig. Dette innebærer at vi til en viss grad også trekker inn elementer i utvalgte bestemmelser i forskriften om behandling av personopplysninger (heretter "pof").[13]

I tillegg til det som eksplisitt fremgår av mandatets punkt 1, ønsker vi å reise spørsmålet om § 2 med legaldefinisjoner innebærer en hensiktsmessig redaksjon og systematikk. Denne diskusjonen har sammenheng med flere punkter i mandatet. En lettere forståelig utforming av bestemmelser som i dag er formulert som legaldefinisjoner, tilsier mer utfyllende formuleringer – noe som gjør det vanskelig å holde fast ved knappe definisjoner. Dersom en velger en annen løsning enn en oppregning av kortfattede definisjoner, får dette åpenbart konsekvenser for strukturen i og redaksjonen av denne delen av loven, jf. vår generelle diskusjon av strukturspørsmål i kapittel 12. I avsnitt 2.6 gjør vi dessuten enkelte lovtekniske vurderinger som berører sammenhengen med annen lovgivning, spesielt forvaltningsloven.

## 2.2 "Personopplysning"

### 2.2.1 Generelt

Begrepet "personopplysning" er helt sentral for forståelsen av personopplysningsloven. I det følgende analyserer vi viktige aspekter ved begrepet. Analysen synliggjør hvor komplekst dette begrepet er, og identifiserer de viktigste tilknyttede rettsspørsmålene.

"Personopplysning" er basert på personverndirektivet artikkel 2 bokstav a som på engelsk lyder:

> (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Den norske legaldefinisjonen er vesentlig mer kortfattet, men er ikke ment å avvike fra direktivets definisjon:

> 1) personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson.

Den definisjonen som ble foreslått i NOU 1997:19 (jf. s. 164) lå vesentlig nærmere direktivets definisjon, og ga således betydelig mer informasjon om hvilke vurderinger som må skje for å ta stilling til om det foreligger en personopplysning eller ikke. Her gjennomgår vi kortfattet de viktigste avgrensingsspørsmålene i definisjonen, og peker på mulige avgrensinger som kan snevre inn innholdet av definisjonen.

---

[13] Forskrift 15. desember 2000 nr. 1265.

Begrepet ”personopplysning” er helt avgjørende for å ta stilling til om loven gjelder eller ikke, se § 3 om lovens saklige virkeområde. Et innsnevret begrep, vil derfor innebære et snevrere virkeområde. En klargjøring av begrepet, vil innebære at det blir lettere å ta stilling til om loven gjelder eller ikke.

Loven henvender seg til et stort antall personer, som ikke har spesielle forutsetninger for å bruke lovforarbeider, følge med på rettspraksis eller lese faglitteratur. Dersom det kan unngås, er det uansett lite hensiktsmessig å utforme lovgivning på en måte som forutsetter slik innsats fra personer som primært har andre oppgaver. Alle grunnleggende elementer i loven, og i særdeleshet de sentrale legaldefinisjonene, må derfor kunne leses og forstås rimelig presist, uten videre undersøkelser i øvrige rettskilder. Dette tilsier en definisjon der de viktigste vurderingstemaene kommer tydelig frem. En slik tydeliggjøring legger også det beste grunnlaget for en videre diskusjon vedrørende innholdet av definisjonen.

Direktivet bruker ”personal data” om det den norske loven betegner ”personopplysning”. Det samme gjør Europarådets personvernkonvensjon som Norge har ratifisert og som Direktivet bygger på.[14] ”Data” kan peke i retning av en formalisert representasjon (i form av tegn, sifre og lignende) av informasjon som er egnet for overføring, tolking og videre behandling, for eksempel med automatiske hjelpemidler. Denne type forståelse av ”data” er vanlig i fagområdene informatikk og rettsinformatikk.[15] Med en slik tilnærming oppstår informasjon når dataene fortolkes i en bestemt kontekst, for eksempel ut i fra et bestemt formål, i en bestemt beslutningssituasjon eller lignende. En konsekvens er at ”data” kan gi ulik ”informasjon” avhengig av sammenhengen det står i.

Det er usikkert om direktivet og konvensjonen faktisk legger til grunn en informatisk forståelse av ”data” og ”informasjon”. Det at direktivet bruker ”data”, ikke ”informasjon”, som det primære reguleringsobjekt kan tyde på en slik begrepsforståelse: en slik tilnærming er jo et logisk trekk dersom en forutsetter at ”informasjon” kun er det semantiske innholdet som tillegges data. Direktivet (og konvensjonen) definerer imidlertid ”data” som ”any *information*” (vår kursiv), noe som også kan tyde på det ikke skal skilles mellom ”data” og ”informasjon” i tråd med en informatisk tilnærming til begrepene. Et skille mellom begrepene kunne muliggjort en vesentlig innsnevring av personopplysningslovens saklige virkeområde. Dette ville imidlertid neppe vært i tråd med direktivet (eller konvensjonen), og skillet vil konkret kunne være vanskelig å trekke. ”Personopplysning” er innarbeidet, og det skal derfor meget sterke grunner til for å endre på lovens bruk av dette begrepet. Den videre diskusjonen forutsetter at begrepet beholdes, og at eventuelle innsnevringer kun gjelder det begrepsmessige innholdet.

### 2.2.2 Ulike uttrykksformer

Personopplysninger kommer til uttrykk på mange ulike måter, og definisjonen av ”personopplysning” dekker en hvilken som helst uttrykksmåte; dvs. i tekst, bilde, lyd, opplysning om person generert av ulike typer sensorer (iris-gjenkjenning, bevegelsessensor mv.). Mange har klare assosiasjoner til opplysninger i form av tekst når de leser loven, noe som raskt vil lede til feiloppfatninger. Det er derfor etter vår mening grunn til å vurdere om

[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (E.T.S. No. 108), vedtatt 28.1.1981, i kraft 1.10.1985 (heretter også ”Europarådskonvensjonen”).

[15] Jf. for eksempel Dahlbom og Mathiassen 1993 s. 26–27; Andersen 1989 s. 15; Bing 1988 s. 111; Selmer 1995.

dette aspektet bør komme klarere frem i tilknytning til definisjonen. I avsnitt 2.2.8 innarbeider vi et forslag til lovtekst i bestemmelsens annet ledd som tydeliggjør at personopplysninger kan fremkomme på mange ulike måter.

Vi forstår direktivet slik at det ikke er rom for å snevre inn definisjonen på dette punktet, ved for eksempel å ekskludere opplysninger i form av lyd eller lignende. Direktivet dekker i utgangspunkt behandling av personopplysninger i form av lyd eller bilde, jf. punkt 14 og 16 i direktivets fortale.[16]

### 2.2.3 Opplysningstype og opplysningsverdi – herunder om sensitive opplysninger

Det kan reises spørsmål om "personopplysning" betegner en opplysnings*type* eller en *–verdi* (forekomst). Denne spørsmålsstillingen skyldes måten persondatasystemer er bygget opp, dvs. innretningen av persondatabaser og -registre mv. Systemet/registeret vil inneholde en klassifisering av de ulike opplysningene som skal inngå i systemløsningen. For eksempel velger en opplysninger vedrørende opplysningstypene adresse, sivil status, alder, inntekt, diagnose osv. Disse blir fastlagt når databasen/registeret utformes, lenge før det blir registrert én eneste konkret forekomst (opplysningsverdi). Mange av lovens bestemmelser skal vurderes før konkrete opplysninger faktisk blir registrert. På det tidspunktet loven krever etterlevelse av disse bestemmelsene, er det derfor ikke mulig å vurdere annet enn opplysnings*typene*. Således må alle krav i loven som må oppfylles før behandling av personopplysninger starter, primært gjelde de opplysningstyper som det er plan om å behandle. I tillegg kan en selvsagt legge til grunn *forventninger* om hvilke opplysningsverdier som vil kunne bli registrert, men dette vil kun være antagelser og kan neppe få stor innvirkning på de rettslige vurderingene.

Personopplysning som opplysningstype kan innebære meget forskjelligartede situasjoner, avhengig av hvor stor grad av formalisering som skjer. Dersom en planlegger opplysningstypen "kjønn", er det kun to verdier som er aktuelle; "mann" og "kvinne". Opplysningstyper kan imidlertid være langt videre og mindre strengt definerte. En opplysningstype kan f.eks. være "partens innsigelser" som kan ha ethvert relevant innhold, eventuelt innenfor plassmessige begrensninger. I mange tilfeller vil det føles anstrengt å operere med skillet mellom opplysningstype og opplysningsverdi. For eksempel vil utsagn i dagligprosa, fremsatt på internettside om ansatte i barnevernet, være en ytring som det ikke er naturlig eller vanlig å tenke på som en "personopplysning" av en viss type og viss verdi; her smelter de to elementene sammen.

For den enkelte som ønsker å ivareta sine personverninteresser, er det mindre interessant hvilke opplysningstyper som det er lagt til rette for i datasystemet. Her er det forekomsten av konkrete opplysninger om personen som er viktig. Personer kan ønske at opplysninger om dem blir slettet, rettet eller supplert, men det er av mindre betydning at systemløsningen rommer en mulighet for å registrere visse opplysningstyper.

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

[16] Etter artikkel 33 skal EU-kommisjonen undersøke anvendelsen av direktivet til behandling av slike opplysninger og foreslå "appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society". En kartlegging av hvordan EU-medlemsstater har implementert direktivet i forhold til slike opplysninger finnes i British Institute of International and Comparative Law 2003.

hensiktsmessig definisjon av "personopplysning". Spørsmålet kan begrunne at en i visse bestemmelser understreker at det er personopplysnings*type* det siktes til. Dette er gjort fire steder i den gjeldende lovteksten.[17] 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 opplysning*typer*, 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: opplysning*styper 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) medlemsskap 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. Den foreslåtte presiseringen innebærer at behandlingsansvarlige må gjøre en konkret sensitivitetsvurdering. I eksempelet med Ila fengsel, vil adresseopplysninger knyttet til innsatte personer bli å anse som sensitive, fordi adresselisten "er egnet til å åpenbare … at en person har vært … dømt for en straffbar handling."[18]

### 2.2.4 Opplysninger om levende og døde personer

Begrepet "personopplysning" dekker i utgangspunktet bare levende personer.[19] Etter vår mening bør dette klart fremgå av lovteksten, bl.a. fordi spørsmålet har stor betydning for langtidslagring av informasjon og arkivverket. Imidlertid vil enkelte opplysninger om avdøde mennesker samtidig være opplysninger om levende mennesker, jf. neste avsnitt om forholdet mellom fysiske og juridiske personer. Det kan være vanskelig å avgrense de opplysninger som kan sies å gjelde både en levende og død person. For eksempel kan opplysninger om foreldres familieforhold ses som en opplysning om alle personer (særlig barn) som levet i familieforholdet. "Avdøde NN var barnemishandler", kan for eksempel ses som en

---

[17] Se § 3 fjerde ledd (saklig virkeområde), § 18 første ledd bokstav d (rett til innsyn), § 21 første ledd bokstav b (informasjonsplikt ved bruk av personprofiler) og § 32 første ledd bokstav e (meldingens innhold).

[18] Jf. forvaltningsloven § 13 annet ledd som også lar taushetsplikten omfatte ellers åpne personopplysninger dersom "opplysninger røper et klientforhold eller andre forhold som må anses som personlige".

[19] Se Ot.prp. nr. 92 (1998–1999) s. 102.

opplysning om NNs barn, og kanskje også om personens ektefelle. I andre tilfeller er det en så klar sammenheng mellom opplysninger om familiemedlemmer at det ikke kan være tvil at opplysningen gjelder flere. Dette gjelder eksempelvis opplysninger om slektskaps- og adopsjonsforhold og opplysninger om arvelige sykdommer mv., jf. "moren fødte barn som hadde skader pga hennes alkoholmisbruk", og "faren har Huntingdons sykdom". En avgrensing av personopplysningsbegrepet i forhold til avdøde mennesker, bør formuleres slik at kun opplysninger om en avdød person som med stor sikkerhet også er opplysning om en eller flere levende personer er omfattet. Vi mener følgende formulering langt på vei dekker denne målsettingen:

> Opplysninger om døde personer som samtidig er opplysninger om levende personer, regnes bare som personopplysninger dersom de gjelder den levende personens familiemessige relasjoner eller arvelige, helsemessige forhold.

### 2.2.5 Fysiske og juridiske personer

Lovens definisjon av personopplysning vedrører "en enkeltperson". Det er samtidig klart at dette – i utgangspunktet – ikke omfatter *juridiske* personer, dvs. organisasjoner, virksomheter, bedrifter mv. Avgrensingen mot juridiske personer skaper særlig to utfordringer. For det første vil opplysninger om en persons relasjon til juridiske personer både fremstå som en opplysning om den fysiske og den juridiske personen. At NN er ansatt i Justisdepartementet er både en opplysning om NN og om Justisdepartementet. Spørsmålet kommer på spissen i tilfeller der person- og firmanavn er likt – noe som ofte kan skje med enkeltmannsbedrifter mv. Opplysninger om et enkeltmannsforetak kan falle inn under loven i den grad de kan knyttes til den fysiske personen bak foretaket.[20] Slik overlapping er neppe til å unngå, men det kan være grunn til å tydeliggjøre skillet mellom opplysninger om fysiske og juridiske personer.

Som nevnt vil opplysninger som både er knyttet til en fysisk og en juridisk person, i utgangspunktet regnes som "personopplysning". For å snevre inn personopplysningsbegrepet og samtidig gjøre det klarere, er det mulig å kvalifisere en delmengde av slike opplysninger som "personopplysninger":

> Opplysninger som både gjelder fysiske personer og organisasjoner, regnes bare som personopplysninger dersom de direkte gjelder personers posisjoner, klientforhold, personlige relasjoner, handlinger, preferanser, evner eller behov.

Andre opplysninger om juridiske personer vil dermed falle utenfor definisjonen og dermed lovens saklige virkeområde. Bruk av kriteriet "direkte" signaliserer at dersom det er knyttet et organisasjonsnummer (og ikke fødsels- og personnummer) til en opplysning, vil ikke opplysningen regnes som "personopplysning".

Skillet mellom fysiske og juridiske personer skaper også problemer fordi kredittopplysninger om andre enn enkeltpersoner er omfattet av loven i medhold av personopplysningsforskriften § 4-1 annet ledd.[21] Behandling av kredittopplysninger om et selskap, en forening, stiftelse mv., skal etter dette reguleres av personopplysningsloven, *selv om* det ikke er tale om

[20] Ot.prp. nr. 92 (1998–1999) s. 102. Sml. NOU 1997:19 s. 54 der det står at "opplysninger om enkeltmannsforetak alltid vil være opplysninger om fysiske personer".

[21] Jf. hjemmelen i pol § 3 siste setning.

opplysninger om fysiske enkeltpersoner og således faller utenfor lovens saklige virkeområde. Hva som regnes som kredittopplysninger følger av pof § 4-2 som definerer kredittopplysningsvirksomhet.

Det er etter vår mening ønskelig at juridiske personer har vern i forbindelse med kredittopplysningsvirksomhet. Vi mener likevel at det er ønskelig å holde fast ved at personopplysningsloven kun gjelder opplysninger om fysiske enkeltpersoner, noe som også er i tråd med direktivet (”natural person ('data subject')”). Loven skal ”[…] beskytte den enkelte mot at personvernet blir krenket […]” (jf. § 1). Lovens anvendelse på kredittopplysninger om juridiske personer i henhold til personvernforskriften, kommer i konflikt med dette ønsket om å renskjære lovens saklige virkeområde. Den beste lovtekniske løsningen vil etter vår mening være å plassere en bestemmelse tilsvarende den i pof § 4-2 annet ledd i annen lovgivning vedrørende bank og finansieringsvirksomhet mv. Vi tar imidlertid ikke stilling til den nøyaktige plassering av en slik bestemmelse.

### 2.2.6 Forholdet mellom personopplysninger og fysiske ”personobjekter”

I definisjonen av ”personopplysning” heter det at dette gjelder ”opplysninger og vurderinger som kan *knyttes til* en enkeltperson” (vår kursiv). I kravet om sammenknytning ligger det tilsynelatende en forutsetning om at en ”personopplysning” og en (fysisk) ”enkeltperson” ikke kan være det samme. Spørsmålet kommer på spissen i tilfeller der humant biologisk materiale kan brukes til å si noe om den personen som dette materialet stammer fra, for eksempel i tilknytning til DNA-analyse. Behovet for personvern og integritetsvern ellers i slike sammenhenger er åpenbart. Spørsmålet er imidlertid om én og samme lov bør forstås slik at den både regulerer konkrete fysiske/fysiologiske forhold og forhold vedrørende informasjon om fysiske personer.

Dersom man forstår ”person*opplysning*” i retning av ”data” slik vi var inne på i avsnitt 2.2.1, dvs. som et ufortolket materiale som er knyttet til en person, er det mulig at også humant materiale kan innfortolkes i definisjonen og dermed i lovens saklige virkeområde.[22] Skal man være konsekvent, vil en slik fortolkning imidlertid ha overraskende og dyptgripende konsekvenser. I så fall kan ikke bare små bestanddeler fra den menneskelige kroppen (f.eks. celler) ses som ”personopplysning”, men også organer, deler av organer og – prinsipielt sett – hele menneskekropper.[23]

Humant materiale i biobanker er regulert i biobankloven,[24] jf. lovens § 3 første ledd. Opplysninger som er utledet av slikt materiale skal reguleres av personopplysningsloven, helseregisterloven[25] eller annen særlig personopplysningslovgivning, se § 3 annet ledd. Det er da nærliggende å mene at humant materiale utenfor biobanker heller ikke bør anses å være ”personopplysning” før opplysninger faktisk er utledet fra materialet.

---

22 Dersom en derimot anser ”data” som betegnelse på formaliserte tegn, sifre ol som er ment å *representere* noe (en gjenstand eller prosess) fra ”den virkelige verden” (og ikke objektene/prosessene selv), er det vanskeligere (dog ikke umulig) å hevde at humant biologisk materiale kan være opplysninger.

23 I hvert fall dersom en ikke forutsetter at det humane materialet er *borttatt* fra kroppen. Sml. biobankloven § 2 tredje ledd hvor humant biologisk materiale er definert som ”[…] organer, deler av organer, celler og vev og bestanddeler av slikt materiale fra levende og døde mennesker”.

24 Lov 21. februar 2003 nr. 12.

25 Lov 18. mai 2001 nr. 24.

Personvernnemnda har tatt stilling til spørsmålet om humant biologisk materiale kan regnes som "personopplysning" i henhold til personopplysningsloven, se klagesak 2002 nr. 8.[26] Flertallet av nemndas medlemmer uttalte at man bør tolke personopplysningsloven slik at det ble opprettholdt "et så skarpt skille som mulig mellom personopplysninger og biologisk eller organisk materiale". Dette standpunktet innebærer at humant materiale ikke i seg selv er å anses som "personopplysning". Identifiserende elementer og analysedata knyttet til slikt materiale, vil imidlertid kunne falle innenfor definisjonen.

Spørsmålet om forholdet mellom humant biologisk materiale og helseopplysninger (dvs. en type "personopplysninger", se helseregisterloven § 2 nr. 1), ble også drøftet av Helseforskningsutvalget, som ga følgende begrunnelse for å skjelne mellom opplysninger og humant materiale:

> Humant biologisk materiale er som nevnt *fysiske objekter* og stiller derfor andre krav til oppbevaring, vedlikehold, utlevering og destruksjon enn det helseopplysninger gjør. […]
> Humant biologisk materiale skiller seg i tillegg fra helseopplysninger ved at det kan gjøres nye analyser, og spesielt at det kan analyseres i lys av fremtidig kunnskap med hittil ukjente metoder. Utvalgets forslag innebærer at nye analyser må begrunnes, forhåndsgodkjennes, og bekjentgjøres, og at alle analyseresultater skal reguleres som helseopplysninger.[27]

I forslaget til helseforskningslov[28] resulterte disse overlegningene i separate men koordinerte bestemmelser om behandling av henholdsvis helseopplysninger og humant biologisk materiale, se lovforslagets kapitler 6 og 7. Både Biobankutvalget og Politiregisterutvalget har imidlertid inntatt et annerledes standpunkt pga. den nære sammenhengen mellom biologisk materiale og opplysninger som er fremkommet eller kan fremkomme ved analyse av materialet.[29] Biobankutvalget mente likevel at helseregisterlovens bestemmelser ikke gjelder direkte for biologisk materiale.[30]

De aller fleste EU-medlemstaters lovgivning om personopplysningsvern gir ingen direkte eller uttrykkelig beskyttelse til humant biologisk materiale, og få staters myndigheter synes å ha inntatt et offisielt standpunkt på problemstillingen.[31] Datatilsynet i Danmark har derimot bestemt at humant biologisk materiale kan være personopplysninger i henhold til den danske personopplysningsloven[32] og at en ikke-elektronisk systematisk samling av slikt materiale i en biobank kan utgjøre et manuelt register etter lovens § 1 stk. 2.[33]

Etter vår mening er det behov for å avgrense "personopplysning" mot humant biologisk materiale av ethvert slag og i enhver form. Loven blir åpenbart lettest å forstå og praktisere med en slik presisering på plass. Dersom lovgiver skulle ønske også å innbefatte humant materiale, må dette uansett klart fremgå av loven, og hver enkelt bestemmelse må prøves og

---

[26] Til grunn for nemndas vedtak lå bl.a. en utredning av spørsmålet fra førsteamanuensis Lee A. Bygrave ved Universitetet i Oslo, se <http://www.personvernnemnda.no/vedtak/2002_8_vedlegg.htm>. Saken gjaldt sletting av biologisk materiale med tilhørende personopplysninger som var blitt "gjenglemt" ved Ullevål sykehus da den forsker som hadde konsesjon fra Datatilsynet til å behandle opplysningene hadde sluttet i sin stilling ved sykehuset.

[27] Jf. NOU 2005: 1, avsnitt 29.1.

[28] Jf. NOU 2005: 1.

[29] Jf. NOU 2001: 19 s. 22 og 73, og NOU 2003: 21 s. 142.

[30] NOU 2001: 19 s. 120.

[31] Jf. Beyleveld m.fl. 2004 s. 193–197.

[32] Lov 31. mai 2000 nr. 429 om behandling af personoplysninger.

[33] Jf. Datatilsynets journal nr. 2000-321-0049. Saken er kort omtalt i Datatilsynets årsberetning for 2000, tilgjengelig ved <http://www.datatilsynet.dk/publikationer/index.html>. Vedtaket gjelder fremdeles.

forklares i forhold til slik anvendelse (jf. f.eks. reglene om retting og sletting av personopplysninger i pol §§ 27 og 28).

Følgende forslag til presisering, tydeliggjør dette skillet og innebærer en presisering av "personopplysning" og dermed lovens saklige virkeområde:

> Humant biologisk materiale (inklusive bestanddeler av slikt materiale) regnes ikke i seg selv som personopplysning etter denne loven.

### 2.2.7 Krav til persontilknytning og identifikasjon

Begrepet personopplysning forutsetter en *mulig* tilknytning mellom personinformasjon og en bestemt person (jf. "[…] *kan knyttes til* en enkeltperson […]", vår kursiv). Det er med andre ord ikke påkrevet at opplysninger faktisk *er* knyttet til en person, men nok at dette foreligger som en mulighet. Denne egenskapen ved definisjonen har meget stor innvirkning på spørsmålet om lovens saklige virkeområde, og innebærer at mange opplysninger må bli behandlet i samsvar med loven selv om den behandlingsansvarlige aldri vil gjøre bruk av persontilknytningen.

En mulig innsnevring av definisjonen kan være å kreve at det faktisk vil bli etablert en tilknytning mellom en opplysning og en bestemt person for at det skal sies å foreligge "personopplysninger". En slik endring ville gi betydelige konsekvenser, fordi opplysninger som kun er knyttet til erstatninger for personidentitet ikke vil bli regnet som "personopplysning" før den virkelige identiteten er etablert. Opplysninger som kun er knyttet til IP-numre,[34] mobilnumre, personnumre, pseudonymer osv ville i så fall ikke være personopplysninger før de faktisk ble knyttet til en person.

Det er flere vanskelige problemer knyttet til en slik innsnevring av definisjonen. Et åpenbart problem er at flere slike "mellomstasjoner" gjør det så lett å etablere virkelig identitet at det er liten grunn til å legge vekt på at personidentitet ikke inngår. Dette gjelder eksempelvis for mobilnumre og bolignumre. Et annet problem er at enkelte "mellomstasjoner" er entydige adresser for kommunikasjon (IP-numre, telefonnumre, bolignumre), noe som uansett gjør det lett å bruke opplysningene til å kommunisere med tilknyttede personer uavhengig av hvilken nærmere identitet de har. En slik innsnevring av definisjonen av "personopplysning" vil etter vår mening uansett gi så vidtrekkende og usikre resultater at det ikke kan tilrådes. Vi mener dessuten det vil stride mot direktivets bestemmelser, se straks nedenfor.

En mulig innskrenkning av "personopplysning" som er beslektet med den vi har nevnt ovenfor, er å konkret angi at bestemte opplysninger som er knyttet til pseudonymer ikke skal regnes som "personopplysninger" så lenge virkelige identiteter ikke er tilknyttet. Det vil da foreligge personopplysninger frem til pseudonymisering har skjedd, og dessuten ved eventuell tilbakeføring til virkelig identitet. Så lenge opplysningene er pseudonyme ville loven eller deler av den, med andre ord ikke gjelde. Alternativt kunne en tenke seg at pseudonyme opplysninger ikke blir trukket inn i selve definisjonen, men i stedet brukt i en unntaksbestemmelse vedrørende lovens saklige virkeområde. Slik kunne en angi hvilke deler av loven som skal gjelde for, eller ikke gjelde for, pseudonyme personopplysninger. En slik løsning ligner den som er benyttet i § 7 vedrørende kunstneriske formål mv., og som fastsetter at bare en del av loven gjelder i slike tilfeller.

[34] Dvs. nummeret på en datamaskin som er knyttet opp til internettet.

De to sist nevnte endringsmulighetene har den fordel at det vil kunne påvirke behandlingsansvarlige i retning av å pseudonymisere langt flere personopplysninger enn i dag, noe som innebærer at opplysninger ikke kan relateres til enkeltpersoner så lenge pseudonymiseringen opprettholdes. Dette ville i så fall gi en personverngevinst, samtidig som flere virksomheter ville kunne få klare lempinger i kravene til sin informasjonsbehandling. En ulempe er imidlertid at slik pseudonymisering som kan være aktuell må være pålitelig, noe som kan innebære så store kostnader for den behandlingsansvarlige at det derfor vil være uaktuelt. En personvernmessig ulempe er at den registrertes rettigheter til innsyn, informasjon, retting og sletting vil bli kraftig redusert så lenge pseudonymiseringen består.

I direktivet er ”personal data” definert som ”any information relating to an identified or identifiable natural person (‘data subject’)” (artikkel 2 bokstav a). Direktivet synes med andre ord å forutsette at alle opplysninger som kan relateres til en fysisk person må regnes som ”personopplysning”. Direktivets definisjon sier imidlertid også noe om identifiseringsmåten:

> an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Definisjonen legger her opp til to hovedmåter å identifisere på. For det første med et identifikasjonsnummer, dvs. der hvor numre trer i stedet for virkelig identitet. For det andre peker definisjonen på kombinasjoner av andre opplysninger, som til sammen gir grunnlag for å konkludere med hensyn til en persons identitet.

Et pseudonym vil kanskje kunne atskille seg fra begge de tilfeller som direkte er omhandlet i direktivets definisjon. Det kan argumenteres at et pseudonym ikke er et identifikasjons-nummer, fordi slike numre nettopp er kjennetegnet ved at de entydig skal knytte opplysninger til en bestemt person samtidig som identiteten er åpen. Et pseudonym trenger heller ikke være en kombinasjon av andre opplysninger om personers fysiske, sosiale og psykiske forhold mv, men kan være en beregnet størrelse som ikke styres av egenskaper ved aktuelle person, men av avanserte algoritmer mv. Dersom pseudonymer etableres ved hjelp av en pseudonymforvalter, dvs. en tredjemann som må bidra for å avdekke virkelige identiteter, vil heller ikke den behandlingsansvarlige være i stand til å identifisere personene på egen hånd. Punkt 26 i direktivets fortale fastslår at

> … to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person […].

Pseudonymisering kan tenkes utført på måter som innebærer at verken behandlingsansvarlig (”controller”) eller databehandler (pseudonymforvalter) kan skaffe seg tilgang til virkelige identiteter på egen hånd – i hvert fall på lovlig vis og uten uforholdsmessig stor arbeidsinnsats eller uforholdsmessige store kostnader. Gitt at i vurdering av identifiseringsmuligheter skal det i følge punkt 26 i fortalen kun tas hensyn til hjelpemidler som det er *rimelig* å ta i bruk, kan det da stilles spørsmål om det er mulig å foreta pseudonymisering på måter som gjør at opplysningene faller utenfor direktivets definisjon av ”personal data”.

Det er imidlertid vanskelig å fastslå med stor grad av sikkerhet at pseudonymisering (i motsetning til full anonymisering) vil kunne føre til at opplysningene ikke er omfattet av direktivet eller personopplysningsloven. Identifiseringskravet etter direktivet (samt

Europarådskonvensjonen) kan tolkes dithen at det simpelthen går ut på muligheten til å *skille* en person fra andre personer ved å knytte vedkommende til opplysninger (av et eller annet slag).[35] Identifikasjon krever således ikke kjennskap til en persons navn, kun til ett eller flere spesifikke kjennetegn som skiller vedkommende i en gitt kontekst fra andre personer. Det kan argumenteres at et pseudonym av sin natur utgjør et slikt kjennetegn.

Samtidig hersker det (fremdeles) betydelig usikkerhet i EU-/EØS-medlemsland om hvorvidt pseudonymisering skal kunne unngå direktivets krav. Dette gjelder også spørsmålet om hvorvidt direktivet kommer til anvendelse på behandling av personopplysninger med henblikk på full anonymisering av disse.[36]

På bakgrunn av usikkerheten ønsker vi ikke å fastholde eller foreslå at behandling av pseudonymiserte opplysningene faller *helt* utenfor personopplysningslovens virkeområde. Det er likevel lite tvilsomt at pseudonymisering kan betraktes som en "appropriate safeguard" etter flere av direktivets bestemmelser (jf. artikkel 6(1)(b), artikkel 6(1)(e), artikkel 11(2)), dvs. bestemmelser som i hovedsak angår behandling av personopplysninger til historiske, statistiske og/eller vitenskapelige formål. Pseudonymisering kan da – i det minste – legitimere lemping av de kravene i personopplysningsloven som angår slik behandling.

Det kan dessuten vurderes om ikke flere krav etter loven kunne bortfalle dersom det igangsettes en streng form for pseudonymisering som tilfredsstiller nærmere angitte kriterier for "kvalifisert" pseudonymiseringsprosess.[37] En slik prosess ville da innebære at en persons virkelig identitet blir skjult ved bruk av alias eller annet kjennetegn som erstatter alle ekte identifiserende kjennetegn ved personen, og som gjør det tilnærmet umulig å avsløre personens virkelig identitet uten kjennskap til pseudonymiseringsnøkkelen. En slik prosess kan gjøre det forsvarlig å unnta pseudonymiserte opplysninger fra bestemmelser i loven som gir rettigheter til den registrerte (innsynsrett mv.). Vi er imidlertid ikke helt trygge på at dette er rettslig holdbart etter direktivet. Det er selvsagt også grunn til å gjøre en mer inngående vurdering av hvilke bestemmelser i loven det i tilfellet bør unntas fra. En slik tilnærming er etter vår mening uansett rettspolitisk velbegrunnet, bl.a. fordi den må antas å stimulere til større grad av pseudonymisering. Som del av vårt radikale lovforslag inkluderer vi derfor en unntaksbestemmelse med grunnlag i en nærmere spesifisert pseudonymiseringsprosess, jf. forslag til § 3d.

Identifikasjonskravet innebærer at personer må kunne knyttes til en opplysning med en forholdsvis stor grad av sikkerhet og nøyaktighet. Dersom opplysninger er knyttet til et IP-nummer, og denne maskinen har flere brukere, vil det kunne være usikkert hvilken person som opplysningene om bruken av tjenestene på nettet gjelder. Er det 3–4 eller flere kollegaer på et arbeidssted som kan knyttes til "bruksmønsterinformasjonen" for samme felles maskin, vil opplysningene neppe bli regnet som "personopplysning" fordi tilknytningen til en bestemt person er for usikker. Dersom opplysningen derimot gjelder et medlem av en husstand, f.eks. et familiemedlem, tilsier hensynet til privatlivets fred (jf. formålsbestemmelsen i pol § 1) at opplysningen regnes som "personopplysning" selv om det er flere enn 3–4 personer som kan knyttes til opplysningene. Formålsbestemmelsens vektlegging av privatlivets fred, tilsier her mindre strenge krav til nøyaktig identifisering. En mulighet er å presisere at det alltid

[35] Jf. bl.a. Bygrave 2002 s. 43.

[36] Se bl.a. Beyleveld m.fl. 2004 s. 138 flg.

[37] Sml. kriteriene for "avansert" og "kvalifisert" elektronisk signatur i henhold til e-signaturloven § 3 nr. 2 og 3.

foreligger tilstrekkelig identifikasjon så lenge opplysningene kan knyttes til ett av medlemmene av en husstand:

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

En lignende presisering er blitt gjort i Finlands lov om personopplysningsvern[38] som i 3 § nr. 1 definerer "personuppgifter" som

> alla slags anteckningar som beskriver en fysisk person eller hans egenskaper eller levnadsförhållanden som kan hänföras till honom själv eller till hans familj eller någon som lever i gemensamt hushåll med honom.

I forhold til usikker identifisering utenfor husstander (i arbeidslivet, foreninger mv.), vil det være mulig å fastsette at en opplysning ikke regnes som personopplysning dersom usikkerheten gjelder mer enn et visst antall personer, for eksempel 5 personer. Konkret vurdert kan det imidlertid være grunn til å sette grensen både høyere og lavere enn dette, og vi finner det derfor ikke hensiktsmessig å foreslå en klar grenseverdi.

### 2.2.8 Et revidert personopplysningsbegrep

Den foregående gjennomgangen gir grunnlag for å endre lovteksten på flere punkter. Nedenfor formulerer vi et nytt sett av regler der det direkte tas stilling til flere tolkningsspørsmål som i dag oppfattes som vanskelige. Utgangspunktet ligner den gjeldende definisjonen i pol § 2 nr. 1, men er langt mer utfyllende og gir etter vår mening betydelig større grad av klarhet og forutberegnelighet. Presiseringene innebærer dessuten at lovens virkeområde blir betydelig klarere og skarpere avgrenset. Samlet sett vil forslaget gi et noe snevrere virkeområde enn etter dagens lov. Forslaget er dessuten dekkende i forhold til definisjonen i direktivet. Forslaget kan ses som "modularisert", dvs. det er mulig å velge bort ett eller flere av leddene, fra og med annet ledd. Med presiserende bestemmelser fra og med annet til femte ledd, vil en sprenge rammene for en definisjonsliste, tilsvarende den som er valgt i den nåværende lov. En mer omfattende og presis regulering vil derfor kreve en annen redaksjon og endret tekstoppsett i forhold til dagens lovbestemmelser.

Vårt forslag til bestemmelse som angir "personopplysning" er følgende:

> Med "personopplysning" forstår en i denne loven: opplysninger og vurderinger som direkte eller indirekte kan knyttes til en levende identifiserbar, fysisk enkeltperson.
>
> Personopplysninger kan komme til uttrykk som skrift, bilde, lyd eller andre signaler.
>
> Opplysninger om døde personer som samtidig er opplysninger om levende personer, regnes bare som personopplysninger dersom de gjelder den levende personens familiemessige relasjoner eller arvelige, helsemessige forhold.
>
> Opplysninger som kan knyttes til ett eller flere medlemmer av samme husstand regnes alltid som personopplysninger.

[38] Personuppgiftslag / Henkilötietolak 22. april 1999 nr. 523.

> Opplysninger som både gjelder fysiske personer og organisasjoner, regnes bare som personopplysninger dersom de direkte gjelder personers personlige relasjoner, klientforhold, formelle posisjoner, handlinger, preferanser, evner eller behov.
>
> Humant biologisk materiale (inklusiv bestanddeler av slikt materiale) regnes ikke i seg selv som personopplysning i denne loven.

## 2.3 Personregister

Begrepet ”personregister” brukes i loven for å angi det saklige virkeområdet, se § 3 første ledd bokstav b. I personregisterloven av 1978[39] var dette det bærende begrepet i lovgivningen. Personopplysningslovens definisjon lyder:

> personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen (jf. § 2 nr. 3)

Denne definisjonen er nesten identisk med den som tidligere inngikk i personregisterloven § 1. Den norske legaldefinisjonen i pol § 2 nr. 3 skal dessuten tilsvare definisjon av ”personal data filing system” i personverndirektivet artikkel 2 bokstav c:

> any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Direktivets definisjon legger betydelig større vekt på hvor personopplysningene i registeret befinner seg. Dette kunne ha vært av spesiell betydning dersom en benytter begrepet på elektronisk behandling av opplysninger fordi det da lettere kan skje distribuert behandlingen av opplysninger. Imidlertid er helt eller delvis elektronisk behandling regulert uavhengig av om det foreligger et register (”filing system”) eller ikke, og registerbegrepet får bare betydning i tilfelle av manuell behandling. Derfor er formuleringen i den norske loven etter vår mening skjønnsomt utformet og i samsvar med direktivet.

I utgangspunktet gjelder de samme lovbestemmelsene for personregistre som for elektronisk behandling av personopplysninger.[40] ”Register” anvendes flere steder i loven for å angi bestemte informasjonssamlinger, se §§ 10, 26 og 30 første ledd bokstav h. I nevnte bestemmelser brukes imidlertid ikke det generelle uttrykket ”personregister”, men ”register” brukes som betegnelse på bestemte samlinger av opplysninger (”strafferegistre” (§ 10) og ”reservasjonsregister” (§ 26)), samt som allmenn betegnelse (”offentlig register”, § 30). For øvrig brukes ”personregister” for å angi meldeplikt (§ 31) og krav til meldingers innhold (§ 32).

Et vanskelig spørsmål er hva som er personregisterbegrepets ”nedre grense”, dvs. hvor mange personer det må være opplysninger om for at det skal kunne sies å foreligge et register. I klagesak 2005 nr. 1 slo Personvernnemnda fast at navngivelse av to personer ikke er tilstrekkelig. Etter vår mening bør registerbegrepet klargjøres og snevres inn. Nedenfor kommer vi inn på det gjenfinningskriteriet som er lagt til grunn ved fortolkning av

---

[39] Lov om personregistre mm. 9. juni 1978 nr. 48 (heretter også ”pregl”) – nå opphevet.

[40] Imidlertid er personregistre ikke omfattet av detaljerte regler om informasjonssikkerhet i personopplysningsforskriften, se pof § 2-1.

registerbegrepet. Etter vår mening bør det ikke være nok at det finnes tilgjengelig systematikker og/eller hjelpemidler for gjenfinning. Det bør i tillegg stilles krav om at det faktisk er behov for slike gjenfinningsmuligheter. Den eneste begrunnelsen for å skjelne mellom opplysninger i et register og opplysninger i en løpende saksprosa (som i manuell form faller utenfor loven), er jo at registre letter gjenfinning og bruk av personopplysninger. Dersom det imidlertid er et lite antall personer det er opplysninger om, vil det være like raskt å lese igjennom en tekst som er satt opp uten register som med en registersystematisering.

Personvernnemnda har i to klagesaker tatt stilling til spørsmål som er relevante for avgrensning av personregisterbegrepet. I klagesak 2002 nr. 8 måtte Personvernnemnda ta stilling til spørsmålet om humant biologisk materiale som sådann kunne regnes som personopplysninger. Som tidligere nevnt mente nemndas flertall at slikt materiale i seg selv ikke kunne anses å være personopplysninger. Det ligger implisitt i dette standpunktet at en systematisert samling av slikt materiale (alene) ikke kan regnes som "personregister".

I sak 2005 nr. 1 måtte Personvernnemnda ta stilling til spørsmålet om opptak av personstemme kunne anses å være "personregister". I saken ble "gjenfinningskriteriet" spesielt diskutert. Dersom et register ikke klart legger til rette for gjenfinning av opplysninger om bestemte enkeltpersoner, vil ikke dette kriteriet være oppfylt, og det kan ikke anses å foreligge et "personregister". Med utgangspunkt i Høyesteretts "gatekjøkkenkjennelse" som gjaldt fjernsynsopptak,[41] kom Personvernnemnda frem til at lydopptak på kassetter ikke kunne sies å utgjøre et personregister fordi gjenfinningskriteriet ikke var oppfylt når opptaket måtte avspilles for å finne opplysninger.[42]

Etter vår mening kan det ut i fra disse sakene være grunn til å klargjøre og avgrense registerbegrepet noe nærmere. For det første kan det være grunn til å tydeliggjøre gjenfinningskriteriet som del av personregisterbegrepet. Det bør komme bedre frem at for at systematisering skal kunne ha rettslig relevans skal den ha en effekt i forhold til gjenfinningsmulighet.

Når det gjelder biologisk humant materiale har vi i avsnitt 2.2.6 anbefalt at slikt materiale ikke bør regnes som "personopplysning". I så fall vil samlinger av slikt materiale heller ikke kunne utgjøre et "personregister". Når det gjelder annet fysisk materiale som er informasjonsbærere (disker, CD mv.), kan det likevel sies å være et behov for presiseringer, herunder i form av angivelse av kvantitative krav.

---

41 Jf. Rt. 1991 s. 616.

42 Gjenfinningskriteriet er også gjort til del av § 37 annet ledd, og er der et vilkår for at hele personopplysningsloven skal gjelde for fjernsynsovervåkning. Formuleringen lyder: "… lagres på en måte som gjør det mulig å finne igjen opplysninger om en bestemt person". Gjenfinningskriteriet er dessuten fremhevet i forarbeidene (jf. Ot.prp. nr. 92 (1998–99) s. 23–24, 25) for å avgjøre hvorvidt det skjer behandling med "elektroniske hjelpemidler" (jf. § 3 første ledd nr. 1). At kriteriet er relevant i den henseende synes også å følge indirekte av § 37 annet ledd. Direktivet og de fleste andre EU-/EØS-lands lovgivning synes derimot å fokusere på om behandling skjer automatisk ("by automatic means", jf. direktivet artikkel 3 nr. 1), dvs. uten intervensjon av mennesker. Personvernnemnda har i klagesak 2005 nr. 1 dermed valgt å legge til grunn at begrepet "elektroniske hjelpemidler" ikke skal avgrenses ved bruk av gjenfinningskriteriet, men med hensyn til hvorvidt det foregår en automatisert prosess. I angjeldende sak kom nemnda frem til at manuelt opptak av en telefonsamtale ikke utgjorde behandling med elektroniske hjelpemidler, selv om selve opptakerutstyret teknisk sett er elektronisk. Etter nemndas tilnærming vil heller ikke f.eks. opptak av personopplysninger ved bruk av et håndholdt videokamera anses å være behandling med "elektronisk hjelpemidler". Tilnærmingen reiser muligens enkelte problemer, men vi har ikke hatt kapasitet til å utrede disse i denne omgang.

Konklusjonene på diskusjonene ovenfor kan oppsummeres i følgende nye definisjon av ”personregister”:

> Personregister: systematiske fortegnelser over personopplysninger eller lagringsmedier som understøtter gjenfinning av opplysninger om bestemte personer.

Elementet ”eller lagringsmedier” i denne definisjonen er særlig viktig i forhold til opptak av bilde og/eller lyd på ulike typer lagringsenheter. En samling DVDer, alfabetisert etter personnavn og med lyd og/eller bildeopptak av personer (eksempelvis fra jobbintervjuer, overvåkningssituasjoner mv.), må i seg selv regnes som et personregister når systematiseringen letter gjenfinning av person. Det er etter vår mening vanskelig å angi et antall personer som skal utgjøre en nedre grense for hva som skal regnes som et register, men er antallet under 20 kan det være tvilsomt om fortegnelsen ”[…] understøtter gjenfinning av opplysninger om bestemte personer”.

## 2.4 Behandling av personopplysninger

Selv om mandatet ikke eksplisitt ber om analyse av det definerte uttrykket ”behandling av personopplysninger”, tilsier våre undersøkelser at også dette punktet må belyses nærmere. Dette uttrykket – og avledede former – er helt sentralt i loven, dvs. i forhold til virkeområde, alminnelige regler for behandling, rettigheter, konsesjons- og meldeplikt mv. Legaldefinisjonen (jf. § 2 nr. 2) lyder:

> behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Definisjonen gjenspeiler definisjonen i personverndirektivet artikkel 2 bokstav b:

> … 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Det er flere problemer knyttet til denne definisjonen og dermed til helt grunnleggende forståelser av loven. Et grunnleggende problem oppstår fordi definisjonen i § 2 nr. 2 tar utgangspunkt i verbformen (å behandle), mens ”behandling” ofte oppfattes som en substantivform (en behandling). Det som skal behandles (og meldes mv.) blir derfor ofte betegnet (”behandlingen”), dvs. i bestemt form. Dermed ”sklir” omtalen mellom handlinger og objekter/ting. Observasjoner om språkbruk betyr imidlertid ikke at det ikke er mulig å lese lovteksten utelukkende som beskrivelse av en (type) handling. Problemet er at behandlingen skjer med hjelpemidler (systemer, registre) som oppfattes som ting. Dermed er det nærliggende å fokusere på dette hjelpemiddelet i stedet på selve handlingen. I tillegg kommer at behandlingen i loven er forutsatt å skje ”med elektroniske hjelpemidler” (§ 3 første ledd bokstav a). Hjelpemiddelet er med andre ord satt i sentrum i viktige deler av loven (saklig virkeområde), men er ikke forutsatt å spille noen rolle i forhold til rettigheter, melde- og konsesjonsplikt mv. Dette kan sies å innebære en inkonsistens som gjør det vanskelig å få et klart bilde av lovens bestemmelser.

Etter vår mening er det grunn til å alvorlig vurdere om to ulike termer bør brukes for å betegne ”behandling” som henholdsvis handling og objekt. En mulighet er at konsesjons- og meldeplikten knyttes opp til objekter, for eksempel i form av ”informasjonssystemer”.

Det er også et problem at ”behandling” er et dagligdags og lite presist ord, noe som legger til rette for assosiasjoner og oppfatninger som det ikke er grunnlag for i rettskildene. For eksempel er det lett å forstå ”behandling” som en betegnelse på konkret/individuell behandling av personopplysninger, selv om det primært er *type* behandling, særlig sett i forhold til et eller flere formål, en ønsker å angi.[43] Direktivet benytter ”processing”, og begrepet ”prosessering” ville bedre markert at det ikke dreiet seg om noe dagligdags som (ofte) er av teknologisk karakter. Videre går det frem av direktivet at en ”processing” består av ”operations”, dvs. at det utføres operasjoner (handlinger) på personopplysningene. Også dette blir mer presist, men brukt på denne måten er både ”prosessering” og ”operasjoner” antagelig mest egnet til å fremmedgjøre den vanlige brukeren av loven.

Et tredje problem er at ”behandling av personopplysninger” ikke knytter an til andre kjennetegn ved informasjonsbehandlingen. Det etableres med andre ord noe nytt som ikke er relatert til andre beskrivelser av informasjonsbehandlingen. Personopplysninger vil for eksempel alltid bli behandlet i et ”informasjonssystem” eller ”datasystem”, eller mer presist i ”personalsystemer”, ”epostsystemer”, ”arkivsystemer” mv. Selv om slike systembetegnelser ikke alltid er lett avgrensbare, utgjør de størrelser som mange som skal etterleve loven (for den behandlingsansvarlige) kjenner. En kunne også tenke seg en tilnærming der ”behandling” ble knyttet opp til resultater av behandlingen. Således inngår for eksempel mange behandlinger av personopplysninger i beslutningsprosesser, for eksempel slik at det treffes et enkeltvedtak, etableres et kundeforhold eller lignende. Der det ikke skjer en beslutning, vil det ofte utføres en transaksjon, for eksempel en betalingstransaksjon. Det er etter vår mening en utfordring å tilpasse personopplysningslovens behandlingsbegrep slik at det blir lettere enn i dag å forstå sammenhenger med annet kjent systematikk vedrørende informasjons-behandling, slik vi her har nevnt noen eksempler på.

Behandlingsbegrepet inngår ikke direkte i mandatet for vårt oppdrag, og endret språkbruk i samsvar med vurderingene i dette avsnittet ville få så store konsekvenser, at vi har valgt å ikke fremme forslag om dette.

## 2.5 Behandlingsansvarlig

### 2.5.1 Generelt

”Behandlingsansvarlig” er i følge pol § 2 nr. 4:

> den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.

Loven regulerer i stor utstrekning den behandlingsansvarliges forhold, bl.a. ved å pålegge plikter og ved å gi registrerte personer rettigheter overfor den behandlingsansvarlige. For at loven skal ha tilfredsstillende effekt, er det derfor helt avgjørende at det er lett å fastslå hvem

[43] Det skal således ikke sendes melding til Datatilsynet hver gang en behandler personopplysninger, men når en igangsetter en ny *type* behandling.

som er behandlingsansvarlig. Dessuten gjelder straffeansvar og erstatningsansvar for den som har behandlingsansvaret, se §§ 48 og 49.

"Behandlingsansvarlig" tilsvarer direktivets "controller" som i artikkel 2 bokstav d er definert som:

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

Også på dette punktet er personverndirektivet mer utfyllende enn den norske loven, men det er neppe videre innholdsmessig forskjell mellom de to formuleringene. For det første er det på det rene at både en fysisk og en juridisk person kan være behandlingsansvarlige. Det er imidlertid ikke alltid klart hvor ansvaret for juridiske personer skal plasseres. Dette gjelder særlig spørsmålet om plassering av behandlingsansvar i større selskapsstrukturer og innen de ulike hierarkiske nivåene i offentlig forvaltning. Dessuten er det til en viss grad uavklart i hvilken grad enkeltpersoner hos en behandlingsansvarlig virksomhet har et personlig ansvar.

"Behandlingsansvarlig" forekommer i formen "databehandlingsansvarlig" i helseregisterloven og tilhørende forskrifter. "Data" er her lagt til for å understreke at det ikke dreier seg om medisinsk behandlingsansvar. Også i valutaregisterloven er behandlingsansvarlig definert, men her på en måte som avviker fra personopplysningslovens og personverndirektivets definisjon: "Den enhet som er gitt i ansvar å samle inn opplysninger samt vedlikeholde og drifte registeret", se lovens § 2 nr. 3. Registeret inneholder personopplysninger, og definisjonen må derfor forstås i samsvar med personverndirektivets definisjon.

Også den norske loven åpner for delt behandlingsansvar, men lovteksten er taus om dette og forarbeidene gir bare veiledning i situasjoner der behandlingsansvar er delt mellom et over- og et underordnet forvaltningsorgan. I departementets merknader til § 2 nr. 4 er det også nevnt en mulighet for å fastsette i lov hva som skal være formål for en behandling og hvilke hjelpemidler som skal benyttes, jf. direktivet artikkel 2 bokstav d. Forskjellen mellom direktivet og personopplysningsloven er på dette punktet primært at direktivet eksponerer flere tolkningsspørsmål enn det den knappe norske definisjonen gjør.

De nevnte og andre tolkningsspørsmål fremstår i dag som til dels vanskelige å ta stilling til. Dessuten har behandlingsansvarlig flere roller knyttet til sin virksomhet, for eksempel rollen som "daglig ansvarlig" (jf. pol § 32 bokstav c), og daglig leder (jf. pof § 2-7). I tillegg er det flere roller som ligger mer implisitt i bestemmelsene, for eksempel sikkerhetsrevisor (jf. pof § 2-5). Et synspunkt som ble fremholdt av flere av våre kilder var at det kan være vanskelig å danne seg et klart bilde av hva behandlingsansvaret innebærer uten å gå nærmere inn på de ulike rollene den behandlingsansvarlige kan/skal ha. På lignende måte kan det være fruktbart å tydeliggjøre ansvar andre aktører har; særlig gjelder dette klargjøring av "databehandlers" stilling, se nedenfor i avsnitt 2.6.8.

### 2.5.2 Den behandlingsansvarliges bestemmelsesrett

I følge definisjonen av "behandlingsansvarlig" skal denne bestemme *formålet* med behandling av personopplysninger, og hvilke *hjelpemidler* som skal anvendes som ledd i behandlingen. Samtidig pålegges det imidlertid den behandlingsansvarlige å etterleve en lang rekke plikter

etter loven, og det settes opp skranker for hva den behandlingsansvarlige kan foreta seg med opplysningene. Slike plikt- og forholdsnormer forutsetter en langt videre bestemmelsesrett enn det som direkte gjelder formål og hjelpemidler. Sagt med andre ord, vil det være meningsløst å tillegge behandlingsansvar til en person eller virksomhet som *bare* har bestemmelsesrett med hensyn til formål og hjelpemidler. Imidlertid kan slik bestemmelsesrett være en indikasjon på rett til å bestemme også over de mange andre forhold som loven regulerer.

Etter vår mening er med andre ord definisjonen av "behandlingsansvarlig" lite dekkende, og ikke i samsvar med de krav som i loven stilles til den ansvarlige. Dette er imidlertid en svakhet som også hefter ved den tilsvarende definisjonen av "controller" i personverndirektivet. En endring av ordlyden av den norske definisjonen av "behandlingsansvarlig" for å sikre en klarere og mer konsistent etterlevelse av loven og dermed en lojal etterlevelse av direktivet, er neppe i konflikt med direktivet. Det er imidlertid et poeng at elementene i direktivets og den norske lovens definisjon (hjelpemidler og formål), fortsatt bør inngå. Økt presisjonsnivå bør primært kommer som tillegg til den nåværende lovteksten. Vi foreslår derfor følgende definisjon av "behandlingsansvarlig":

> Med behandlingsansvarlig forstår en i denne loven en virksomhet eller person som har rett til å bestemme over behandling av personopplysninger i siste instans, herunder over formålet med behandlingen og hvilke hjelpemidler som skal brukes.

Presiseringen "i siste instans" er uttrykk for at behandlingsansvaret kan delegeres, og at den behandlingsansvarlige er den med øverste bestemmelsesrett. Den som får delegert behandlingsansvar til seg, opptrer således på vegne av behandlingsansvarlige, men er selv ikke behandlingsansvarlig.

### 2.5.3 Behandlingsansvarlig som fysisk eller juridisk person

"Behandlingsansvarlig" kan være en fysisk eller juridisk person, men der det er en juridisk person som bestemmer over behandlingen av personopplysninger, må loven forstås slik at det er den juridiske personen som alltid har behandlingsansvaret. I slike tilfeller eksisterer det med andre ord ingen valgfrihet vedrørende plassering av ansvaret. Personer kan være adressater for det ansvaret den juridiske personen har, dvs. slik at ansvaret er knyttet til virksomhet XX v/ den øverste ledelsen. Den øverste ledelsen kan være et styre, en person som er daglig leder, eller lignende.

Slik "behandlingsansvarlig" er definert i loven, synes den å forutsette at det *faktisk* er truffet bestemmelser vedrørende formål og hjelpemidler, og at en formell rett til å bestemme ikke er nok. Et tilsvarende fortolkningsproblem gjelder direktivets definisjon av "controller" ("*determines* the purposes and means", vår kursiv). Også etter direktivet er det derfor fare for en pulverisering av ansvar med mindre en også tar hensyn til den potensielle bestemmelsesretten som en ledelse har overfor behandling av personopplysninger som helt eller delvis skjer i tilknytning til virksomheten, i regi av egne ansatte eller i samarbeid med eksterne.

Etter vår mening bør en juridisk person ikke kunne la være å utøve behandlingsansvar og på det grunnlaget hevde at virksomheten ikke er ansvarlig for behandlingen. I de fleste tilfeller er det klart hvilken juridisk person som har den formelle kompetansen til å bestemme.

Uklarhetene oppstår primært dersom behandlingen skjer i et samarbeid mellom flere juridiske eller fysiske personer, uten at det er gjort nærmere avtale om hvorledes ansvaret skal fordeles.

Et lignende spørsmål er om behandlingsansvaret også omfatter behandling som underordnede i den behandlingsansvarlige organisasjon utfører selv om behandlingen ikke har vært gjenstand for noen beslutning, men skjer ut i fra ansattes selvstendige initiativ eller lignende. Spørsmålet er ikke drøftet i forarbeider eller – så vidt vi vet – i forvaltnings- eller rettspraksis. Mye taler imidlertid for å tydeliggjøre et ansvar for den juridiske personen i tilfeller der det kunne ha vært utøvet styring og instruksjon med medarbeiderene. En juridisk person bør imidlertid ikke uten videre ha behandlingsansvar for illojal og/eller ulovlig behandling av personopplysninger som ansatte utfører uten den behandlingsansvarliges vitende. I hvert fall gjelder det så lenge den juridiske personen har opptrådt aktsomt.

Vi antar etter dette at det kan være grunn til å klargjøre at "behandlingsansvarlig" også betegner en posisjon med formell/potensiell rett til å bestemme over formål og hjelpemidler knyttet til behandlingen av personopplysninger.

Det er en forutsetning for at behandlingsansvaret kan legges til en juridisk person at denne virksomheten har sivilprosessuell partsevne, dvs. at virksomheten kan opptre som saksøkt i en tvist for domstolene, se tvisteloven[44] § 2-1. Dersom virksomheten er så løst organisert at den ikke har partsevne, må behandlingsansvaret tillegges de juridiske eller fysiske personer som deltar i den løse organisasjonsstrukturen. Forholdsvis løse og virtuelle og/eller nettverkslignende organisasjoner er praktisk innen en rekke livsområder, og ikke minst i forbindelse med nærings- og forvaltningsvirksomhet knyttet til internettet. Mangfoldet av organisatoriske løsninger kan imidlertid gjøre det vanskelig å foreskrive enkle og dekkende løsninger på hvorledes behandlingsansvaret skal plasseres.

I mange tilfeller vil fysiske personer ha behandlingsansvar. Dette gjelder for det første når de handler på egne vegne, og for det andre når de deltar i et samarbeid som er for løst til å utgjøre en juridisk person med partsevne. Dersom enkeltpersoner driver næringsvirksomhet, og behandlingen av personopplysninger skjer innenfor rammene av denne, vil imidlertid ansvaret ligge på foretaket, dvs. på den juridiske personen. Behandlingsansvaret kan med andre ord både ligge på en juridisk person med én person som deltaker og en juridisk person som utgjør en stor og kompleks organisasjon. Det er åpenbart en stor utfordring å utforme behandlingsansvaret på en måte som passer i forhold til begge ytterpunkter.

Når en juridisk person har behandlingsansvaret kan det stilles spørsmål om hvem som skal utøve dette ansvaret. Oppfatningen har vært at det er den øverste lederen i den juridiske virksomheten som utøver behandlingsansvaret. Etter vår mening er det her grunn til å følge systemet i tvisteloven og domstolsloven[45] vedrørende "stedfortreder for upersonlige rettssubjekter", som også åpner for delegasjon av denne funksjonen, se tvl § 2-5, jf. dl § 191.

### 2.5.4 Vertikalt delt behandlingsansvar

Loven utelukker ikke delt behandlingsansvar, men det er uttalt i merknader til bestemmelsen at en bør tilstrebe at behandlingsansvaret er i ett og samme organ. Dette fremstår imidlertid

[44] Lov om mekling og rettergang i sivile saker 17. juni 2005 nr. 90 (heretter også "tvl").

[45] Lov om domstolene 13. august 1915 nr. 5 (heretter også "dl").

ikke som annet enn en tilråding, og er neppe til hinder for delt behandlingsansvar også i situasjoner der ansvaret kunne vært plassert på mer enn én juridisk eller fysisk person.

I forarbeidene til loven er det bare hierarkisk delte behandlingsansvar som er kommentert. Dette er situasjoner der ansvaret er delt mellom over- og underordnet del av en organisasjonsstruktur. Forholdet mellom et departement og et direktorat er et eksempel innen offentlig sektor, mens forholdet mellom moder- og datterselskap er et eksempel fra privat sektor. I forarbeidene skriver departementet om dette:

> Det vil kunne være slik at et overordnet organ, f eks et departement, fastsetter de overordnete formålene for personopplysningsbehandlingen, mens underordnete organer, f eks direktorater, vil detaljere formålene med behandlingen og velge praktiske hjelpemidler. I slike tilfeller vil begge organene kunne være «behandlingsansvarlig» etter loven her, og ha en selvstendig plikt til å oppfylle lovens krav. Man bør imidlertid tilstrebe og plassere behandlingsansvaret i ett og samme organ. I denne sammenheng vil det gjerne være naturlig å plassere behandlingsansvaret der man har den daglige og mest omfattende befatningen med personopplysningene.[46]

En slik vertikal deling av behandlingsansvaret som departementet skisserer, er etter vår mening uheldig og unødvendig. Dersom det foreligger et overordningsforhold som innebærer kompetanse til å fastsette formål og hjelpemidler vedrørende den behandling av personopplysninger som underordnede organer foretar, bør den behandlingsansvarlige alltid være denne overordnede organisasjonen. Et annet forhold er at ansvaret kan *delegeres* til vedkommende underordnet organisasjon, og der spesielt tilordnes en person eller en stilling. Slik bør for eksempel Arbeids- og inkluderingsdepartementet være behandlingsansvarlig for den behandling som skjer i trygdetaten (Rikstrygdeverket, fylkestrygdekontorene og trygdekontorene mv.). Imidlertid bør behandlingsansvaret delegeres til det nivået som har de beste forutsetninger for en effektiv utøvelse av ansvar (f.eks. til direktoratsnivået). Poenget er at delegasjon ikke fritar den delegerendes ansvar; den delegerende vil ha plikt til reellt å følge opp behandlingsansvaret og eventuelt instruere de aktuelle underordnede organisasjonene.

En slik løsning der behandlingsansvaret alltid legges til toppen av organisasjonshierarkier, har i og for seg ligget som et potensiale i den eksisterende lovteksten. Loven har imidlertid lite tydelige organisasjonsmessige bestemmelser, der ”behandlingsansvarlig” og ”databehandler” er de eneste aktørene som har kommet tydelig frem fordi de er definerte i § 2. Som vi kommer tilbake til, opererer imidlertid loven med flere organisatoriske roller knyttet til behandlingen av personopplysninger. I tillegg kan behandlingsansvaret delegeres. Dette gjør det mulig å legge mindre vekt på å plassere behandlingsansvaret nær ”der man har den daglige og mest omfattende befatningen med personopplysningene”, slik departementet uttrykte seg i forarbeidene til loven.

Den overordnede kompetansen til å bestemme vedrørende formål og hjelpemidler som loven forutsetter at behandlingsansvarlig skal ha, ofte ikke kan kombineres med en nærhet til der behandlingen skjer. Når flere roller trekkes inn, kan behandlingsansvarliges overordnede funksjon tydeliggjøres, samtidig som det daglige ansvaret knyttes til særskilte roller, lenger ned i hierarkiet i den behandlingsansvarliges organisasjon eller til en underordnet organisasjon.

Dersom det ikke foreligger et overordningsforhold som gjør delegasjon og instruksjon vedrørende behandlingsansvaret mulig, kan heller ikke behandlingsansvaret plasseres i den

[46] Ot.prp. nr. 92 (1998–99) s. 103.

overordnede organisatoriske enheten. Datatilsynet er for eksempel et uavhengig forvaltningsorgan administrativt underordnet Kongen og Fornyings- og administrasjonsdepartementet. Her kan (og skal) ansvaret for behandling av personopplysninger i tilknytning til administrasjon plasseres hos departementet. På andre områder eksisterer det imidlertid intet overordningsforhold, og ingen instruksjonsmyndighet. Derfor er det Datatilsynet selv som må være behandlingsansvaret for all behandling av personopplysninger som skjer for tilsynsformål, dvs. i tilknytning til myndighetsutøvelsen etter loven.

### 2.5.5 Horisontalt delt behandlingsansvar

Etter vår mening er det kun i tilfeller der flere aktører som ikke står i under- eller overordningsforhold til hverandre samarbeider at det bør være aktuelt med delt behandlingsansvar. Dette er praktisk på mange områder, og særlig i tilknytning til internett-baserte tjenester, samt i tilknytning til nye samarbeidsformer mellom offentlige forvaltningsorganer. Slike samarbeidsforhold kan ha mange partnere og inngå i kompliserte strukturer, og det er store muligheter for å utvikle stadig nye former for samarbeid som det i lovgivningen neppe er mulig å være ajour med. Loven må derfor legge opp til å håndtere delt behandlingsansvar på robuste måter, dvs. uavhengig av nærmere valg av detaljert samarbeidsmodell.

Delt behandlingsansvar må klart holdes adskilt fra situasjoner der flere behandlingsansvarlige bruker samme databehandler, dvs. der én og samme oppdragstaker behandler personopplysninger på vegne av flere behandlingsansvarlige (som oppdragsgivere). I sist nevnte forhold er det flere selvstendige bestillinger overfor databehandler, og selv om de behandlingsansvarlige kan ha koordinert bestillingene seg imellom, er det avgjørende at hver av dem har en uavhengig bestemmelsesrett vedrørende formål, hjelpemidler mv., som ikke på bindende måter er begrenset av samarbeidet. *Egentlig delt* behandlingsansvar oppstår når flere aktører som i utgangspunktet har selvstendig behandlingsansvar, inngår i et forpliktende forhold som innebærer at den bestemmelsesretten som er tillagt hver av de behandlingsansvarlige utøves felles, dvs. at de gjennom felles beslutninger vedrørende formål, hjelpemidler mv. disponerer på en måte som er rettslig bindende for samarbeidspartnerne.

Når aktører går inn i et slikt forpliktende samarbeid, samtidig som de opprettholder egen organisasjon, innebærer det at det felles behandlingsansvaret er *avgrenset*. Det vil derfor lett skje at visse typer behandling av personopplysninger er omfattet av delt behandlingsansvar, mens det for andre deler gjelder et eneansvar for behandlingen. Ved delt behandlingsansvar vil det derfor alltid være viktig å klargjøre hvorledes ansvaret er delt.

Når behandlingsansvaret er delt, innebærer det utøvelse av felles bestemmelser over formål og hjelpemidler mv. Som understreket i avsnitt 2.5.2 er det imidlertid også en rekke andre forhold som den behandlingsansvarlige har ansvar og bestemmelsesrett overfor. Dette gjelder for eksempel kravene til opplysningskvalitet, gjennomføring av individuelle rettigheter, internkontroll og informasjonssikkerhet. Et reellt felles behandlingsansvar innebærer derfor felles bestemmelse vedrørende en lang rekke forhold, og det er neppe mulig å avgrense de felles bestemmelsene til spørsmål om formål og hjelpemidler. Dersom flere aktører går sammen om et felles informasjonssystem som skal behandle personopplysninger, må de felles bestemmelsene dekke alle forhold som loven aktualiserer i forhold til den delen av systemløsningen som er gjort felles. I et samarbeid med felles mottak av personinformasjon via et internett-basert rutine, må det felles behandlingsansvaret med andre ord dekke alle

aspekter ved denne felles rutinen. I tillegg vil hver av samarbeidspartnerne ha særskilt behandlingsansvar for den videre behandlingen av personopplysninger som skjer utenfor det aktuelle samarbeidet.

Det forhold at delt behandlingsansvar nødvendigvis må dekke en rekke spørsmål som er regulert i loven, der det kan oppstå uenighet og tvil mellom de samarbeidende aktørene, gjør det nødvendig å etablere en "beslutningsmekanisme". Kompetanse til å fastsettelse formål, krav til opplysningskvalitet og sikring av personopplysninger mv., bør med andre ord klart legges til en beslutningsmekanisme som inngår i samarbeidsforholdet. Utøvelse av behandlingsansvaret gjør det altså nødvendig at det blir tydelig hvorledes den felles bestemmelsesretten faktisk blir utøvet. Sammen med behovet for tydelig å angi samarbeidspartnerne og gjenstanden for samarbeidet, peker dette i retning av minimumskrav til *institusjonalisering* av slikt samarbeid. I vårt radikale lovforslag § 7 har vi på denne bakgrunn tatt inn et krav om avtaleregulering av hvorledes behandlingsansvaret er fordelt,[47] jf. lignende bestemmelse i pol § 15.

### 2.5.6 Tildeling av behandlingsansvar i lov mv.

Direktivets definisjon gir klart uttrykk for at det i lov eller i medhold av lov kan fastsettes hvem som er behandlingsansvarlig. Dette er også i samsvar med norsk praksis. I valutaregisterforskriften er for eksempel behandlingsansvaret lagt til Toll- og avgiftsdirektoratet,[48] og etter helseregisterloven er databehandlingsansvaret for flere sentrale helseregistre lagt til Nasjonalt folkehelseinstitutt.[49] Sosial- og helsedirektoratet er i forskrift gjort behandlingsansvarlig for alkoholtilvirkingsregisteret,[50] samt for register over salgs- og skjenkebevillinger.[51] I tillegg er Utlendingsdirektoratet (UDI) gjort behandlingsansvarlig for nasjonalt personregister for introduksjonsordning og opplæring i norsk og samfunnskunnskap for nyankomne innvandrere (Nasjonalt introduksjonsregister).[52] Disse tilfeller ga *medio* desember 2005 en fullstendig oversikt over tilfeller av behandlingsansvar som er tildelt i lov eller forskrift.

Tildeling av behandlingsansvar i lov og forskrift er spesielt aktuelt for offentlig sektor, noe praksis til nå klart viser, jf. ovenfor. I prinsippet kan en imidlertid tenke seg at behandlingsansvar i privat virksomhet også kan bli gjenstand for konkret lovregulering, for eksempel dersom viktige forbrukerinteresser skulle tilsi dette. Uten at det er klare holdepunkter for noe annet, eliminerer imidlertid ikke slik tildeling av ansvar – uansett sektor – de overordningsforhold som eksisterer. Dersom behandlingsansvaret for eksempel legges til Utlendingsdirektoratet, og Arbeids- og inkluderingsdepartementet har instruksjons-myndighet på området, kan en slik tilordning av ansvar direkte til et direktorat ikke frita departementet for behandlingsansvar på sitt myndighetsområde. Fastsettelse i eller i medhold av lov av hvem som skal ha behandlingsansvar, bør etter vår mening derfor primært skje i tilfelle der det ikke er en overordnet offentlig myndighet på det aktuelle saksområdet, eller dersom tildelingen av ansvar gjelder privat virksomhet. Innen offentlig sektor bør tildeling av behandlingsansvar i lov eller forskrift derfor primært skje i forhold til uavhengige organer

47 Jf. også Olsen og Mahler 2005, avsnitt 4.2.7.

48 Se forskrift 6. desember 2004 nr.1573 § 1

49 Se f.eks. forskrift 17. oktober 2003 nr. 1246 § 1-5.

50 Se forskrift 8. juni 2005 nr. 539 § 7-2.

51 Se forskrift 20. april 2005 nr. 342 kapittel 3.

52 Se forskrift 20. april 2005 nr. 342 § 8 annet ledd.

(typisk tilsyn og ombudsmenn), samt overfor andre enheter der overordningsforholdet er svakt eller uavklart.[53]

### 2.5.7 Ulike roller som er tillagt den behandlingsansvarlige

Det er vanskelig å forstå personopplysningsloven uten å skjelne mellom aktører og roller. Behandlingsansvarlige og de registrerte personer[54] er betegnelsen på to aktører som alltid eksisterer når det skjer behandling av personopplysninger.[55] Loven inneholder også bestemmelser om andre aktører, og disse kommer vi tilbake til i neste avsnitt. Poenget her er at det til aktøren "behandlingsansvarlig" er knyttet flere *roller*. Behandlingsansvarlige skal med andre ord fylle flere roller som dels går tydelig frem av loven, og som dels fremgår mer implisitt. Behandlingsansvarlig kan være alt fra én fysisk person til store juridiske personer. Dette innebærer at når den behandlingsansvarlige er én fysisk person, vil denne personen måtte fylle alle roller, mens i en stor organisasjon kan rollene fordeles på mange personer/stillinger. Som roller regner vi bare det som kan innehas av én og samme person, dvs. når den behandlingsansvarlige er en fysisk person. Her skal vi kort gjennomgå de aktuelle rollene. Gjennomgangen er både basert på loven og på forskriftene til loven. Vi trekker inn forskriftene fordi det ikke er mulig å gi noe helhetlig bilde av kravene til organisering av den behandlingsansvarliges virksomhet, uten å beskrive alle roller. Rollene i forskriften er ikke mindre betydningsfulle enn rollene som er beskrevet i loven.

Ut over den generelle rollen som behandlingsansvarlig, er det to roller knyttet til den behandlingsansvarlige som eksplisitt er beskrevet i lov og forskrift. Dette gjelder for det første den daglige ansvarlige, jf. "hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter" (§ 32 første ledd bokstav c). Denne rollen fremgår bare av § 32 som beskriver innholdet av meldinger som skal sendes Datatilsynet før behandling av personopplysninger starter. Daglig ansvar er her knyttet til hver meldepliktig behandling, og det er på det rene at det kan være forskjellige daglig ansvarlige for forskjellige behandlinger som meldes. Loven må muligens forstås slik at det for hver behandling kun skal være én daglig ansvarlig person, men så lenge antallet personer ikke gir pulverisering av ansvar, er det neppe grunn til å nekte flere enn én daglig ansvarlig. Etter ordlyden skal det daglige ansvaret være knyttet til bestemt(e) person(er), jf. "*hvem* som har …" (vår kursiv). I sin melderutine, er denne rollen imidlertid knyttet til en bestemt *stillingsangivelse* i organisasjonen.[56]

Også forskriften angir roller som den behandlingsansvarlige skal fylle. Dette gjelder for det første "[d]en som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver", dvs. daglig leder (se pof § 2-3 første ledd). Etter forskriften har daglig leder ansvar for at kapittelet om informasjonssikkerhet følges. Bestemmelsene om informasjonssikkerhet er gitt innenfor rammene av pol § 13, med hjemmel i bestemmelsens siste ledd.[57] Daglig leder betegner den øverste operative leder for en virksomhet, typisk en administrerende direktør,

---

53 Vi antar at dette f.eks. kan være tilfelle innen visse saksområder i forholdet mellom Jernbaneverket og Samferdselsdepartementet, og Statistisk sentralbyrå og Finansdepartementet mv. Flere offentlige virksomheter som primært har tjenesteytende funksjoner og/eller befinner seg i gråsonen mellom offentlig og privat virksomhet, kan ha behov for lovregulert plassering av behandlingsansvar.

54 "Registrert", jf. pol § 2 nr. 6.

55 De registrerte er normalt flere personer, mens behandlingsansvarlig er ofte én fysisk eller juridisk person.

56 Se meldeskjema punkt 3.

57 Etter ordlyden er det ingen krav om at daglig leder skal ha ansvar for at sikkerhetsbestemmelsene i pol § 13 blir fulgt fordi ansvaret etter pof § 2-3 bare gjelder informasjonssikkerhetsbestemmelsene i forskriftens kapittel 2. Forskriftsbestemmelsene om informasjonssikkerhet gjelder ikke for manuell behandling av personregistre, se pof § 2-1 første ledd. Samlet sett innebærer dette at daglig leder ikke har eksplisitt ansvar for informasjonssikkerhet knyttet til manuelle personregistre (!).

generalsekretær eller lignende. Dersom det er en person som er behandlingsansvarlig alene, er det denne personen som må anses som daglig leder. Daglig leder er ikke nødvendigvis den samme som rollen som øverste leder for den behandlingsansvarlige når dette er en juridisk person. Ledes virksomheten av et styre, er det for eksempel virksomheten v/ styrets leder som representerer den behandlingsansvarlige, mens daglig leder er administrerende direktør eller lignende.

For internkontroll (pol § 14 og kapittel 3 i forskriften), er det ikke gitt bestemmelser med tilordning av ansvar til en bestemt stilling. Dette er til tross for at internkontrollen er mer vidtrekkende og minst like viktig for ivaretakelsen av personvernet som arbeidet med informasjonssikkerhet.

Forskriften inneholder også angivelse av flere gjennomgripende aktiviteter som peker i retning av roller med ansvar for å utføre aktiviteten. Dette gjelder særlig krav om sikkerhetsrevisjon i pof § 2-5. Forskriften innebærer trolig bare krav om intern sikkerhetsrevisjon, dvs. slik at den personen som leder et slikt arbeid (sikkerhetsrevisor) er del av den behandlingsansvarliges organisasjon. Kravet i pof § 2-7 om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet, peker i retning av at slik sikkerhetsrevisor skal identifiseres. Her tar vi ikke stilling til spørsmålet. Poenget her er at enkelte handlinger/aktiviteter med sentral betydning for personvernet, kan tenkes å bli tydeligere knyttet opp til roller hos den behandlingsansvarlige, for på den måten å klargjøre organiseringen av arbeidet med personvern i virksomheten.

På det aller laveste nivået, krever personopplysningsforskriften en tydelig organisering av all virksomhet som gjelder behandling av personopplysninger. Blant annet innebærer pof § 2-8 at alle medarbeidere hos den behandlingsansvarlige skal være autorisert til all bruk av personopplysninger som de blir pålagt. Bruken skal dessuten begrenses til slike pålegg.

I større organisasjoner er det åpenbart nødvendig å foreta en nærmere organisering av arbeidet som kan bidra til at personopplysningsloven og forskriften blir etterlevet. Behovet oppstår dessuten i tilknytning til løst samarbeid mellom flere behandlingsansvarlige, der det kan oppstå uklarhet om ansvars- og funksjonsfordelingen. Etter vår mening, er det særlig to spørsmål det her er ønskelig å ta stilling til. For det første er spørsmålet om de roller loven og forskriften i dag opererer med bør beholdes, og om en eventuelt har behov for å etablere nye og/eller tydeligere roller enn i dag. Det andre spørsmålet er hvorledes krav til roller hos den behandlingsansvarlige skal reguleres, dvs. om det skal gis spredte bestemmelser i lov og forskrift, eller om det skal gis en bestemmelse som gir samlet oversikt over slike organisatoriske krav. Vår oppfatning er at det generelt er stort behov for å klargjøre de aktuelle rollene, og tydeliggjøre hvilke relasjoner det er mellom disse. Det er imidlertid behov for å regulere disse forholdene sammen med andre organisatoriske spørsmål, se neste avsnitt.

### 2.5.8 Aktører som den behandlingsansvarlige skal/kan samarbeide med

Behandling av personopplysninger gjelder primært forholdet mellom behandlingsansvarlige og registrerte personer. Dette er således hovedaktørene. I tillegg kan andre aktører komme inn; dels på bestemte vilkår som loven stiller, og dels som et resultat av at den behandlingsansvarlige velger det. Flere av disse aktørene har en uklar profil i loven.

#### 2.5.8.1 Behandlingsansvarliges representant

Personopplysningsloven § 4 siste ledd fastsetter at en behandlingsansvarlig som er etablert utenfor EØS-området og benytter hjelpemidler i Norge, skal ha *en representant* som er etablert i Norge.[58] I loven heter det at "[b]estemmelsene som gjelder for den behandlingsansvarlige gjelder også for representanten". I forarbeidene til loven fremgår det at representanten skal handle i behandlingsansvarliges sted, dvs. sikre at alle plikter mv. som behandlingsansvarlige har, blir etterlevet. Den behandlingsansvarlige er likevel ansvarlig, og myndigheter og registrerte personer kan både forholde seg til den behandlingsansvarlige og dennes representant i Norge. Opplysning om hvem som er representant for den behandlingsansvarlige, skal inngå som del av meldingen til Datatilsynet (se § 32 første ledd bokstav a). I loven sies det ingen ting om representantens rolle i tilknytning til søknad om konsesjon, men i Datatilsynets konsesjonsskjema er det tatt med tilsvarende opplysninger om representanten som i meldeskjemaet.[59]

Behandlingsansvarliges representant er bare nevnt i § 4 siste ledd, og i § 18 (innsyn), § 19 (informasjon ved innsamling av personopplysninger) og § 32 (innhold av meldinger til Datatilsynet). I de tre sistnevnte bestemmelsene er representanten kun nevnt i oppregninger av informasjon som skal gis. For øvrig er representanten ikke nevnt, og det fremgår for eksempel bare som en tolking av § 4 tredje ledd at registerte personer kan gjøre henvendelser om innsyn mv. til behandlingsansvarliges representant. I forskriftene er representanten over hode ikke omhandlet.

Etter vår mening er det grunn til å tydeliggjøre hvilken rolle den behandlingsansvarliges representant har, jf. vårt radikale lovforslag §§ 7 og 7a. Dette gjelder særlig i forhold til registrerte personer.

#### 2.5.8.2 Databehandler

"Databehandler" er definert i loven som "den som behandler personopplysninger på vegne av den behandlingsansvarlige", se § 2 nr. 5. Tilsvarende definisjon i personverndirektivet understreker tydeligere hvem som kan være databehandler eller "processor": "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". Den norske definisjonen må leses i samsvar med direktivet. I konsesjonsskjemaet ser det imidlertid ut som det er gjort en forutsetning om at databehandler er et firma. Således spørres det om "Fullstendig navn/firma på databehandleren" samt organisasjonsnummer (derimot ikke personnummer).[60]

Databehandler blir først aktuell dersom det oppstår et oppdragsforhold, dvs. dersom behandlingsansvarlig inntar rollen som oppdragsgiver overfor en oppdragstaker og oppdraget går ut på å behandle personopplysninger på oppdragstakers vegne. Bestemmelsen kan lett bli misforstått ved at "databehandler" oppfattes som betegnelse på den/de personer som faktisk behandler personopplysninger, jf. rollen som "medarbeidere" som kort er omtalt i forrige avsnitt. Årsaken er trolig at "databehandler" er et begrep som ligger nær dagligspråk og gir umiddelbare (gale) assosiasjoner om betydningen. Ut over definisjonen (i § 2 nr. 5) er databehandler kun omhandlet på måter som ikke er egnet til å avkrefte mulige

[58] Se tilsvarende bestemmelse i personverndirektivet artikkel 4 nr. 2. Forutsetningen for plikten til å ha representant er at hjelpemidlene i Norge blir benyttet til noe mer enn å overføre personopplysninger via Norge. Se videre kapittel 4.

[59] Se konsesjonsskjemaet punkt B.

[60] Se konsesjonsskjemaet punkt D.

misoppfatninger av hvem databehandler er. Dette gjelder § 13 (informasjonssikkerhet), § 14 (internkontroll) og § 15 (databehandlers rådighet over personopplysninger).

I motsetning til hva tilfellet er for behandlingsansvarliges representant, er databehandler gitt en rolle vedrørende registrertes rettigheter, jf. lovens kapittel III om informasjon om behandling av personopplysninger. Således sies det i § 24 at den registrerte kan henvende seg til databehandler for å få slik informasjon. I tillegg er databehandler nevnt i § 32 første ledd bokstav a, blant opplysningene som skal gis i melding til Datatilsynet. Databehandler er imidlertid ikke nevnt i §§ 18 og 19 på tilsvarende måte som behandlingsansvarliges representant. Detter virker umotivert og inkonsistent. I forskriften er databehandler over hode ikke nevnt.

Etter vår mening er det behov for å tydeliggjøre definisjonen av "databehandler" for å unngå misforståelser, jf. vårt radikale lovforslag § 7b. I tillegg er det grunn til å synliggjøre databehandler i flere andre bestemmelser, særlig bestemmelser vedrørende registrertes rett til informasjon.

#### 2.5.8.3 Personvernombud

*Personvernombud* er en aktør som er introdusert i pof § 7-12, dvs. i det kapittelet av forskriften som gjelder unntak fra meldeplikt (kapittel 7, II). Oppnevning av ombudet er her satt inn som et mulig alternativ til meldeplikt:

> Datatilsynet kan samtykke i at det gjøres unntak fra meldeplikt etter personopplysningsloven § 31 første ledd, dersom den behandlingsansvarlige utpeker et uavhengig personvernombud som har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet skal også føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32.

Personvernombud nevnes dessuten i pof § 7-27 som angår forskningsprosjekter. Her står det at nærmere angitte forskningsprosjekter kan unntas fra konsesjonsplikt dersom de er tilrådd av et personvernombud:

> Behandling av personopplysninger i forbindelse med et forskningsprosjekt er unntatt fra konsesjonsplikt etter personopplysningslovens § 33 første ledd dersom prosjektet er tilrådd av personvernombud. Omfatter prosjektet medisinsk og helsefaglig forskning, skal det i tillegg være tilrådd av en regional forskningsetisk komité.
>
> Forskningsprosjekter av stort omfang og lang varighet, samt forskning på store datasett som ikke er pseudonymisert eller avidentifisert på annen sikker måte, er ikke unntatt. Unntaket omfatter bare frafallsanalyser (analyser av fordelinger over utdanning, inntekt og ytelser m.m. blant fremmøtte og ikke-fremmøtte for å beregne betydningen av frafallet) i den grad de er basert på samtykke.

Forskriften stiller som krav at personvernombudet skal være "uavhengig" (jf. § 7-12), et krav som også må antas å gjelde for ombudets rolle i henhold til § 7-27, men det går ikke frem av selve forskriften hva som ligger i dette kriteriet, og det gis heller ingen nærmere beskrivelse av ombudets arbeidsområde og funksjon. I kgl. res. 15. desember 2000 nr. 1265 (om personopplysningsforskriften) er det imidlertid gitt kommentarer til den enkelte forskriftsbestemmelse, herunder § 7-12. Det er her sagt at ombudet skal være en fysisk person, og skal ha ansvar på et "bestemt og begrenset område". Det heter videre at ombudet skal "føre fortegnelser over behandlinger og behandlingsansvarlige, kontrollere den

behandlingsansvarliges behandlinger og bistå de registrerte med å ivareta sine rettigheter etter personopplysningsloven og forskrifter …". Det er vanskelig å ha noen sikker formening om hva som ligger i "bestemt og begrenset område", når dette står sammen med "føre fortegnelser over … behandlingsansvarlige" (som jo forutsetter at det kan være mange behandlingsansvarlige for hvert ombud). Dette åpner for fagspesifikke eller bransjespesifikke ombud, dvs. ombud som er felles for flere behandlingsansvarlige.

Som det fremgår av bestemmelsen, er det ingen automatikk i at oppnevning av personvernombud skal gi lettelse i meldeplikten. I desember 2005 var det i følge Datatilsynets hjemmeside i alt 17 personvernombud. Av disse var 15 "interne", dvs. ombudet var ansatt hos den behandlingsansvarlige. I to tilfeller var det en "ekstern" ombudsordning. Størst aktør her er Norsk Samfunnsvitenskapelige Datatjeneste A/S (NSD) som var personvernombud for mer enn 100 forskningsinstitusjoner. Et annet "eksternt" ombud er It-Con A/S, et selskap innen telebransjen som selger spill og tilbehør til mobiltelefoner.[61] Hos begge eksterne ombud, er selve ombudsrollen knyttet opp til en bestemt person. Det samlede antallet virksomheter som er knyttet til en ombudsordning, var i underkant av 130. De langt fleste av disse var forskningsinstitusjoner knyttet til NSD. Andre virksomhetsområder av betydning er helse og et mindre antall kommuner. Bortsett fra Statistisk sentralbyrå, sykehus og universiteter, var det ingen store virksomheter som hadde personvernombud, verken i offentlig eller privat sektor.

Ordningen med personvernombud er etter vår mening uklar. Slik den i dag praktiseres, kan slike ombud både være eksterne i forhold til behandlingsansvarlige (NSD og It-Con A/S) og knyttet til én enkelt behandlingsansvarlig (de øvrige). De to typetilfellene fremstår som vidt forskjellige. For eksterne personvernombud fremstår ombudet som en ytre privat "kontrollinstans", noe som gjør rollen som uavhengig aktør langt lettere å ha tiltro til enn dersom personvernombudet er ansatt hos den behandlingsansvarlige. Likevel vil slike ombud motta vederlag for ombudsrollen. Dersom denne inntekten utgjør en stor del av ombudsmannens inntekter eller uansett utgjør et stort beløp eller er del av forretningsprofilen, kan de økonomiske interessene true uavhengigheten. Det er også vanskelig å forestille seg hvorledes et ombud som har så mange "kunder" som NSD i Bergen kan "kontrollere den behandlingsansvarliges behandlinger og bistå de registrerte med å ivareta sine rettigheter". Kontrollen må nødvendigvis primært være basert på skriftlig materiale, og for at registrerte personer skal ha særlig hjelp fra ombudet med å realisere sine rettigheter, må det være opplysning om ombudets funksjon i informasjon som gis av den enkelte behandlingsansvarlig.

Registrerte personer må også kunne ha full tillit til ombudets faglige dyktighet vedrørende personvernspørsmål. Et firma som It-Con A/S, som ikke har noen informasjon om ombudsrollen på sine hjemmesider, kan selvfølgelig inneha betydelig kompetanse innen personopplysningsrett. Det er imidlertid et spørsmål hvor sannsynlig det er at innbyggerne i de kommuner dette firmaet er personvernombud for stoler på at firmaets kompetanse er tilstrekkelig, slik at firmaet og ikke Datatilsynet blir kontaktet. Vi har ikke gjort noen systematisk undersøkelse av hvilken informasjon som blir gitt fra behandlingsansvarlige, men i flere kommuner som hadde It-Con A/S som personvernombud, forekom ikke ordet "personvern" på kommunens hjemmeside, og ingen informasjon var gitt om ombudsordningen. I en kommune, var det informasjon om ombudsordningen i et nyhetsoppslag, og firmaet ble nevnt, men uten at det var gitt kontaktinformasjon av noe slag.

---

[61] Se selskapets hjemmeside, der det kun reklameres for spilleprodukter mv., men ikke står noe om selskapet: <http://www.It-Con.no/>.

Slik personvernombudene kan være innrettet, er de dels en del av behandlingsansvarliges organisasjon, og fyller således en rolle i denne organisasjonen på linje med andre roller som loven foreskriver (daglig ansvarlig, daglig leder, sikkerhetsrevisor). De andre rollene er imidlertid ikke uavhengige, men forutsetter under- og overordningsforhold. Personvernombudet blir dermed en "frispiller" i spørsmål vedrørende arbeidsgiverens behandling av personopplysninger, og har alle aspekter ved personopplysningsloven og forskriften som arbeidsområde. Ordningen er imidlertid ikke bundet opp til at ombudspersonen faktisk skal ha tid/arbeidsforhold som tillater effektiv kontroll og assistanse.

Etter vår mening er forskriftens ordning med personvernombud uklart beskrevet, meget mangelfullt integrert i loven og uensartet praktisert. I avsnitt 10.4 foreslår vi en endret ombudsmodell. Uansett hvilken modell en velger, er det imidlertid viktig å etablere ombudsmannen på en måte som klart definerer forholdet til andre aktører og roller etter loven, og med klart definerte arbeidsområder, fullmakter mv.

### 2.5.9 Behandlingsansvarliges straffeansvar

Personopplysningslovens straffebestemmelse lyder:

> **§ 48.** ***Straff***
>
> Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller grovt uaktsomt
>
> a) unnlater å sende melding etter § 31,
> b) behandler personopplysninger uten nødvendig konsesjon etter § 33,
> c) overtrer vilkår fastsatt etter § 35 eller § 46,
> d) unnlater å etterkomme pålegg fra Datatilsynet etter § 12, § 27, § 28 eller § 46,
> e) behandler personopplysninger i strid med § 13, § 15, § 26 eller § 39, eller
> f) unnlater å gi opplysninger etter § 19, § 20, § 21, § 40 eller § 44.
>
> [...]

Bestemmelsen er skrevet etter mønster fra personregisterloven § 32, og innebærer kun straffesanksjonering av et utvalg bestemmelser som lovgiver har ment var tilstrekkelig klare, jf. legalitetsprinsippet.[62] Det fremgår at "den som" kan straffes er personer, og at foretaksstraff skal kunne ilegges i tillegg, i samsvar med straffeloven §§ 48a og 48b. "Behandlingsansvarlig" og "databehandler" er aktører med forholdsvis klare plikter etter loven, og er "den" som mange av bestemmelsene retter seg mot. Analysen ovenfor viser imidlertid at behandlingsansvarlig og databehandler i svært mange tilfelle er juridiske personer, men at det kan være uklart hvilken person som skal representere disse aktørene.

I merknadene til bestemmelsen uttaler departementet at "[s]traffebudet omfatter både ansatte hos den behandlingsansvarlige og andre hjelpere som denne benytter (f.eks. databehandlere)".[63] Dette kan forstås slik at enhver ansatt som har fått oppgaver i henhold til arbeidsgivers (behandlingsansvarliges) arbeidsordning, kan straffes for brudd på de utvalgte bestemmelsene. Behandlingsansvarlig har for eksempel gitt en ansatt i oppgave å være

---

62 I departementets merknad til bestemmelsen nevnes ikke dette hensynet, men det vises til forslaget til straffebestemmelse i NOU 1997:19, der argumentet er fremført, jf. Ot.prp. nr. 92 (1998–1999) s. 134.

63 Ot.prp. nr. 92 (1998–1999) s. 135.

”daglig ansvarlig” for en behandling som er konsesjonspliktig, men der vedkommende person unnlater å søke konsesjon. Spørsmålet er om slike enkeltpersoner skal være hjemfallen til straff, eller om straffeansvaret skal ligge på den person som er den øverste lederen for den behandlingsansvarlige virksomheten. Det kan etter vår mening oppfattes som for tilfeldig og urettferdig om den øverste ledelsen kan fordele straffeansvaret gjennom sin arbeidsorganisering. Det er derfor nærliggende å rette straffesanksjonen mot den person som er den behandlingsansvarliges og (eventuelt) databehandlerens øverste leder.

Personopplysningsloven § 4 siste ledd krever at behandlingsansvarlige som er etablert utenfor EØS-området skal ha en representant i Norge. Bestemmelsens siste setning lyder: ”Bestemmelsene som gjelder for den behandlingsansvarlige gjelder også for representanten”. Spørsmålet er så om dette også gjelder straffeansvaret i følge § 48. Vi finner ikke noe direkte om dette i forarbeidene, men et bekreftende svar ligger trolig implisitt i uttalelsen om at straffebudet omfatter både behandlingsansvarlige og ”andre hjelpere”.[64] Situasjonen kan i så fall tenkes å bli at både behandlingsansvarlige og dennes representant kan straffes. Straff for representanten har imidlertid en så indirekte og lite klar hjemmel at straff etter vår mening ikke bør gjøres gjeldende.

Etter vår mening tilsier legalitetsprinsippet at det klargjøres utenfor enhver rimelig tvil hvilke personer som kan straffes etter denne bestemmelsen. Det bør dessuten fremgå klart at det her er tale om et personlig straffeansvar, og at virksomhetsstraff kan komme til anvendelse i tillegg til det personlige straffeansvaret. Vurdering av § 48 om straff inngår ikke i mandatet, og vi avholder oss derfor fra å fremme konkrete forslag til endret lovtekst.

Forskriftens § 9-3 om straff dekker alle bestemmelsene i kapitlene 2 til 7 og dessuten utvalgte bestemmelser i kapittel 8. Også her er gjerningspersonen angitt ved hjelp av formuleringen ”den som”. I kapitlene 3 (internkontroll), 4 (kredittopplysningsvirksomhet), 7 (melde- og konsesjonsplikt) og 8 (fjernsynsovervåkning) blir situasjonen tilsvarende som etter lovens straffebestemmelse. I andre kapitler i forskriften er det andre aktører som er aktuelle. I kapittel 2 om informasjonssikkerhet er daglig leder gjort ansvarlig for at bestemmelsene i dette kapittelet følges, se § 2-3 første ledd. Lovens straffebestemmelse rammer behandlingsansvarliges og databehandlers brudd på § 13 om informasjonssikkerhet. For behandlingsansvarliges virksomhet innebærer dette trolig at både behandlingsansvarliges øverste ledelse og daglig leder av databehandlers virksomhet kan straffes. Forskriftens § 2-3 gjelder derimot ikke for databehandlers virksomhet, og daglig leder for denne virksomheten kan derfor formodentlig ikke straffes i henhold til pof § 9-3. Imidlertid kan behandlingsansvarlig straffes for brudd på loven som databehandler har gjort seg skyldig i, se pol § 13 tredje ledd om behandlingsansvarliges plikt til å føre tilsyn med databehandler.

I kapitlene 5 (Reservasjonsregisteret) stiller forskriften primært krav til Registerenheten ved Brønnøysundregistrene, og i kapittel 6 (overføring av personopplysninger til utlandet), gjelder bestemmelsene Datatilsynets saksbehandling. Forskriftens bestemmelse om straff, gjelder også disse kapitlene.

Det er etter vår mening grunn til å spørre om hensiktsmessigheten ved å beholde et personlig straffeansvar som på lite spesifikke og dermed uklare måter kan synes å dekke en lang rekke personer innenfor vidt ulike roller. Uansett begrunner både hensynet til etterlevelse av loven og krav til tilstrekkelig klare straffebestemmelser at en gjennomgår bestemmelsene i loven og

[64] *Ibid.*

forskriften i sammenheng, for på den måten å ta stilling til om det er tilstrekkelig tydelig hvem den enkelte bestemmelse retter seg mot.

## 2.6 Avsluttende betraktninger vedrørende lovens definisjoner

Personopplysningsloven § 2 inneholder på mange måter nøkkelen til forståelsen av loven. Uten innsikt i denne paragrafen er det for eksempel ikke mulig å ta stilling til om loven gjelder en bestemt informasjonsbehandling eller ikke. Definisjonene gjør bruk av ord fra daglig norsk, som ikke gir indikasjoner på at det kan ligge spesielle meninger bak, og som derfor bare tilsynelatende er lett forståelige. Til sammenligning bruker personverndirektivet – i alle fall i engelsk versjon – språklige uttrykk som ikke på tilsvarende måte kan beskrives som alminnelige.

Definisjonene i den norske loven er gjort lite komplekse, og er vesentlig mer kortfattet formulert enn i personverndirektivet. Dette innebærer at flere viktige vurderingstemaer ikke er gjort synlig i den norske lovteksten, noe som legger til rette for misoppfatninger og fare for å overse vesentlige rettslige spørsmål.

Både den norske loven og direktivet gjør bruk av en lovgivningsteknikk der definisjoner presenteres i en liste, uten at det angis hva definisjonene har betydning for. Selv om dette er en vanlig teknikk, er det etter vår mening lite vellykket at definisjonene ikke settes inn i en sammenheng som indikerer hvilke rettsspørsmål de har betydning for.

For å klargjøre definisjonene, står en etter vårt syn overfor valget mellom en moderat og en radikal endring. En moderat endring kan innebære at en i hovedsak beholder innholdet og strukturen i § 2 slik den nå står, og gjennomfører presiseringer på utvalgte punkter. En mer radikal tilnærming kan være å bryte opp § 2 i flere bestemmelser for å gjennomføre en tydelig gruppering av rettsspørsmål, tydeliggjøre alle vesentlige rettslige vurderinger og sette de sentrale rettsspørsmålene inn i en klarere sammenheng.

# Kapittel 3

## Personopplysningslovens saklige virkeområde

### 3.1 Om mandatet

I rammen gjengir vi mandatets punkt 2 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

> *Lovens saklige virkeområde*
>
> Personopplysningsloven § 3 angir lovens saklige virkeområde. Det er bestemt i annet ledd at loven ikke gjelder for behandling av personopplysninger som foretas for personlige eller private formål. Departementene ber **utrederne vurdere om personopplysningsloven § 3 er i samsvar med EU-direktivet og ny rettspraksis**. Det vises her spesielt til EF-domstolens dom 6. november 2003 (sak C-101-01) i den såkalte Lindqvist-saken om privat bruk av personopplysninger, jf. direktivet artikkel 3 nr. 2 og fortalens 12. betraktning. **Utrederne bør vurdere om det er behov for en justering av § 3 som følge av denne dommen.** Det samme gjelder Personvernnemndas avgjørelse 2005/1 …".

Vi forstår dette mandatpunktet som i hovedsak en diskusjon av konsekvensene av EF-domstolens avgjørelse i *Lindqvist*-saken for anvendelse og utforming av personopplysningsloven § 3 annet ledd. Mandatpunktet nevner dessuten Personvernnemndas avgjørelse i sak 2005 nr. 1. Denne avgjørelsen har vi valgt å behandle i forrige kapittel, jf. avsnitt 2.3, og vi avstår dermed fra å drøfte den her.

### 3.2 Personopplysningsloven § 3 annet ledd

#### 3.2.1 Anvendelse av bestemmelsen før *Lindqvist*-avgjørelsen

Personopplysningsloven § 3 annet ledd lyder:

> Loven gjelder ikke behandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål.

Bestemmelsen er ment som en videreføring av rettstilstanden i henhold til personregisterloven, som (i forhold til privat sektor) kun fikk anvendelse på "privat næringsvirksomhet, foreninger eller stiftelser" (jf. pregl. § 1 tredje ledd).[65] Bestemmelsen tar også sikte på å avgrense personopplysningslovens virkeområde i tråd med EUs personverndirektiv artikkel 3 nr. 2 (gjengitt nedenfor).

Hovedbegrunnelsen for en slik avgrensning er, ifølge forarbeidene, at

> [d]et vil … kunne fremstå som et uønsket inngrep i den enkeltes privatliv om man skulle gi behandlingsregler som åpner for kontroll med slik behandling av personopplysninger som vedkommende foretar som privatperson. Samtidig er det klart at personvernkonsekvensene av

[65] Jf. også NOU 1997: 19 s. 58; Ot.prp. nr. 92 (1998-99) s. 105.

> denne formen for behandling gjennomgående vil være beskjedne, slik at lovregulering er unødvendig og ville virke unødvendig ressurskrevende.[66]

Når det gjelder typer aktiviteter som faller inn under § 3 annet ledd, står det i forarbeidene at unntaket bl.a. omfatter "private hjemmesider på internett med informasjon av privat og personlig karakter".[67] Unntaket gjelder derimot ikke for "økonomisk aktivitet som overstiger det som er vanlig for fritidsaktiviteter". Enkeltpersoners aktivitet "som ledd i engasjement for politiske eller ideelle organisasjoner" er heller ikke omfattet. Dessuten gjør forarbeidene det klart at referansene til "privat" og "personlig" langt på vei dekker det samme, og at de omfatter "familiemessige gjøremål" samt "fritidsaktiviteter".

Før EF-domstolens avgjørelse i *Lindqvist*-saken (jf. nedenfor), var utgangspunktet for anvendelsen av unntaket en vurdering av behandlingens *formål* snarere enn en vurdering av behandlingens kontekst. Hovedkriteriet for anvendelsen av unntaket var derfor hvorvidt en person foretok behandling for (rent) private eller personlige formål, ikke hvorvidt behandlingen foregikk innenfor en (rent) privat eller personlig kontekst, sfære eller sammenheng. Dette fremgår både av bestemmelsens ordlyd og av forarbeidene.

Mindre klart er om det ved anvendelsen av unntaket skal legges til grunn den behandlingsansvarliges egen subjektiv oppfatning av behandlingens formål eller om det skal legges til grunn en mer objektiv (inter-subjektiv) test der en tar utgangspunkt i formålets art og andre omstendigheter ved behandlingen. Forarbeidene trekker i retning av en objektiv test, noe som også er påpekt av Lovavdeling.[68]

Når det gjelder hjemmesider på internett antok Datatilsynet at opplasting av personopplysninger til slike hjemmesider ville falle inn under unntaket dersom formålet med behandlingen kunne anses å være av privat karakter. Opplasting av personopplysninger til en personlig hjemmeside for hobbyformål – eksempelvis som ledd i slektstreforskning – ble ansett som et typisk tilfelle i så henseende. Et mer kontroversielt tilfelle gjaldt et nettsted <glattcella.com>, der privatpersoner i 2002 publiserte navn på kjente personer (artister, idrettsutøvere) som hadde begått forseelse/forbrytelse og satt i varetekt: Datatilsynet mente at virksomheten hadde et rent privat formål og dermed falt utenfor personopplysningslovens virkeområde.[69] Tilsynets vurdering av virksomhetens formål som rent privat var høyst tvilsom. Viktigst var imidlertid at det synes å ha hersket konsensus om at det ikke var avgjørende for anvendelse av unntaket i pol § 3 annet ledd i internett-sammenheng om en større ubestemt krets av personer kunne få adgang til opplysningene. Dette fremgår ikke eksplisitt av unntakets ordlyd, men ble ansett å ligge implisitt til grunn i forarbeidene. Selv om forarbeidene refererer til "private hjemmesider" ble ikke denne referansen ansett å forutsette at hjemmesiden kun er tilgjengelig for et lite og bestemt antall av personer; det var snarere hjemmesidens bruksformål som sto i fokus.

På dette punktet er det verdt å merke seg at forarbeidene til den danske personopplysningsloven også har antatt at opplasting av personopplysninger til en

---

66 Ot.prp. nr. 92 (1998-99) s. 105.

67 Ot.prp. nr. 92 (1998-99) s. 105.

68 Jf. brev av 11. februar 2002 fra Lovavdelingen til Datatilsynet (ref. 01/08493 ES KES/bj) vedrørende fjernsynsovervåking og personopplysningsloven § 3.

69 Jf. Schartum og Bygrave 2004 s. 126.

hjemmeside vil kunne falle inn under unntaket i den danske loven som tilsvarer pol § 3 annet ledd.[70]

### 3.2.2 Direktivet artikkel 3 nr. 2

Angjeldende bestemmelse lyder:

> This Directive shall not apply to the processing of personal data … by a natural person in the course of a purely personal or household activity.

Fortalens punkt 12 utdyper i begrenset grad innholdet i formuleringen ”purely personal or household activity” ved at den nevner ”correspondence and the holding of records of addresses” som eksempler på slike aktiviteter.

Ordlyden av den engelske versjonen av artikkel 3 nr. 2 er lik den svenske versjonen, som refererer til behandling av personopplysninger ”som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll”. Oppbyggingen og formuleringen av disse versjonene av artikkel 3 nr. 2 er noe annerledes til pol § 3 annet ledd. I motsetning til sistnevnte fokuserer de på den type *aktivitet* som danner behandlingens kontekst; formålet eller hensikten med behandlingen er av mindre synlig betydning.

Ordlyden i pol § 3 annet ledd synes å bygge i stor grad på den danske versjonen som refererer til behandling ”som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter”. Her får behandlingens formål en mer synlig plass i bestemmelsen selv om ”personlige” mv. knyttes opp til ”aktiviteter”, ikke ”formål”.

Også de franske og tyske versjonene fokuserer i noe grad på behandlingens formål. Den franske versjonen refererer således til ”traitement ... *pour* l’exercice d’activités exclusivement personnelles ou domestiques” (vår utheving); den tyske versjonen til ”die von einer natürlichen Person *zur* Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten” (vår utheving).

### 3.2.3 *Lindqvist*-dommen

EF-domstolens avgjørelse 6.11.2003 i sak C-101/01, *Bodil Lindqvist*,[71] gjaldt en kvinne som jobbet som frivillig og ubetalt konfirmantleder for et kirkesamfunn i Sverige. I denne rollen hadde hun publisert personopplysninger om enkelte av sine medarbeidere på en hjemmeside. Hjemmesiden var opprettet for at hennes medarbeidere lettere skulle få den informasjonen de behøvde. Hjemmesiden kunne nås via særskilt lenke på den svenske statskirkens nettsted, men den var ellers personlig. Lindqvist hadde ikke informert de aktuelle personene om publiseringen eller innhentet deres samtykke.

Et av spørsmålene domstolen måtte ta stilling til var om Lindqvists behandling av personopplysninger falt innenfor unntaket i artikkel 3 nr. 2. Domstolen slo kortfattet fast at den angjeldende behandlingen falt utenfor unntaket. Ifølge domstolen skal unntaket tolkes

---

[70] Jf. Blume 2000 s.37 og videre henvisninger; Nielsen og Waaben 2001 s. 71 og videre henvisninger.

[71] Jf. European Court Reports 2003 s. I-12971.

> as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[72]

Avgjørelsen synes å fastholde at det ikke er formålet med behandlingen som er avgjørende når en bedømmer om unntaket i artikkel 3 nr. 2 kommer til anvendelse, men snarere hvorvidt aktiviteten som behandlingen er del av, er privat eller lignende. For at unntaket kommer til anvendelse må behandlingskontekst være lukket i betydning at behandlingen foregår innenfor en begrenset og antageligvis liten personkrets.

I mange, hvis ikke de fleste tilfeller vil fokus på behandlingsformål gi samme utfall som fokus på behandlingskontekst, men ikke alltid. Opplasting av personopplysninger til en personlig hjemmeside for hobbyformål er nettopp et tilfelle der det ikke vil være samsvar (forutsatt naturligvis at hjemmesiden er tilgjengelig for alle som er koblet til nettet), og der forarbeidene til personopplysningsloven, samt praksis deretter, hadde fastholdt som behandling utenfor lovens virkeområde. *Lindqvist*-avgjørelsen viser at dersom behandling tilgjengeliggjør personopplysninger til et ubestemt antall personer – som ofte vil være tilfellet med opplasting av opplysninger til internettet – kan ikke behandlingen regnes som del av en privat aktivitet selv om formålet med behandlingen ellers er personlig (f.eks. hobby).

Således synes EF-domstolen å lage et skille mellom "det private" og "det personlige" hvor førstnevnte angår (i det minste) type og grad av lukkethet/(u)tilgjengelighet overfor andre personer, mens sistnevnte angår fokus og formål (og dermed behov, ønsker, interesser mv.) – et skille som ikke fremgår klart av direktivets ordlyd. Samtidig gir ikke avgjørelsen direkte svar på hvordan opplasting og videre behandling av personopplysninger i sammenheng med en personlig hjemmeside kan falle innenfor unntaket etter artikkel 3 nr. 2. Spørsmål som reiser seg i den henseende er:

1. Hva slags mekanismer kan skape "privathet" på nettet?
2. Hvor liten må personkretsen som har adgang til opplysningene være?

Det er likevel rimelig å anta at det ved bruk av eksempelvis krypterings- og passordmekanismer er mulig å skape den nødvendige graden av privathet på nettet som medfører at unntaket etter artikkel 3 nr. 2 kommer til anvendelse. Det er dessuten rimelig å anta at antall personer med adgang til opplysningene ikke i betydelig grad må overstige det som ville typisk gjelder for en familie, husholdning eller nær vennekrets.

## 3.3 Endringsforslag

Selv om *Lindqvist*-avgjørelsen klart bryter med tidligere praksis i henhold til anvendelse av personopplysningsloven § 3 annet ledd er det ikke dermed gitt at bestemmelsen bør endres. Datatilsynet synes på forholdsvis smidig vis å ha kunnet rette seg etter avgjørelsen, og i våre samtaler med andre personer og organisasjoner som har betydelig praktisk erfaring med loven har det ikke kommet frem at avgjørelsen skaper store problemer i henhold til ordlyden i § 3 annet ledd – i alle fall når bestemmelsen leses uavhengig av forarbeidene. Det virker fullt mulig å fortolke bestemmelsen slik at forutsetningen for at et formål kan regnes som privat eller personlig er at behandlingen skjer innenfor en lukket sfære.

---

[72] *Ibid.*, avsnitt 47.

Mer problematisk er forarbeidene: Der er det langt flere formuleringer (bl.a. referansen til "private hjemmesider" kombinert med stor fokus på behandlingsformål) som ikke gir samme "takhøyde" for EF-domstolens avgjørelse som lovbestemmelsen synes å gi. Det kan likevel argumenteres for at disse formuleringene vil få liten betydning for hvordan loven anvendes: "vanlige" mennesker leser ikke forarbeider, og Datatilsynet og de aller fleste (hvis ikke alle) eksperter på feltet kjenner til *Lindqvist*-avgjørelsen og retter seg etter den.

Vi mener likevel at det prinsipielt sett er ønskelig at lovens ordlyd samt forarbeider best mulig gjenspeiler gjeldende rett. Og selv om personopplysningsloven § 3 annet ledd kan gi rom for *Lindqvist*-avgjørelsen er det klart at bestemmelsen har uheldig fokus, ikke bare i lys av denne avgjørelsen, men også til en viss grad i lys av formuleringen i direktivet artikkel 3 nr. 2. Etter vår mening bør § 3 annet ledd omformuleres slik at det kommer tydelig frem at det som er avgjørende for anvendelsen av unntaket er hvorvidt aktiviteten som behandlingen er del av, er privat eller lignende. Vi foreslår følgende ny formulering av § 3 annet ledd:

> Loven gjelder ikke behandling av personopplysninger som den enkelte foretar som ledd i rent personlige, familiemessige eller andre private aktiviteter.

Denne formuleringen bygger tett på direktivet samtidig som den antyder at alle angjeldende aktiviteter skal i grunn være private. Det kan reises spørsmål om referansen til "private" bør suppleres med et kriterium som svært tydelig kommuniserer "lukkethet" overfor omverdenen. En kunne f.eks. tilføye "andre private aktiviteter" med formuleringen "som ikke er tilgjengelige for et ubestemt antall eller ubestemt krets av personer".[73] Vi mener imidlertid at "private" gir tilstrekkelig klare signaler om lukkethet og at tilføyelse av enda flere kriterier vil da virke unødvendig tungt.

[73] Sml. definisjonen av "forskrift" i forvaltningsloven § 2 første ledd bokstav c.

# Kapittel 4

## Personopplysningslovens geografisk virkeområde

### 4.1 Om mandatet

I rammen gjengir vi mandatets punkt 3 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Personopplysningslovens geografisk virkeområde*

Personopplysningsloven § 4 angir det geografiske virkeområdet for personopplysningsloven: "Loven gjelder for behandlingsansvarlige som er etablert i Norge".

Det er ikke helt klart hva som ligger i lovens etableringsprinsipp. Dette kommer særlig på spissen i forbindelse med store internasjonale aktører som har etablert datterselskap eller kontorer i flere land. En praktisk problemstilling kan gjelde en internasjonal legemiddelprodusent, med hovedkontor i et annet land innen EØS og datterselskap, eventuelt bare et kontor, etablert i Norge. Det er imidlertid ofte at det norske datterselskapet eller kontoret ikke er involvert i prosjekter. Datatilsynet forstår § 4 slik at den norske loven likevel kommer til anvendelse med den følge at Datatilsynet må foreta forhåndsvurderingen. Det er ønskelig å få **vurdert hvordan dette har sammenheng med direktivets grunntanke om at lovgivningen i det land hvor behandlingsansvarlige holder til skal legges til grunn**. Problemstillingen har en side mot prinsippet om "fri flyt" og ønsket om å unngå for mange tillatelser og forhåndskontroll.

Departementet ber utrederne vurdere **det nærmere innholdet av etableringsbegrepet**, samt **hensiktsmessigheten av å basere det geografiske virkeområdet på etableringsprinsippet**. Eventuelle foreslag skal være i samsvar med EU-direktivet.

Vi forstår mandatpunktet slik at det først legger opp til en redegjørelse for etableringsbegrepet og -prinsippet i henhold til EU rett, deriblant personverndirektivet, og deretter til en mer rettspolitisk vurdering av dette prinsippets anvendelse i forhold til personopplysningsloven. Mandatpunktet krever følgelig fokus på personopplysningsloven § 4 første ledd der etableringsprinsippet er lagt til grunn, men derimot ingen drøftelse av de øvrige ledd til § 4. Vi finner likevel grunn til å drøfte enkelte problemer som § 4 annet ledd reiser.

### 4.2 Personopplysningsloven § 4 første ledd

Hovedregelen etter personopplysningsloven § 4 første ledd er at loven gjelder for behandling av personopplysninger som forestås av en behandlingsansvarlig som er *etablert* i Norge. Regelen handler ikke bare om lovens geografisk virkeområde, den er i grunn også en regel om lovvalg.[74] Den betyr at loven ikke skal anvendes på behandling av personopplysninger som utføres av behandlingsansvarlige som er etablert i andre EØS-land, selv om opplysningene gjelder personer som er bosatt i Norge eller behandlingen helt eller delvis finner sted i Norge; behandlingen skal da underlegges regelverk i de andre EØS-landene. Samtidig vil loven

[74] Men ikke en regel om jurisdiksjon eller verneting. For en drøftelse av forholdet mellom lovvalgsregler og vernetingsregler i sammenheng med lovgivning om personopplysningsvern (særlig personverndirektivet), se Bing 1999.

under gitte omstendigheter kunne komme til anvendelse på behandling av opplysninger om personer som er bosatt i andre land eller på behandling som helt eller delvis skjer utenfor Norge; loven vil med andre ord kunne ha en viss ekstra-territorial virkning. Regelen er på dette punktet nokså lik det vi antar var regelen etter den gamle personregisterloven: Sistnevnte skulle komme til anvendelse på et utenlandsk personregister dersom en organisasjon som var etablert i Norge hadde "råderett" over registeret.[75]

## 4.3 Direktivet artikkel 4 nr. 1 bokstav a

Personopplysningsloven § 4 første ledd er basert på direktivet artikkel 4 nr. 1 bokstav a som lyder:

> Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

Artikkel 4 tar bl.a. sikte på å unngå at personer blir unndratt beskyttelse ved omgåelse av lovgivning om personopplysningsvern. Dette fremgår av punkt 18 i direktivets fortale:

> Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.

Et annet siktemål er å unngå kumulativ anvendelse av flere lands lovgivning på en behandling. Dette går frem delvis av fortalens punkt 18 samt Europakommisjonens bemerkninger til de tidligere direktivforslag av henholdsvis 24. september 1990[76] og 15. oktober 1992.[77] Siktemålet ligger samtidig innbakt i det såkalte "etableringslandsprinsipp" som artikkel 4 – og dermed pol § 4 første ledd – er delvis utslag av.

## 4.4 Etableringslandsprinsippet

Etableringslandsprinsippet (også kalt "opprinnelseslandsprinsipp" / "country of origin principle" / "Herkunftslandprinzip") innebærer at en organisasjon i utgangspunktet kun skal forholde seg til nasjonale rettsregler i det EU-/EØS-medlemsland hvor den er etablert; organisasjonen skal følgelig kunne utøve virksomhet i andre medlemsland uten å være underlagt disse landenes regelverk.[78] Hovedbegrunnelsen for prinsippet er å fremme forutsigbarhet for organisasjoner som ønsker å foreta aktivitet på tvers av landegrenser (innenfor EU-/EØS-området), og dermed fremme realisering av Det indre marked og dets fire friheter. Prinsippet har basis i EF-traktatens bestemmelser om henholdsvis etableringsfrihet

---

75 Jf. brev av 25. september 1997 fra Lovavdelingen til Datatilsynet (ref. 97/02197KJR/HSD/bj). Sml. Djønne m.fl. 1987 s. 156 (utenlandske registre *muligens* dekket av personregisterloven dersom en norsk-etablert organisasjon kunne endre på opplysningene i registrene). Se også Jarbekk 1996 s. 29flg.

76 COM(90) 314 final - SYN 287.

77 COM(92) 422 final - SYN 287.

78 For en mer inngående redegjørelse for prinsippet se bl.a. Thaulow 2003 og Hörnle 2005.

og fri bevegelse av tjenester (jf. artikkel 43 flg. og 49 flg.). Prinsippet er videre lagt til grunn i mye EU-/EF-lovgivning fra nyere tid, jf. direktiv 2000/31/EF om e-handel (artikkel 3),[79] direktiv 89/552/EØF om grenseoverskridende fjernsynstjenester (endret ved direktiv 97/36/EF) (artikkel 2),[80] og direktiv 99/93/EF om elektroniske signaturer (artikkel 4).[81] I tillegg er prinsippet lagt til grunn i personverndirektivet.

Det er samtidig viktig å merke seg at disse rettsinstrumentene viser noe variasjon når det gjelder prinsippets utforming og gjennomslag. Variasjonene skyldes i hovedsak ulikheter mellom de hensyn som hvert instrument skal ivareta. Dessuten signaliserer variasjonene at det ikke kan tas for gitt at sentrale begrep som inngår i prinsippet – så som etableringsbegrepet – har nøyaktig samme betydning i alle EU-/EF-rettslige sammenhenger der de er benyttet. Dette kommer vi tilbake til straks nedenfor.

## 4.5 Etableringsbegrepet

Hva betyr så "etablert" i henhold til personopplysningsloven § 4 og personverndirektivet artikkel 4? Forarbeidene til personopplysningsloven påpeker at begrepet innebærer at det "faktisk utøves aktiviteter innenfor en forholdsvis fast struktur",[82] og viser her til punkt 19 i direktivets fortale. Betraktningen refererer til

> the effective and real exercise of activity through stable arrangements.

Betraktningen i fortalen påpeker videre at en organisasjons rettslige form eller struktur ikke er av avgjørende betydning i vurderingen av hvorvidt organisasjonen er etablert i et land:

> the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect.

Det foreligger ingen avgjørelser av EF-domstolen som direkte angår innholdet av etableringsbegrepet etter personverndirektivet. Derimot har domstolen truffet flere avgjørelser som tolker etableringsbegrepet i forhold til EF-traktatens bestemmelser om etableringsfrihet og fri bevegelse av tjenester. Disse avgjørelsene er i det minste relevante for en forståelse av etableringsbegrepet i direktivet. Som påpekt ovenfor kan det imidlertid ikke tas for gitt at begrepet i direktivet er ensbetydende med det tilsvarende begrepet som er brukt i EF-traktaten eller andre instrumenter. Likeledes kan ikke alle fortolkninger av begrepet gitt i henhold til ett rettsområde eller -instrument tas til inntekt for å fastlegge begrepets betydning i henhold til ett annet rettsområde/-instrument.[83] Med tanke på at personverndirektivet har en

---

79 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (heretter også "e-handelsdirektivet").

80 Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities (heretter også "fjernsynstjenesterdirektiv").

81 Directive 99/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

82 NOU 1997:19 s. 136; Ot.prp.nr. 92 (1998–99) s. 105.

83 Dette gjelder særlig EF-domstolens fortolkninger av etableringsbegrepet som er avsagt i forhold til bestemmelser vedrørende vernetingsspørsmål, jf. spesielt Brusselkonvensjonen (Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters 1968) artikkel 5 nr. 5, artikkel 8(2) og artikkel 13(2) – nå erstattet av Brusselforordningen (Council Regulation (EC) No. 44/2001 of 22.12.2000 on jurisdiction and enforcement of judgments in civil and commercial matters), jf. særlig artikkel 5 nr. 5, artikkel 9 nr. 2 og artikkel 15 nr. 2. I forbindelse med *Centros*-saken (C-212/97, *Centros Ltd mot Erhvervs- og Selskabsstyrelsen*, European Court Reports 1999 s. I-1459) fastholdt Generaladvokat La Pergola at en ikke kunne anvende domstolens avgjørelser om etableringsbegrepet etter Brusselkonvensjonen artikkel 5 nr. 5 i saker som angår

sterk menneskerettslig forankring (og ikke kun markedsmessige formål),[84] kan det nok tenkes at etableringsbegrepet i direktivet må få en viss selvstendig betydning i forhold til hva som er lagt til grunn etter EU-/EF-rett ellers.

Når dette er sagt, er det lite tvilsomt at EF-domstolens rettspraksis etter EF-traktatens bestemmelser om etableringsfrihet utgjør et viktig referansepunkt for tolkning av etableringsbegrepet i direktivet.[85] Avgjørelsen i *Factortame*-saken er i så måte grunnleggende. Her fastslår domstolen at

> the concept of establishment within the meaning of Article 52 et seq. [nå artikkel 43] of the Treaty involves the actual pursuit of an economic activity through a fixed establishment in another Member State for an indefinite period.[86]

Til tross for at personverndirektivet bruker en noe annerledes formulering enn domstolen gjør, er det mulig å kjenne igjen disse kriteriene i punkt 19 av direktivets fortale.

I flere andre saker har domstolen trukket opp grensen mellom det som utgjør etablering etter EF-traktaten artikkel 43 og det som utgjør tjenesteytelser etter traktaten artikkel 49. Domstolen har i disse sakene understreket at en virksomhet må utøves på en tilstrekkelig fast og regelmessig måte for at etableringsreglene (i motsetning til reglene om tjenesteytelser) skal komme til anvendelse. Avgjørelsen av 11. desember 2003 i *Schnitzer*-saken gir en à jour oppsummering av domstolens praksis vedrørende skillet mellom midlertidig utøvelse av aktivitet (tjenesteytelse) og aktivitet som er tilstrekkelig permanent til å bli ansett som etablering:

> The Court has held that the temporary nature of the activity of the person providing the service in the host Member State has to be determined in the light not only of the duration of the provision of the service but also of its regularity, periodical nature or continuity. The fact that the activity is temporary does not mean that the provider of services within the meaning of the Treaty may not equip himself with some form of infrastructure in the host Member State (including an office, chambers or consulting rooms) in so far as such infrastructure is necessary for the purposes of performing the services in question (Case C-55/94 Gebhard [1995] ECR I-4165, paragraph 27, and Case C-131/01 Commission v Italy [2003] ECR I-1659, paragraph 22).
>
> The Court has distinguished that situation from that of a Member State national who pursues a professional activity on a stable and continuous basis in another Member State where he holds himself out from an established professional base to, amongst others, nationals of that Member State. The Court has drawn the conclusion that such a national comes under the provisions of the chapter relating to the right of establishment and not those of the chapter relating to services (see Gebhard, cited above, paragraph 28).
>
> Thus, 'services' within the meaning of the Treaty may cover services varying widely in nature, including services which are provided over an extended period, even over several years, where, for example, the services in question are supplied in connection with the construction of a large

---

begrepets innhold etter EF-traktatens etableringsregler da "that case-law was developed for purposes that are entirely different from those at issue here" (jf. avsnitt 19).

84 Jf. særlig EF-domstolens avgjørelse av 20. mai 2003 i sak C-465/00, *Rechnungshof mot Österreichischer Rundfunk mfl.* og forente saker C-138/01 og C-139/01, *Neukomm og Lauermann mot Österreichischer Rundfunk.*, European Court Reports 2003 s. I-4989 avsnitt 39–45, 71flg.

85 Derfor er det ikke helt riktig når forarbeidene til personopplysningsloven hevder: "*Avgjørende* er om den behandlingsansvarlige har tilstrekkelig tilknytning til Norge til å være etablert slik uttrykket forstås *ut fra en alminnelig språklig forståelse*", jf. Ot.prp.nr. 92 (1998–99) s. 105 (vår uthevning).

86 C-221/89, *The Queen mot Secretary of State for Transport, ex parte Factortame Ltd and others*, European Court Reports 1991 s. I-3905 avsnitt 20.

> building. Services within the meaning of the Treaty may likewise be constituted by services which a business established in a Member State supplies with a greater or lesser degree of frequency or regularity, even over an extended period, to persons established in one or more other Member States, for example the giving of advice or information for remuneration.
> No provision of the Treaty affords a means of determining, in an abstract manner, the duration or frequency beyond which the supply of a service or of a certain type of service in another Member State can no longer be regarded as the provision of services within the meaning of the Treaty.
>
> It follows that the mere fact that a business established in one Member State supplies identical or similar services with a greater or lesser degree of frequency or regularity in a second Member State, without having an infrastructure there enabling it to pursue a professional activity there on a stable and continuous basis and, from the infrastructure, to hold itself out to, amongst others, nationals of the second Member State, is not sufficient for it to be regarded as established in the second Member State.[87]

Ut fra en samlet vurdering av denne rettspraksisen kan vi fastslå at 3 sentrale kumulative kriterier inngår i etableringsbegrepet:

1. Utøvelse av aktivitet
2. Gjennom fast organisatorisk infrastruktur
3. Over ubestemt tidsrom.

Det er lite tvilsomt at alle tre kriterier også må inngå i etableringsbegrepet etter personverndirektivet artikkel 4 og derfor også personopplysningsloven § 4. Som nevnt ovenfor kan det imidlertid tenkes at disse instrumentenes menneskerettslige fundament krever en mer liberal fortolkning og anvendelse av kriteriene, dvs. at det skal mindre til før en organisasjon er ansett å være etablert etter direktivet artikkel 4 enn ellers er tilfellet etter EF-traktatens bestemmelser om etableringsfrihet og fri bevegelse av tjenester.

Hvorvidt en organisasjon har opparbeidet tilstrekkelig tilknytning til et land til å være etablert der vil bero på en helhetsvurdering av alle 3 kriterier. Organisasjonens rettslige form eller struktur vil være ett moment i denne vurderingen, men ikke avgjørende. Likeledes vil formell registrering av en virksomhet i en stat ikke nødvendigvis bety at virksomheten er etablert i vedkommende stat.[88] En organisasjon kan f.eks. være etablert i et land selv om den kun oppretter et datterselskap eller en filial der og beholder hovedkvarteret i et annet land.[89] Rettspraksis i henhold til EF-traktatens bestemmelser om etableringsfrihet gjør det videre klart at i enkelte tilfeller kan etablering skje ved opprettelse av et enkelt kontor administrert av virksomhetens personale eller en person som har fullmakt til å opptre som agent for virksomheten:

> it must be acknowledged that an insurance undertaking of another Member State which maintains a permanent presence in the Member State in question comes within the scope of the provisions of the Treaty on the right of establishment, even if that presence does not come in the form of a branch or agency, but consists merely of an office managed by the undertaking's own staff or by a person who is independent but authorized to act on a permanent basis for the undertaking, as would be the case with an agency.[90]

---

87 Jf. sak C-215/01, *Bruno Schnitzer*, European Court Reports 2003 s. I-14847 avsnitt 28–32. For en lignende oppsummering se også avgjørelsen i sak C-171/02, *Kommisjonen mot Portugal*, European Court Reports 2004 s. I-5645 avsnitt 24–28.

88 Jf. avgjørelsen i *Factortame*-saken der domstolen fant at registrering av et fiskefartøy i det engelske fiskebåtregisteret ikke var ensbetydende med etablering av fiskerivirksomhet i England.

89 Jf. eksempelvis selskapskonstellasjonene i sak 79/85, *Segers*, European Court Reports 1986 s. 2375, og i sak C 212/97, *Centros*, European Court Reports 1999 s. I-1459.

90 Jf. sak C-205/84, *Kommisjonen mot Tyskland*, European Court Reports 1986 s. 3755 avsnitt 21.

En handelsreisende som er på forretningsreise i et land vil derimot ikke tilfredsstille etableringskriteriene – noe som også forarbeidene til personopplysningsloven påpeker i forhold til pol § 4 første ledd.[91] Det er videre høyst tvilsomt at markedsføring rettet mot et land fra en virksomhet etablert i et annet land i seg selv vil tilfredsstille kriteriene for etablering i landet som mottar markedsføringen.[92] Det samme må nok antas å gjelde selv om virksomheten kanaliserer markedsføringen gjennom et nettsted på en server som er lokalisert i mottakerlandet. Nettstedet i seg selv vil neppe kunne kvalifisere som fast organisatorisk infrastruktur.[93] Støtte for dette finner vi også i punkt 19 i fortalen til e-handelsdirektivet:

> the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity.

Artikkel 2 bokstav c i samme direktiv fastslår også i henhold til en "established service provider" at

> The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.

Selv om det ikke kan tas for gitt at etableringsbegrepet i e-handelsdirektivet har akkurat samme innhold som begrepet i personverndirektivet går det nokså klart fram av begge instrumenter at de tar utgangspunkt i samme rettspraksis om begrepet, særlig avgjørelsen i *Factortame*-saken. Det er også verdt å nevne at arbeidsgruppen som er etablert etter personverndirektivet artikkel 29[94] bruker bestemmelsene i e-handelsdirektivet som referansepunkt for å hevde at markedsføring via et nettsted i seg selv ikke vil tilfredsstille etableringskriteriene i henhold til personverndirektivet artikkel 4:

> The place of establishment of a company providing services via an Internet web site is not the place, at which the technology supporting its web site is located or the place at which its web site is accessible, but the place where it pursues its activity [med henvisning i fotnote til "Directive 2000/31/EC, recital 19"]. Examples are: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London.[95]

## 4.6 Etablering av behandlingsansvarlig i flere land

Generelt sett tillater EU-/EF-retten at en virksomhet er etablert i flere land samtidig. Det er med andre ord vanligvis ikke nødvendig å utpeke kun ett etableringsland per virksomhet. Dersom en virksomhet er etablert i flere land vil dens enkelte etableringer (i form av avdelinger, filialer mv.) i hvert land i utgangspunktet være underlagt angjeldende lands

---

91 Ot.prp.nr. 92 (1998–99) s. 106; NOU 1997:19 s. 136.

92 Sml. en upublisert sak fra Finland der McDonalds-konsernet visst nok er blitt ansett å være etablert i landet etter § 4 i den finske personopplysningsloven på grunnlag av markedsføring som konsernet, via kabel-fjernsyn, overførte til Finland fra utlandet, jf. Kuner 2003 s. 66.

93 Sml. Foss og Bygrave 2000 s. 125 flg som i henhold til vernetingsreglene i Brusselkonvensjonen artikkel 13 nr. 2 argumenterer for at et nettsted muligens kunne utgjøre en "branch, agency or establishment". Derimot inntar de motsatt standpunkt i henhold til Brusselkonvensjonen artikkel 5 nr. 5 i hovedsak grunnet prosessuelle hensyn, jf. *ibid.* s. 132–133.

94 Dvs. Working Party on the Protection of Individuals with regard to the Processing of Personal Data – heretter "artikkel 29 arbeidsgruppen".

95 Artikkel 29 arbeidsgruppen 2002 s. 8.

regelverk. Hvordan får dette utslag i forhold til anvendelse av lovgivning om personopplysningsvern?

Personopplysningsloven gir *prima facie* lite veiledning her. Forarbeidene til loven berører derimot spørsmålet. Ifølge forarbeidene vil eksempelvis et multinasjonalt konsern som behandler personopplysninger både i Norge og et eller flere andre land (f.eks. England og Frankrike), og som har avdelinger el. etablert i alle disse land, være underlagt henholdsvis norsk, fransk og engelsk lovgivning om personopplysningsvern.[96] Som støtte for dette standpunktet viser forarbeidene til personverndirektivet artikkel 4 nr. 1 bokstav a. Forarbeidene påstår at denne bestemmelsen stipulerer at en behandlingsansvarlig som er etablert i flere EU-medlemsland er forpliktet til å overholde den nasjonale lovgivningen *i de respektive land*.[97] Det kan stilles spørsmål om ikke forarbeidene er noe unyanserte på dette punktet.

Den relevante delen av artikkel 4 nr. 1 bokstav a lyder:

> when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by *the national law applicable* [vår utheving].

Jamfør også punkt 19 i direktivets fortale:

> when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.

Disse bestemmelsene refererer kun til en situasjon som involverer *én* behandlingsansvarlig (”the same controller” / ”single controller”). Bestemmelsene vil ikke alltid være relevante i en situasjon der ett multinasjonalt konsern har etableringer i flere land. Ett multinasjonalt konsern vil ofte kunne romme flere behandlingsansvarlige (jf. avsnitt 2.5 ovenfor). Som Kuner så treffende påpeker, ”the rule ’one company, one controller’ does not apply”.[98]

Ut fra disse bestemmelsene er det videre ikke helt klart hvilken medlemsstats lovgivning skal komme til anvendelse; bestemmelsene refererer kun til ”the national law applicable”. Denne formuleringen kan tilsynelatende dekke lovgivning i alle respektive land, i flere av disse eller i kun ett av dem. Tvetydigheten her gjelder ikke bare den engelske versjonen av direktivet artikkel 4 nr. 1 bokstav a, men også andre språkversjoner så som den franske:

> si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable.

– og danske:

> en registeransvarlig, som er etableret på flere medlemsstaters område, skal træffe de nødvendige foranstaltninger til at sikre, at hver af disse virksomheder eller organer opfylder kravene i den gældende nationale lovgivning.

---

96 Jf. Ot.prp.nr. 92 (1998–99) s. 106; NOU 1997:19 s. 136.

97 *Ibid.*

98 Jf. Kuner 2003 s. 64.

Mindre tvetydig er den tyske versjonen som synes å peke i retning av at hvert lands lovgivning skal anvendes i forhold til angjeldende etablering:

> Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im *jeweils* anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält.[99]

Tross tvetydigheten er det klart mulig og naturlig å tolke bestemmelsene dit hen at i en situasjon som faktisk involverer én behandlingsansvarlig med etableringer i flere land skal hvert lands lovgivning anvendes i forhold til den angjeldende etableringens behandling av personopplysninger. Denne tolkningen er lagt til grunn bl.a. av EU-kommisjonen:

> As regards the country of origin rule, the Directive … allows for the organisation of processing under a single data controller, which means complying only with the data protection law of the controller's country of establishment. This of course does not apply where a company has chosen to exercise its right of establishment in more than one Member State.[100]

Artikkel 29 arbeidsgruppen forfekter samme standpunkt:

> When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in course of their activities. It is not an exception to the country of origin principle. It is merely its strict application: where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments.[101]

Som nevnt ovenfor synes også den tyske versjonen av direktivet å støtte opp under denne tolkningen.

Det kan imidlertid ikke tas for gitt at en dermed *automatisk* skal anvende lovgivningen i alle land hvor en behandlingsansvarlig er etablert. Etter vår mening må bestemmelsene om flere etableringer leses i sammenheng med hele artikkel 4 nr. 1 bokstav a. Denne tilnærmingen gir holdepunkt for å hevde at lovgivningen i det enkelte etableringsland kun skal anvendes på behandling av opplysninger som har en sammenheng med den lokale etableringens virksomhet. Dette følger av kravet som ligger innbakt i artikkel 4 nr. 1 bokstav a første ledd om at behandlingen må skje "in the context of the activities of an establishment of the controller".[102] Selv om denne formuleringen er nokså diffus, er den antageligvis tatt med nettopp for å skille ut situasjoner der en etablering i realitet kun har et rent formell eller teknisk forhold til en bestemt behandling av personopplysninger; behandlingen skjer utelukkende for en annen (utenlandsk) etablerings formål og virksomhet. I slike situasjoner vil den behandlingen som den lokale etableringen foretar antageligvis ikke kunne anses å være "in the context of the activities" av etableringen, men "in the context of the activities" av

---

99 Jf. videre den tyske versjonen av fortalens punkt 19: "Wenn der Verantwortliche im Hoheitsgebiet mehrerer Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muß er vor allem zu Vermeidung von Umgehungen sicherstellen, daß jede dieser Niederlassungen die Verpflichtungen einhält, die im *jeweiligen* einzelstaatlichen Recht vorgesehen sind, das auf ihre *jeweiligen* Tätigkeiten anwendbar ist".

100 Jf. EU-kommisjonen 2003 s. 17.

101 Jf. Artikkel 29 arbeidsgruppen 2002 s. 6.

102 Løsningen stemmer også overens med annet EU-regelverk så som e-handelsdirektivet, jf. særlig punkt 19 i direktivets fortale som kommenterer hvordan lovvalgsspørsmålet skal løses når en tjenesteyter etter direktivet er etablert i flere medlemsstater. Se nærmere om dette i bl.a. Thaulow 2003 s. 91–94.

den utenlandske etableringen. Konsekvensen da vil antageligvis være at behandlingen kun er underlagt lovgivningen som gjelder for sistnevnte etablering.

Denne tilnærmingen får støtte i teori.[103] Den synes også å ha blitt lagt til grunn av flere EU-land, deriblant Danmark[104] og Østerrike.[105] Den østerrikske Datenschutzgesetz § 3 nr. 2 fastholder således:

> Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

Forarbeidene til den danske personopplysningsloven går inn for en lignende regel og uttaler i den forbindelse at et behandlingsansvarlig selskap som er etablert i både Danmark og Sverige vil være underlagt dansk lovgivning

> for så vidt angår den behandling av oplysninger, som udføres for den danske 'gren' af selskabet, uanset om behandlingen sker i Sverige eller Danmark.[106]

En slik tilnærming vil kunne bidra til å redusere Datatilsynets (og eventuelt andre nasjonale datatilsynsmyndigheters) arbeidsbyrde ved at tilsynet lettere vil kunne slippe å gå i gang med temmelig tungvinte vurderingsprosesser (f.eks. forhåndskontroll) overfor lokale etableringer i situasjoner der disse etableringene ikke er involvert i nevneverdig grad i aktivitet som er igangsatt og styrt av etableringer i et annet EU-/EØS-land og som ellers vil være underlagt lovgivning i dette landet, jf. Datatilsynets dilemma som er nevnt i mandatpunktet ovenfor.

Det er samtidig viktig å presisere at den skisserte løsningen kun bør gjelde når behandlingen er underlagt lovgivning i et annet EU-/EØS-land som fullt ut tilfredsstiller personverndirektivets krav og – muligens – krav etter den "lokale" lovgivningen, jf. bl.a. det nevnte formålet i fortalens 19. betraktning om å unngå omgåelse av nasjonale regler. Implisitt i dette vilkåret er at det finnes mekanismer for at lokale myndigheter kan anvende den utenlandske lovgivningen. Slike mekanismer skal finnes på dette området, jf. særlig personverndirektivet artikkel 28 nr. 6 – omtalt nærmere nedenfor.

Dersom en legger den nevnte tilnærmingen til grunn oppstår spørsmålet om nøyaktig hvordan formuleringen "in the context of activities" skal forstås. Betyr den at angjeldende etablering skal utøve en selv- eller medbestemmelsesfunksjon i forhold til en behandling av personopplysninger, og dermed fungerer som behandlingsansvarlig? Vi mener at formuleringen sikter lavere, dvs. at den kun krever at det finnes en reell forbindelse mellom behandlingens formål og etableringens virksomhet, men uten at etableringen eksempelvis har fattet selvstendige beslutninger om behandlingens formål, rekkevidde og hjelpemidler – noe som også synes å samsvare med dansk og østerriksk rett. Dette betyr at den "lokale" lovgivningen forholdsvis lett vil kunne komme til anvendelse.

Uansett kan Datatilsynet (og tilsvarende myndigheter i andre EU-/EØS-land) i realitet utøve betydelig skjønn i å fastlegge om nasjonal lovgivning skal anvendes eller ikke. Dette skyldes

---

[103] Jf. Korff 2002 s. 44–45, 47.

[104] Jf. *Behandling af personoplysninger*, Betænkning nr. 1345 1977 s. 221.

[105] Jf. Datenschutzgesetz 2000 § 3 nr. 2.

[106] Jf. Betænkning nr. 1345 1977 s. 221.

ikke bare den nokså diffuse måten som bestemmelsene i direktivet artikkel 4 (og personopplysningsloven) er formulert på, men også reglenes forankring i grunnleggende menneskerettigheter. Dette fundamentet, i likhet med det beslektede hensynet til "ordre public", medfører at terskelen for å anvende nasjonalt regelverk er forholdsvis lav. Datatilsynet vil dermed vanligvis lett kunne finne forsvarlige holdepunkter for å insistere på anvendelse av personopplysningsloven selv på en behandling utført av en lokal etablering på vegne av et selskape etablert i et annet land. Et slikt holdepunkt kunne f.eks. være at behandlingen gjelder særlig sensitive opplysninger.

Situasjoner vil kunne oppstå hvor det er vanskelig å anvende kun ett lands lovgivning på en bestemt behandling eller serie med behandlinger av personopplysninger. Dette følger av at direktivet (og personopplysningsloven) åpner for delt behandlingsansvar (jf. avsnitt 2.5 ovenfor) også på tvers av landegrenser. En behandling eller serie med behandlinger kan da styres av flere behandlingsansvarlige som hver for seg er etablert i forskjellige land og underlagt forskjellige lovgivning. Hvorvidt slike situasjoner egentlig oppstår, vil naturligvis bero på en kontekstavhengig vurdering av hvorledes bestemmelsesrett i forhold til bestemte behandlinger eller et informasjonssystem er delt mellom en organisasjons forskjellige etableringer i angjeldende land. La oss som eksempel ta utgangspunkt i en situasjon med et multinasjonalt selskap med avdelinger i Frankrike og Norge. Selskapets fransk-etablerte avdeling beslutter at visse typer opplysninger om ansatte ved den norske avdelingen skal innsamles og deretter overføres til en database lokalisert og administrert i Frankrike. Fransk lovgivning vil komme til anvendelse etter at opplysningene er overført til databasen. Den vil også komme til anvendelse på et tidligere stadium i og med at den vil regulere hvorvidt og hvordan den franske avdelingen kan samle inn opplysningene. Hvis den norske avdelingen i nevneverdig grad er med på å bestemme hvordan innsamlingen og overføringen skjer, vil den kunne inneha en rolle som behandlingsansvarlig; norsk lovgivning vil da komme til anvendelse på den delen av behandlingen eller rekken av behandlinger som skjer i sammenheng med aktivitetene ("in the context of the activities") av avdelingen. Det motsatte kan muligens være tilfellet dersom innsamlingen og overføringen av opplysningene ikke anses å ha sammenheng med den norske avdelingen. Her vil det imidlertid høyst sannsynlig foreligge en sammenheng siden opplysningene handler om avdelingens ansatte. Resultatet er at det vil – i hvert fall i utgangspunktet – kunne oppstå en viss overlapping av franske og norske regler. Overlappingen vil kunne skape et *potensiale* for regelkollisjon, men vil ikke nødvendigvis føre til kollisjon. Vi antar imidlertid at motstridspotensialet i praksis er nokså liten, jf. våre bemerkninger i neste avsnitt.

## 4.7 Hensiktsmessigheten ved etableringslandsprinsippet

Det å basere personopplysningslovens geografiske virkeområde på etableringslandsprinsippet har flere åpenbare fordeler. Prinsippet tillater at behandlingsansvarlige langt på vei kan drive virksomhet på tvers av landegrenser innenfor EØS-området uten å måtte forholde seg til regelverket om personopplysningsvern i mer enn de land der de er etablerte – som i utgangspunktet behøver ikke å være mer enn ett land. Dermed sikres behandlingsansvarlige en stor grad av forutberegnelighet. Samtidig blir behandlingsansvarlige spart for kostnader som de ellers ville måtte betale dersom de eksempelvis måtte forholde seg til lovgivningen i alle land hvor deres virksomhet har berøringspunkter.

På det mer generelle planet kan det hevdes at prinsippet gjør det enklere å utvikle et dynamisk og innovativ felles europeisk marked for tjenester mv. selv om det er vanskelig å påvise med

stor nøyaktighet prinsippets bidrag til økonomisk vekst.[107] Dette gagner ikke bare tjenesteleverandører og -tilbydere men også en rekke andre aktører inklusive sluttbrukere av tjenester.

Behandling av personopplysninger vil ofte medføre flyt av data over landegrenser slik at den lett vil kunne gi opphav til interlegale problemstillinger. Etableringslandsprinsippet tilbyr forholdsvis stabile kriterier for å takle disse problemstillingene. Det er derfor ikke overraskende at prinsippet i nyere tid er lagt til grunn for å løse spørsmål om lovvalg og verneting i mange internasjonale rettsinstrumenter som omhandler forskjellige former for grenseoverskridende informasjonstjenester.[108]

Alle de nevnte fordelene forutsetter at etableringslandsprinsippet har et ganske fast og sikkert innhold. Denne forutsetningen er langt på vei til stede i hvert fall når det gjelder prinsippets anvendelse i henhold til EF-traktatens bestemmelser om etableringsfrihet og fri bevegelse av tjenester. Prinsippets kjerne har nå blitt forholdsvis grundig fastlagt gjennom EF-domstolens praksis etter disse bestemmelsene.

Det gjenstår likevel betydelig usikkerhet om prinsippets anvendelse i henhold til lovgivning om personopplysningsvern. Mandatpunktet er jo et bevis på dette. Denne usikkerheten gjelder flere viktige momenter, ikke minst etableringsbegrepets nøyaktige innhold og hvorledes prinsippet skal slå ut i forhold til etableringer i flere land. Usikkerheten skyldes delvis lovtekniske faktorer, først og fremst tvetydig og komplisert terminologi i personverndirektivet artikkel 4 nr. 1 bokstav a – noe som har forplantet seg i nasjonal implementering av bestemmelsen.[109] Det er dessuten mangel på rettspraksis og autoritativ veiledning ellers som direkte angår artikkel 4 og tilsvarende bestemmelser i nasjonal lovgivning. Overføringsverdien av rettspraksis i henhold til etableringslandsprinsippets anvendelse etter EF-traktatens bestemmelser om etableringsfrihet mv. er antagelig noe begrenset pga. det grunnleggende menneskerettslige elementet i regelverket om person-opplysningsvern. Et særlig viktig moment som trenger avklaring er hvorvidt den enkelte EØS-medlemsstat kan begrense prinsippets gjennomslag av hensyn til dette elementet.

Fordelene ved etableringslandsprinsippet gagner – i hvert fall prosessmessig – behandlings-ansvarlige snarere enn de registrerte. Prinsippets anvendelse i lovgivning om personopplysningsvern medfører at registrerte personer ofte vil bli tvunget til å reise sak mot behandlingsansvarlige som er etablert i andre land enn der de er bosatt; de vil likeledes ofte bli tvunget til å sette seg inn i utenlandsk rett. En slik situasjon er særdeles lite gunstig for de registrerte, særlig med tanke på skjevheter i ressurs- og maktfordeling som ellers pleier å herske i forholdet mellom organisasjoner og enkeltindivider. Dette er hovedgrunnen til at europeisk regelverk om verneting og lovvalg vanligvis har lagt etableringslandsprinsippet til side når det gjelder visse typer forbrukerkjøp.[110] I lys av den nære forbindelsen mellom forbrukervern og person(opplysnings)vern er det noe underlig at prinsippet ikke har blitt satt til side også ved utforming av personverndirektivet.[111]

---

[107] Jf. f.eks. prognosene i Copenhagen Economics 2005.

[108] Se videre bl.a. Bing 2001.

[109] Se videre bl.a. Kuner 2003 kapittel 2 og 5; Korff 2002 avsnitt 4.2.

[110] Jf. bl.a. Brusselkonvensjonen artikkel 13 til 15; forordning nr. 44/2001 artikkel 15 til 17; Romakonvensjonen (Convention on the Law Applicable to Contractual Obligations 1980) artikkel 5.

[111] Se videre kritikken i Bygrave 2000.

En annen mulig ulempe med prinsippets gjennomføring er at det kan vanskeliggjøre enkelte staters evne til å opprettholde regler som er forholdsvis strenge i forhold til økonomisk betydningsfull virksomhet som lett kan flytte på seg. Faren er at selskaper flytter etableringssted til land med regelverk som tilbyr mer gunstige betingelser for deres virksomhet. For å unngå utflyttingen senker stater sine rettslige standarder – en prosess som ofte omtales som "race to the bottom".

Vi har imidlertid ikke merket konkrete indikasjoner på at etableringslandsprinsippets anvendelse i europeisk lovgivning om personopplysningsvern har satt nevneverdig fart i en slik prosess. Et overveldende flertall av EU-baserte selskaper har uttrykt en positiv holdning til europeiske personopplysningsvernlovers formål og krav[112] – noe som kan tyde på at det vil være vanskelig å få en slik prosess i gang. Dessuten er personverndirektivets minstekrav satt forholdsvis høyt. Derfor vil en eventuell "race to the bottom" (innenfor EU-/EØS-området) ikke få dramatiske konsekvenser.

Etableringslandsprinsippet medfører og forutsetter at landet der en organisasjon er etablert, er forpliktet til å føre en effektiv kontroll med organisasjonens virksomhet. Andre forutsetninger er harmonisering av EU-/EØS-medlemsstaters regelverk samt styrket gjensidig bistand mellom forskjellige lands tilsynsmyndigheter. Personverndirektivet har til formål å legge til rette for at disse forutsetningene finnes. Spesielt viktig i den henseende er artikkel 28 nr. 6 som fordrer samarbeid mellom EU-/EØS-landenes datatilsynsmyndigheter og understreker særlig behovet for utveksling av informasjon. Bestemmelsen fastsetter videre at (eksempelvis) Datatilsynet skal kunne anvende andre EU-/EØS-lands personopplysningsvernlovgivning på behandling av opplysninger som skjer i Norge i regi av behandlingsansvarlige som er etablert i et annet EU-/EØS-land. Dette skal tilsynet kunne gjøre av eget tiltak eller etter henvendelse fra et annet lands myndighet. Denne muligheten er nevnt i forarbeidene til personopplysningsloven,[113] men kommer dårlig til uttrykk i selve lovteksten.

Selv om personopplysningslovens geografiske virkeområde er begrenset på måter som gjør at loven ikke kommer til anvendelse på all behandling av personopplysninger som skjer i Norge, har Datatilsynet likevel inngrepskompetanse overfor all behandling (se pol § 46), dog slik at denne kompetansen til dels gjelder håndhevelse av andre EU-/EØS-lands rett. Når en skal vurdere hensiktsmessigheten ved denne ordningen er det viktig å huske på at landenes lovgivning er bygget over samme lest, og langt på vei har samme beskyttelsesnivå.[114] Selv om flere EØS-lands lovgivning kan komme til anvendelse på behandling av personopplysninger som skjer i Norge, kan rettsanvendelsen samlet sett likevel bli forholdsvis enhetlig. Enkelte forskjeller i de respektive regelverk kan likevel føre til kollisjon av regler. Vi kjenner imidlertid ikke til alvorlige tilfeller av regelkollisjon.

## 4.8 Personopplysningsloven § 4 annet ledd

Som påpekt ovenfor krever mandatet en inngående drøftelse av personopplysningsloven § 4 første ledd der etableringsprinsippet er lagt til grunn, men ingen drøftelse av paragrafens øvrige ledd. Vi finner likevel grunn til å nevne enkelte problemer som § 4 annet ledd reiser.

---

[112] Jf. Eurobarometer 2003.

[113] Jf. NOU 1997:19 s. 136 som nevner at "den norske tilsynsmyndigheten [kan] måtte anvende den danske loven på behandling av personopplysninger som finner sted i Norge og som foretas av en virksomhet som utelukkende er etablert i Danmark".

[114] Jf. også artikkel 29 arbeidsgruppen 2002 s. 6–7.

Ifølge § 4 annet ledd skal loven gjelder for behandlingsansvarlige "som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge", med mindre hjelpemidlene kun brukes til å overføre personopplysninger via Norge. Bestemmelsen reiser flere tolkningsspørsmål.

Et spørsmål gjelder rekkevidden av begrepet "hjelpemidler". Begrepet er ikke definert i selve loven. Ifølge forarbeidene skal begrepet tolkes som "alt slags utstyr som kan brukes til å behandle personopplysninger".[115] Dette samsvarer godt med terminologien i direktivet artikkel 4 nr. 1 bokstav c som pol § 4 annet ledd er basert på og som refererer til "equipment, automated or otherwise". Punkt 20 i direktivets fortale refererer derimot kun til "means used" som muligens kunne omfatte ikke bare fysiske innretninger, men også rent organisatoriske tiltak. De franske og tyske versjonene av direktivet bruker dessuten begrep – "moyens" (fransk) og "Mittel" (tysk) – som tilsynelatende har et videre innhold enn utstyrsbegrepet. Det er imidlertid høyst tvilsomt at den norske loven legger til grunn et begrep som omfatter rent organisatoriske tiltak. Eksemplifiseringen i lovens forarbeider av utstyr som er omfattet av hjelpemiddelsbegrepet ("datamaskiner og -terminaler, telenett og intervjuskjemaer")[116] synes å forutsette anvendelse av forholdsvis håndfaste hjelpemidler, noe som også følger av en alminnelig forståelse av begrepet "utstyr". Det gjenstår likevel flere usikkerhetsmomenter i forhold til hjelpemiddelsbegrepet. Dekker begrepet for eksempel datamaskinprogrammer? Hvorvidt er kun data dekket?

Et annet moment som personopplysningsloven og dens forarbeider gir lite veiledning om gjelder forholdet mellom hjelpemidler og angjeldende behandlingsansvarlig. Er det nok for anvendelse av bestemmelsen i § 4 annet ledd at den behandlingsansvarlig kun *bruker* et hjelpemiddel eller er det også påkrevd at vedkommende utøver kontroll over midlet? Hvis kontroll er nødvendig, hvor mye kontroll? Bestemmelsen refererer kun til bruk av et hjelpemiddel (jf. "benytter"). Tilsvarende bestemmelse i direktivet er likeledes (jf. "makes use of"). Men siden bestemmelsene gjelder en *behandlingsansvarlig* forutsetter de antageligvis at vedkommende i det minste har en medbestemmelsesevne i forhold til hjelpemidlet. Dette følger av definisjonen av behandlingsansvarlig / "controller" i henholdsvis pol § 2 nr. 4 og direktivet artikkel 2 bokstav d.[117]

Spørsmål om påkrevd grad av kontroll over hjelpemidler og om hvorvidt hjelpemiddelsbegrepet omfatter data eller programvare blir særlig viktige når bestemmelsen i pol § 4 annet ledd – og angjeldende bestemmelse i direktivet – skal anvendes i forhold til transaksjoner på internett. I den forbindelse har det oppstått betydelig diskusjon om hvor egnet disse bestemmelsene er til å håndtere realitetene i den digitale online verden. Mest kontroversielt er hvorledes bestemmelsene tilsynelatende slår ut på automatiserte mekanismer for lagring av "cookies" (informasjonskapsler) på harddisker til datamaskiner lokalisert i EU-/EØS-land. Dersom f.eks. et selskap etablert i Kina drifter en server som lagrer cookies på harddisken til en datamaskin brukt av en person som oppholder seg i Norge og som via internettet besøkte serveren, vil personopplysningsloven i utgangspunktet komme til anvendelse på selskapets behandling av informasjonskapslene (forutsatt at kapslene anses å være personopplysninger). Her har en behandlingsansvarlig som er etablert utenfor EØS-

[115] Jf. Ot.prp.nr. 92 (1998–99) s. 106. Definisjonen av begrepet i NOU 1997:19 er muligens litt mer snevert – "Med hjelpemidler forstås utstyr og fysiske innretninger som benyttes til å behandle personopplysninger", jf. s. 137.

[116] *Ibid.*

[117] Jf. bl.a. også Dammann og Simitis 1997 s. 129; Kuner 2003 s. 98; artikkel 29 arbeidsgruppen 2002 s. 9.

området behandlet personopplysninger (informasjonskapslene) ved å benytte hjelpemidler (datamaskinen og dens harddisk) som er lokalisert i Norge.

En slik anvendelse av norsk – og annen europeisk lovgivning om personopplysningsvern – er ikke hypotetisk; den er bl.a. lagt til grunn av artikkel 29 arbeidsgruppen.[118] Den skaper imidlertid en reell fare for overdreven regulering, nærmere bestemt en situasjon der regler kommer til anvendelse på en lang rekke aktiviteter uten at det foreligger stor eller nevneverdig mulighet for at de håndheves, og der respekten for reglene dermed blir undergravet.[119] Det er kanskje mulig å begrense denne faren noe ved å tolke personopplysningsloven § 4 annet ledd – og tilsvarende bestemmelse i direktivet – innskrenkende. En kunne kanskje gjøre bestemmelsene gjeldende kun når en behandlingsansvarlig forsøker å unngå lovgivning i et EU-/EØS-land ved å flytte til og reetablere seg i et ikke-europeisk land (men fremdeles bruker hjelpemidler som befinner seg innen EU-/EØS-området), eller en kunne kreve at den behandlingsansvarlige utøver tilnærmet full kontroll over hjelpemidlene (en grad av kontroll som antageligvis ikke eksisterer ved anvendelse av vanlige "cookies"). Vi er imidlertid usikre på om slike innskrenkende tolkninger er rettslig gangbare i forhold til direktivet.

## 4.9 Endringsforslag

Vi avstår fra å foreslå endringer til personopplysningsloven § 4. Dette er til tross for at etableringslandsprinsippet har visse negative slagsider – særlig overfor de registrerte, og til tross for den tvetydige og kompliserte måten prinsippet manifesterer seg på i personverndirektivet og til en viss grad i personopplysningsloven.

Harmoniserte nasjonale bestemmelser om lovvalg er blant de aller viktigste regler for internasjonal handel og grenseoverskridende virksomhet forøvrig. Derfor er det verken ønskelig eller mulig at personopplysningsloven § 4 i vesentlig grad avviker fra formuleringene eller innholdet i direktivets (eller øvrige EØS-lands) regler om lovvalg. I sin nåværende form gjenspeiler personopplysningsloven § 4 essensen i direktivet artikkel 4 på en brukbar måte.

EU-kommisjonen er klar over at artikkel 4 – og særlig da bestemmelsene i artikkel 4 nr. 1 bokstav c – er vanskelig å tolke. Kommisjonen er dessuten klar over at bestemmelsene er blitt implementert av medlemsstater på forskjelligartet vis. Kommisjonen har imidlertid ikke sagt seg villig til å foreslå endringer på bestemmelsene. I dens første rapport om implementering av direktivet, skriver Kommisjonen følgende om artikkel 4:

> This is one of the most important provisions of the Directive from the perspective of the Internal Market and its correct implementation is crucial for the functioning of the system. The implementation of this provision is deficient in several cases with the result that the kind of conflicts of law this Article seeks to avoid could arise. Some Member States will have to amend their legislation in this regard.
>
> The provision was one of the most criticised during the review process. Submissions argued for a country of origin rule that would allow multinational organisations to operate with one set of rules across the EU. Many also argued that the 'use of equipment' was not an appropriate or workable criterion for determining the application of EU law to controllers established outside the EU.

[118] Jf. artikkel 29 arbeidsgruppen 2002 s. 11.

[119] Jf. Bygrave 2000; Kuner 2003 s. 101 flg.

> As regards the country of origin rule, the Directive already allows for the organisation of processing under a single data controller, which means complying only with the data protection law of the controller's country of establishment. This of course does not apply where a company has chosen to exercise its right of establishment in more than one Member State.
>
> As regards the 'use of equipment' the Commission is aware that this criterion may not be easy to operate in practice and that it needs further clarification. Should such clarification not be sufficient to ensure its practical application, it might in due course be necessary to propose an amendment creating a different connection factor in order to determine the applicable law.
>
> The Commission's priority is, however, to secure the correct implementation by the Member States of the existing provision. More experience with its application and more reflection is needed, taking into account technological developments, before any proposal to change Article 4(1)(c) might be made. Notwithstanding the need for this further reflection, it would be wrong to give the impression that the whole of Article 4 is contested. On the contrary, large areas of its application are uncontested and are the subject of unanimous agreement among all data protection authorities and the Commission.[120]

Vi slutter oss til Kommisjonens uttalelser.

Samtidig ser vi for oss at personopplysningsloven § 4 kunne endres på flere måter. Endringene ville i så fall måtte være av kosmetisk karakter. Etableringsbegrepet kunne f.eks. presiseres i selve loven fremfor forarbeidene. Dette er gjort i den engelske personopplysningsloven, jf. Data Protection Act 1988 section 5(3):

> For the purposes of subsections (1) and (2) [of section 5], each of the following is to be treated as established in the United Kingdom
>
> (a) an individual who is ordinarily resident in the United Kingdom,
>
> (b) a body incorporated under the law of, or of any part of, the United Kingdom,
>
> (c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and
>
> (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom
>
> (i) an office, branch or agency through which he carries on any activity, or
>
> (ii) a regular practice;
>
> and the reference to establishment in any other EEA State has a corresponding meaning.

En slik kasuistisk opplisting innebærer en risiko for at etableringsbegrepet er låst fast til formaliteter, i situasjoner der den nærmere grensedragningen krever kontekstavhengige vurderinger. Tilføyelse til personopplysningsloven av en slik kasuistisk opplisting ville dessuten bidra til å gjøre loven enda mer "topptung" med lange definisjoner, særlig dersom definisjonene av flere av lovens øvrige nøkkelbegrep skal utvides, jf. våre forslag i kapittel 2 og 13. Dersom en definisjon av etableringsbegrepet skulle tilføyes loven ville det vært mest hensiktsmessig å ta utgangspunkt i punkt 19 i fortalen til direktivet samt *Factortame*-avgjørelsen ved å definere begrepet som "utøvelse av aktivitet gjennom et fast organisatorisk

[120] Jf. EU-kommisjonen 2003 s. 17.

infrastruktur over ubestemt tid". Vi mener likevel at begrepet "etablert" allerede langt på vei har denne betydningen ut fra en alminnelig språklig forståelse.

De justeringene vi foreslår som mulige i forhold til etablering av én behandlingsansvarlig i flere land (jf. avsnitt 4.6) kan best implementeres i Datatilsynets praksis.

Vi anbefaler imidlertid at lovens bestemmelser om Datatilsynets kompetanse (jf. kap. VIII) blir endret slik at de klarere gjenspeiler kravene etter direktivet artikkel 28 nr. 6. Disse kravene kommer frem i lovens forarbeider, men er knapt synlige i lovteksten. Selv om vi ikke kjenner til konkrete situasjoner der denne mangelen på synliggjøring har skapt problemer for Datatilsynet eller registrerte, er det prinsipielt sett viktig at loven selv vektlegger internasjonalt samarbeid mellom Datatilsynet og andre lands tilsynsmyndigheter. Særlig gjelder det behovet for å understreke at Datatilsynet har kompetanse til å håndheve andre EU-/EØS-lands lovgivning. Vi foreslår at kapittel VIII i loven får en ny § 42a med overskrift "Datatilsynets kompetanse og rolle i internasjonale forhold", og følgende innhold:

> Datatilsynet kan av eget tiltak eller etter henvendelse fra myndighet i et annet land innenfor EØS-området, kontrollere at behandling av personopplysninger som finner sted i Norge er lovlig, selv om behandlingen er underlagt lovgivning i et annet EØS-land. Datatilsynet kan kreve de opplysningene som trengs for å gjennomføre denne kontroll, jf. § 44. Bestemmelsene i §§ 45, 46 og 47 får tilsvarende anvendelse.
>
> Uten hinder av taushetsplikt kan Datatilsynet utveksle opplysninger med datatilsynsmyndigheter i andre EØS-land når dette er nødvendig for å utføre Datatilsynets oppgaver.

# Kapittel 5

## Ytringsfrihet og personvern – personopplysningsloven § 7

### 5.1 Om mandatet

I rammen gjengir vi mandatets punkt 4 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Ytringsfrihet og personvern – personopplysningsloven § 7*

Personopplysningsloven § 7 regulerer forholdet til ytringsfriheten og gjør unntak fra de fleste bestemmelsene i loven for behandling av personopplysninger dersom behandlingen har "kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål". Datatilsynet har en tilsvarende begrenset tilsynsfunksjon i slike saker. **Det er behov for å utrede om dagens regulering i personopplysningsloven gir en tilfredsstillende avveining mellom de ulike hensynene som gjør seg gjeldende**, og om **det er behov for å justere den som følge av Norges internasjonale forpliktelser**, inkludert direktiv 95/46 EF artikkel 9.

Det vises i denne forbindelse til at ESA (EFTA Surveillance Authority) har reist spørsmål om personopplysningsloven § 7 går for langt i forhold til direktivets korresponderende artikkel 9 (brev 28. november 2002):

Norway is invited to explain and clarify the principles relating to data quality. (…)

Section 7 is some how wider than corresponding Article 9 of the Directive. Section 7 does not have any form of limitation for the processing of personal data carried out solely for journalistic purpose. According to Article 9 exemptions or derogations from provision of some rules of the Directive for the processing of personal data carried out solely for journalistic purposes is legitimate "only if they are necessary to reconcile the right to privacy with rules governing the freedom of expression." Since the Norwegian legislation has omitted this sentence, the result could be that any Norwegian journalistic, artistic or literary expression has been given a *carte blanche* to publish any type of personal data by reference to the principle in Section 7 of the freedom of expression.

Forståelsen av kriteriet "journalistiske, herunder opinionsdannede, formål", har vist seg å volde problemer i praksis. Problemene har i særlig grad vist seg ved bruk av internett til å legge ut personopplysninger. **Departementene ber utrederne om å undersøke omfanget av problemstillingen i praksis, særlig knyttet til bruk av internett.** I denne sammenheng vises det til at Personvernnemnda har to saker til behandling hvor problemstillingen er aktuell (Datatilsynets sak nr. 2004/423 og 2004/508). Sakene gjelder et tilfelle fra Bærum kommune hvor sjikanøse personopplysninger om en ansatt i barnevernet ble lagt ut på private internettsteder.

**Det må som ledd i dette vurderes om dagens strafferettslige reaksjoner er tilstrekkelige**, eller **om Datatilsynet bør få en mer sentral rolle i håndhevingen av sanksjoner som retter seg mot overtramp på nettet**, som for eksempel bruk av nettet til å spre krenkende omtale av enkeltpersoner.

Mandatpunktet slik vi tolker det krever i hovedsak en drøftelse av hvorvidt personopplysningsloven § 7 legger opp til en hensiktsmessig avveining mellom personvernhensyn og hensynet til ytringsfrihet i lys av Norges folkerettslige forpliktelser. Relevante forpliktelser i den forbindelse følger av:

- Verdenserklæringen om menneskerettigheter artikkel 12 og 19;
- FN-konvensjonen om sivile og politiske rettigheter (SP) artikkel 17 og 19;
- Den europeiske menneskerettskonvensjon (EMK) artikkel 8 og 10;
- Europarådskonvensjonen artikkel 9;
- Personverndirektivet artikkel 9.

Alle disse bestemmelsene berører direkte forholdet mellom personvern og ytringsfrihet. I det følgende velger vi imidlertid å fokusere på de nevnte bestemmelsene i EMK og personverndirektivet da disse – samt rettspraksis deretter – har størst praktisk betydning for vurderingen av personopplysningsloven § 7. Bestemmelsene i SP har stort sett samme innhold som EMK artikkel 8 og 10. Det er svært usannsynlig at disse setter strengere eller mer omfattende krav enn det EMK gjør.[121] Samtidig har bestemmelsene i SP mindre veiledningsverdi for vår utredning fordi innholdet i konvensjonen ikke er blitt konkretisert eller nyansert i samme grad som for EMK. Når det gjelder Europarådskonvensjonen artikkel 9 er den i seg selv av forholdsvis liten betydning for vår utredning. Bestemmelsen åpner for unntak fra konvensjonens grunnprinsipper i henhold til kriterier som i hovedsak skriver seg fra EMK artikkel 10. Sistnevnte blir dermed "premissleverandøren" for anvendelse av unntaksbestemmelsen i Europarådskonvensjonen.

Mandatpunktet krever spesiell oppmerksomhet vedrørende ytringer som er fremsatt på internett. Vi forstår mandatpunktet slik at drøftelsen i den forbindelse skal gjelde avgrensningene i personopplysningsloven § 7 vurdert opp mot bestemmelser i annen (nasjonal) lovgivning som kan hindre "overtramp på nettet". Mot slutten av kapittelet redegjør vi således for relevante bestemmelser i bl.a. straffeloven.

Mandatpunktet krever ingen særskilt vurdering av personopplysningsloven § 7 opp mot Grunnloven § 100. Vi avstår derfor fra å redegjøre for grunnlovsbestemmelsen. Vi antar likevel at bestemmelsen, særlig i sin ny form, i praksis ikke medfører skranker eller krav som vesentlig adskiller seg fra det som følger av EMK artikkel 10. Vi kan heller ikke se at de nylig vedtatte endringene til Grl § 100 medfører at interesseavveiningen som personopplysningsloven § 7 representerer, må eller bør justeres. Vi presiserer imidlertid at vi ikke har analysert dette forholdet grundig.

## 5.2 Personopplysningsloven § 7

Bestemmelsen lyder:

> For behandling av personopplysninger utelukkende for kunstneriske, litterære eller journalistiske, herunder opinionsdannende, formål gjelder bare bestemmelsene i §§ 13-15, § 26, §§ 36-41, jf. kapittel VIII.

Unntaket betyr at kun en liten del av lovens bestemmelser kommer til anvendelse på angjeldende behandling. Dette er bestemmelser om informasjonssikkerhet (§ 13),

[121] Jf. videre Eggen 1999 s. 194–195; Eggen 2002 avsnitt 4.5.

internkontroll (§ 14), databehandlers rådighet over personopplysninger (§ 15), reservasjon mot direkte markedsføring ( § 26) og fjernsynsovervåking (§§ 36–41). I tillegg kommer bestemmelser om tilsyn og sanksjoner i lovens kapittel VIII til anvendelse så langt de passer i henhold til de førstnevnte bestemmelsene. Det samme må nok gjelde for lovens "konstituerende bestemmelser" i kapitler I og XI selv om de ikke er eksplisitt nevnt i § 7.

Hovedformålet med unntaket er å hindre at personopplysningsloven urettmessig griper inn i ytringsfrihet og krav som bl.a. følger av Grunnloven § 100 og EMK artikkel 10.[122] Unntaket skal med andre ord sørge for en rimelig balanse mellom personvernhensyn og hensynet til ytringsfrihet, dvs. retten til uhindret å kunne motta og spre opplysninger, tanker og ideer.[123]

Unntaket i § 7 gjelder bestemte *formål* for behandling som bestemmelsen gir anvisning på, og for eksempel ikke kategorier av behandlingsansvarlige. Det er med andre ord ikke den behandlingsansvarliges formell yrkesmessig status som er avgjørende for unntakets anvendelse. Unntaket gjelder eksempelvis for enhver persons behandling av personopplysninger i journalistisk øyemed, ikke bare for profesjonelle journalister.[124]

Det er videre kun når behandling skjer *utelukkende* til de angitte formål at unntaket kommer til anvendelse. Dette betyr for eksempel at unntaket ikke gjelder dersom en avis (også) behandler personopplysninger som ledd i markedsføring eller fakturering.[125]

Mens unntaksbestemmelsen forholdsvis klart definerer hvilke bestemmelser i loven som skal gjelde for behandlinger som er omfattet av unntaket, er det mindre klart hvilke behandlinger unntaket skal gjelde for. Kjernebegrepene "kunstneriske", "litterære", "journalistiske" og "opinionsdannende" er ikke definert i loven, og deres leksikalsk betydning er langt fra entydig. Forarbeidene gir beskjeden hjelp her, og legger til grunn at den nærmere grensedragningen av hva som er "kunstneriske" osv. må i noen grad finne sted gjennom praktiseringen av loven.[126]

Forarbeidene erkjenner samtidig at formålskategoriene må tolkes på romslig vis for at unntaksbestemmelsen skal være forenlig med ytringsfriheten.[127] Særlig uttrykket "journalistiske formål" skal tolkes vidt, noe som tilføyelsen av "herunder opinionsdannende" er ment å tydeliggjøre.[128] Formålskategorien omfatter ikke bare behandling av personopplysninger som ledd i massemedias redaksjonelle virksomhet, men også behandling som enkeltindivider, grupper eller organisasjoner foretar "som ledd i ulike ytringer om samfunnsforhold, f.eks. gjennom løpesedler eller annen form for agitasjon".[129] Forarbeidene antyder her at "journalistiske" og "opinionsdannende" virksomhet i tillegg til å ha til hensikt å påvirke holdninger må relatere seg til spørsmål av samfunnsmessig betydning. Ren kommersiell reklamevirksomhet vil f.eks. åpenbart ikke være omfattet selv om den kan være holdningsskapende.[130] Vi mener samtidig at det ligger en forutsetning innbakt her om at ytringen inneholder bestemte synspunkter på forhold som gjør det relevant å ta

---

122 Jf. Ot.prp. nr. 92 (1998–1999) kapittel 11.

123 Ytringsfrihet omfatter også en rett til å ikke ytre seg. Dette aspektet av ytringsfrihet er imidlertid ikke relevant her.

124 Jf. Ot.prp. nr. 92 (1998–1999) s. 80, 107.

125 *Ibid.* s. 81, 107.

126 *Ibid.* s. 82, 107.

127 Jf. også Eggen 1999 s. 198 i forhold til tilsvarende kategorier i personverndirektivet artikkel 9 (som pol § 7 bygger på).

128 Jf. Ot.prp. nr. 92 (1998–1999) s. 82.

129 *Ibid.*

130 Jf. også Haug Aronsen 2002 s. 80–82.

personopplysninger i bruk. Unntaket vil trolig ikke gjelde dersom en f.eks. publiserer personopplysinger på et nettsted uten at en direkte eller indirekte forsøker å knytte opplysningene til en argumentasjon om samfunnsforhold.[131] Dette vil typisk være tilfelle når publiseringen kun er gjort for å pirre allmennhetens nysgjerrighet. Det motsatte vil trolig gjelde dersom publiseringen er ment f.eks. å belyse en persons egnethet til å inneha en maktposisjon av samfunnsmessig betydning. Selv om det må foreligge en sammenheng mellom personopplysningsbruken og det opinionsdannende formålet for at unntaket etter § 7 skal komme til anvendelse, er det likevel trolig ikke påkrevd at sammenhengen må være tett og umiddelbar slik at det skal være mulig å utlede formålet direkte av den ytringen som inneholder personopplysninger.

Personvernnemnda har i klagesak 2005 nr. 3 tatt stilling til rekkevidden av unntaket for behandling til "opinionsdannende" formål. Klagesaken gjaldt det saksforholdet som er nevnt i mandatpunkt 4 ovenfor: En gruppe som følte seg utsatt for maktovergrep fra barnevernet hadde på flere internettsteder publisert sjikanøse opplysninger om identifiserte fagpersoner – i hovedsak barnevernsansatte – som har hatt befatning med konkrete barnevernssaker. Personvernnemnda tok ikke direkte stilling til spørsmålet om hvor tett sammenheng det må være mellom personopplysningsbruken og angjeldende formål for at unntaket i § 7 skulle komme til anvendelse, men påpekte at selv om nettstedene ikke inneholdt en uttrykkelig formålsangivelse, gikk det samlet sett tydelig fram av deres innhold at de hadde til formål å skape offentlig debatt om barnevernets virksomhet i Norge. Nemnda anså det "som nokså klart" at nettstedene dermed hadde et opinionsdannende formål slik at den behandling av personopplysninger som de manifesterer, falt innenfor unntaket. Nemnda mente videre at ytringens form i den henseende er av underordnet betydning:

> Dette formålet forfølges nok på annen måte enn man ville forvente f eks i en dagsavis. Imidlertid fremstår det ikke som om ytringene har andre formål enn å påvirke opinionen og diskusjonen i det offentlige rom. Formen følger til dels av at nettsider tillater andre uttrykk enn de som typisk velges av en avis eller lignende media, og at den som formulerer ytringene, heller ikke begrenses av denne tradisjonen.

Med henvisning til forarbeidenes uttalelser om forholdet til Grunnloven § 100 og EMK tilføyde nemnda at det "ikke er ønskelig å gjøre denne formen for ytringer gjenstand for forhåndsvurderinger, dvs. sensur". Nemnda presiserte imidlertid at nettstedene måtte, i likhet med media for øvrig, overholde andre regler som gjelder omtale av enkeltpersoner, særlig straffelovens bestemmelser om privatlivets fred og ærekrenkelser.

Det er verdt å merke seg at Personvernnemndas tilnærming her – og for så vidt tilnærmingen i forarbeidene – ikke skiller seg vesentlig fra svensk rettspraksis vedrørende tolking av uttrykket "journalistiska ändamål" i den svenske personuppgiftslagen § 7 (som tilsvarer pol § 7). Dette til tross for at den svenske bestemmelsen ikke inkluderer en henvisning til "opinionsbildande ändamål" el. i forlengelsen av unntaket for "journalistiska ändamål". I en sak med faktiske forhold nokså lik de i klagesaken omtalt ovenfor fastslo Sveriges Högsta domstol at hensikten med å anvende uttrykket "journalistiska ändamål" kan

> inte antas vara ... att privilegiera etablerade massmedier eller personer som är yrkesverksamma inom sådana medier. Med uttrycket torde snarare få antas vara avsett att betona vikten av en fri informationsspridning i frågor av betydelse för allmänheten eller för grupper av människor och en fri debatt i samhällsfrågor.[132]

---

[131] Jf. også Schartum og Bygrave 2004 s. 127.

[132] Jf. dom 12. juni 2001 i sak B293-00 ("Ramsbro"-saken); jf. NJA 2001 s. 409.

Domstolen uttalte videre:

> Det syfte för webbsidan som angetts på denna och som B.R. utvecklat i målet måste mot den angivna bakgrunden anses ligga väl inom ramen för ett journalistiskt ändamål att informera, utöva kritik och väcka debatt om samhällsfrågor av betydelse för allmänheten. I vad mån sedan webbsidan kan anses motsvara godtagbar standard enligt de kriterier som man brukar använda när man värderar etablerad journalistisk verksamhet saknar i sig betydelse för bedömningen.

Domstolens avgjørelse støtter opp under det "norske synet" på hvilke betydning unntaket for behandling til journalistiske formål bør ha i forhold til ivaretagelse av ytringsfrihet. Som vi kommer tilbake til i avsnitt 5.4 har dette synet også solid støtte i rettspraksis etter EMK artikkel 8 og 10.

Avgjørelsene av Högsta domstolen og Personvernnemnda har ikke ryddet alle uklarheter og konflikter av banen i tolkningen av hva som ligger i begrepene "journalistiske", "opinionsdannende" mv. Det største uavklarte spørsmål gjelder trolig hvorvidt journalistisk virksomhet forutsetter redaksjonell bearbeiding av informasjon. Spørsmålet har skapt strid særlig i forbindelse med pressens mulighet til å publisere skattelister på internettet uten nevneverdig redaksjonell bearbeiding av listene. Datatilsynet har lenge ment at denne form for publisering ikke er å anse som journalistikk, og pressen har inntatt motsatt standpunkt.[133] Striden har imidlertid mistet betydelig kraft etter at de nye reglene for offentliggjøring av skattelistene ble vedtatt i 2004 (jf. ligningsloven[134] § 8-8). Det prinsipielle spørsmål gjenstår likevel som uavklart og vil kunne få praktisk betydning i andre sammenhenger enn nettpublisering av ubearbeidede skattelister.

De siste årene er et annet problem med anvendelse av § 7 blitt tydeligere: Datatilsynet har vært tilbakeholdne med å prøve grensene for tilsynets kompetanse i forhold til behandling av personopplysninger som "ligger i grenseområdet mellom ytringsfrihet og personvern". Dette kommer bl.a. frem i forbindelse med klagesaken 2005 nr. 3 der tilsynet ikke ville ta stilling til om den angjeldende behandlingen av opplysninger var gjort for opinionsdannende formål eller ikke. Med henblikk på legalitetsprinsippet og EMK artikkel 10(2) mente Datatilsynet at det mangler klar nok hjemmel etter personopplysningsloven til å gi en slik vurdering.

Vi mener imidlertid at Datatilsynet har tilstrekkelig hjemmel i pol § 42 tredje ledd nr. 3: Det å "kontrollere" at loven "blir fulgt", innebærer at tilsynet også skal kunne ta stilling til om en konkret behandling faller inn under unntaksbestemmelsen i § 7, selv om resultatet av vurderingen vil kunne medføre innskrenkinger i ytringsfrihet.

## 5.3 Forholdet til personverndirektivet artikkel 9

Personopplysningsloven § 7 gjennomfører personverndirektivet artikkel 9, som lyder:

> Member States shall provide for exemptions or derogations from the provisions of this Chapter [II], Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

---

[133] Se videre Haug Aronsen 2002 s. 75–78 for en (kritisk) redegjørelse for konflikten.

[134] Lov 13. juni 1980 nr. 24.

Det sentrale normative elementet ved artikkel 9 er et proporsjonalitetsprinsipp: Unntak kan kun gjøres så langt det er nødvendig for å forene retten til privatlivets fred med reglene om ytringsfrihet. De rettighetene som da skal balanseres, er nærmere spesifisert i direktivets fortale, jf. betraktningene i punkt 37 og 10. Lest i sammenheng tydeliggjør betraktningene at avveiningen i det vesentlige dreier seg om forholdet mellom EMK artikkel 8 og artikkel 10.

En del av den grunnleggende avveiningen mellom disse to sett av rettigheter er foretatt ved at artikkel 9 ikke tillater at det gjøres unntak fra flere av direktivets regler, bl.a. reglene i kapittel I (alminnelige bestemmelser), kapittel III (rettsmidler, ansvar og sanksjoner) og kapittel V (adferdskodekser). I følge punkt 37 i fortalen skal det heller ikke gjøres unntak fra reglene om informasjonssikkerhet (jf. artikkel 17). Betraktningen påpeker også at datatilsynsmyndigheter ikke skal være helt avskåret fra å utøve tilsynsmyndighet på dette feltet:

> at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities.

I tillegg medfører proporsjonalitetsprinsippet i artikkel 9 visse begrensninger av EU-/EØS-medlemsstaters adgang til å fastsette unntak. Det er nokså klart at prinsippet ikke tillater at det gis et generelt unntak for virksomhet for en hel bransje (f.eks. pressen).[135] Likeledes skal unntak ikke bli forbeholdt utvalgte yrkesgrupper (f.eks. profesjonelle journalister); unntakene må gjelde for enhver person som behandler personopplysninger til ett eller flere av formålene angitt i artikkel 9.[136]

Det har vært reist spørsmål om direktivet generelt gir nok albuerom til ytringsfrihet. Spørsmålet ble bl.a. reist på slutten av 1990-tallet under utforming av Sveriges personuppgiftslag og da særlig i forhold til de svenske grunnlovsbestemmelsene om trykk- og ytringsfrihet.[137] Spørsmålet ble samtidig vurdert i Norge av Kyrre Eggen på oppdrag av Ytringsfrihetskommisjonen i forbindelse med revisjonen av Grl § 100. Svaret den gangen var et noe nølende nei.[138] Vi slutter oss til både svaret og Eggens tilknyttede resonnement. EF-domstolen har siden besvart spørsmålet med et nei som er langt mindre nølende:

> [T]he provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the … [European Convention for the Protection of Human Rights and Fundamental Freedoms]. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question ….[139]

Artikkel 9 i direktivet legger som nevnt flere begrensninger på medlemsstaters fastsetting av unntak etter bestemmelsen. Den gir likevel statene et betydelig spillerom. Dette spillerommet er nok påkrevd av hensyn til flere prinsipper og doktriner, bl.a. subsidiaritetsprinsippet i EU-/EF-retten[140] og doktrinen om "margin of appreciation" i forhold

---

135 Jf. også Artikkel 29 arbeidsgruppen 1997 s. 8.

136 *Ibid.*

137 Se Öman og Lindblom 2001 s. 78 med videre henvisninger.

138 Jf. Eggen 1999 s. 198, 210–213, 225–226, 248–251.

139 *Lindqvist*-dommen avsnitt 90.

140 Jf. EF-traktaten artikkel 5.

til EMK.[141] Spillerommet er blitt utnyttet fullt ut slik at medlemslandenes implementering av artikkel 9 spriker i mange retninger. Tilstanden er treffende oppsummert av Korff:

> [T]he laws in the Member States in this respect are clearly widely divergent, and range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, to a system which is tantamount to imposing prior restraint on the publication of certain information by the press. Also, some defer expressly to press laws or (self-regulatory or quasi-imposed) codes of conduct and associated regulatory mechanisms, while others set out the relevant rules in the data protection law itself. This is clearly an area in which no serious convergence can be discerned.[142]

Den tilstanden Korff beskriver, er ikke overraskende tatt i betraktning den betydelige mangelen på konvergens i implementering av andre deler av direktivet.[143] Det er samtidig vanskelig å se hvordan spillerommet kunne ha blitt krympet uten å bryte med overordnete styringsprinsipper eller folkerettslige doktriner (som nevnt ovenfor).

Som påpekt i mandatpunkt 4 har EFTA Surveillance Authority (ESA) reist spørsmål om personopplysningsloven § 7 går for langt i forhold til artikkel 9. Grunnen til spørsmålet er at § 7 ikke inneholder en formulering tilsvarende formuleringen i artikkel 9 som uttrykker proporsjonalitetsprinsippet – dvs. at unntak skal gjøres "only if they are necessary to reconcile the right to privacy with rules governing the freedom of expression". Ved utelatelsen av en slik formulering synes ESA å anta at den norske bestemmelsen åpner for en urettmessig vektlegging av hensynet til ytringsfrihet på bekostning av personvernhensyn.

Det er imidlertid høyst tvilsomt at artikkel 9 krever at tilsvarende bestemmelser i nasjonal lovgivning skal inneholde en slik formulering. Poenget med artikkel 9 er å sikre at medlemsstatene selv overholder proporsjonalitetsprinsippet når de vurderer hvilke unntak som skal implementeres. Etter vår mening er det ikke påkrevd at det skjer en proporsjonalitetsvurdering etter at unntak er nedfelt i lovgivning så lenge unntakene selv er blitt utformet i henhold til prinsippet. Proporsjonalitetsvurderinger kan med andre ord være forbeholdt lovgiver; de trenger ikke å bli fortløpende gjennomført i forhold til enhver behandling av eksempelvis tilsynsmyndigheter eller behandlingsansvarlige. Flere andre land – deriblant Sverige[144] og Danmark[145] – synes å ha lagt samme standpunkt til grunn i sin implementering av artikkel 9.

I et svarbrev til ESA har Justisdepartementet skrevet bl.a. følgende om problemstillingen:

> [I]t is not our understanding that the Directive requires the Member States to include this phrase ["only if they are necessary to reconcile the right to privacy with rules governing the freedom of expression"] in their exemptions made under Article 9. The meaning of this phrase is rather that it requires the Member States to determine what exemptions are necessary and to provide for such exemptions only.[146]

Vi er enige med dette synspunktet.

---

[141] Se videre f.eks. Harris mfl. 1995 s. 290–301, 344–353.

[142] Korff 2002 s. 138.

[143] Jf. videre EU-kommisjonen 2003.

[144] Jf. personuppgiftslagen § 7.

[145] Jf. personoplysningsloven § 2 stk. 6–10. Jf. også f.eks. *Behandling af personoplysninger*, Betænkning nr. 1345 1977 s. 208.

[146] Jf. brev 18.2.2003 til ESA (ref. 021/10392 ES KES/GMA/mk).

Det avgjørende spørsmålet blir deretter om de unntak som lovgiver har fastsatt i pol § 7 er resultat av en tilstrekkelig proporsjonalitetsvurdering. Dersom unntakene i pol § 7 hadde gitt en "carte blanche" til publisering av enhver type personopplysninger som ledd i journalistisk mv. virksomhet – som ESA syn(t)es å mistenke er tilfellet – er det på det rene at proporsjonalitetsvurderingen ikke ville vært tilstrekkelig. Men § 7 gir ikke en slik mulighet; bestemmelsen unntar ikke behandling av personopplysninger til angjeldende formål fra regulering etter annen lovgivning eller fra andre typer reguleringer. Som Justisdepartementet påpeker i sitt brev til ESA:

> Section 7 does not prevent liability or sanctions as otherwise provided for by Norwegian law. Prevented is merely the application of a set of rules, which, if they were to be applied to the processing of personal data solely for journalistic, artistic or literary purposes, could amount to censorship.

Det er på det rene at en rekke bestemmelser i annen lovgivning vil kunne anvendes i forhold til publisering av personopplysninger til journalistiske formål mv., jf. bl.a. oversikten i avsnitt 5.5 nedenfor. I tillegg kommer begrensninger som følger av yrkesetiske kodekser, først og fremst pressens Vær Varsom-plakat og avgjørelser i Pressens faglige utvalg.

Et annet mulig problem er imidlertid at mye av fleksibiliteten som direktivet artikkel 9 uttrykker, er blitt fjernet i personopplysningsloven ved at § 7 langt på vei uttømmende angir hvorledes balansen mellom hensynet til ytringsfrihet og personvernhensyn skal være. Paragraf 7 har derfor vært kritisert.[147] Det dynamiske elementet var mye bedre ivaretatt i Skaugeutvalgets lovforslag (jf. § 5):

> Loven gjelder for behandling av personopplysninger som utelukkende finner sted i journalistisk øyemed eller for kunstnerisk eller litterær virksomhet. Det skal gjøres unntak fra bestemmelsene i den grad det er nødvendig for å forene hensynet til ytringsfrihet med hensynet til personvern.[148]

Løsningen som Skaugeutvalget foreslo, ble kraftig kritisert i høringsrunden bl.a. av hensynet til forutberegnelighet. Vi er enige i at forutberegnelighetshensyn må tillegges stor vekt. Dette gjelder særlig når den påkrevde interesseavveiningen er så kompleks. Fordelen med å formulere unntaket slik det siden ble gjort i personopplysningsloven er at en trenger mindre juridisk ekspertise for å tolke § 7 enn om en skulle ta stilling til den folkerettslige utviklingen innen vern av ytringsfrihet.

Det er videre tvilsomt om en løsning tilsvarende § 5 i Skaugeutvalgets lovforslag ville tilfredsstille lovskravet etter EMK artikkel 10 nr. 2. Som Justisdepartementet skriver i sitt brev til ESA,

> [i]t may be argued that merely quoting, in Section 7 of the Personal Data Act, the vague reservation made in Article 9 of the Directive ("only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression"), could create problems with respect to ECHR. It is questionable whether it would be in accordance with the concept of rule of law to leave it to the public to bear the risk of reconciling the different interests at stake. Rather, the vague reservation made in Article 9 of the Directive must in national law be transposed into proper rules of a certain clarity giving the public sufficient foreseeable guidance as regards what is legal and what is not.

---

147 Jf. Haug Aronsen 2002 kapitlene 6 og 7.

148 Jf. NOU 1997:19 s. 165.

Vi er enige.

## 5.4 Forholdet til EMK

Det fremgår av forrige avsnitt at proporsjonalitetsprinsippet med tilhørende vurderinger i stor grad bygger på forholdet mellom EMK artikkel 8 og artikkel 10. Dette forholdet danner dermed et viktig moment i analysen av hvorvidt personopplysningsloven § 7 representerer en tilstrekkelig proporsjonalitetsvurdering. Forholdet er meget sammensatt. Dette skyldes flere faktorer, ikke minst at angjeldende praksis fra Den europeiske menneskerettighetsdomstolen (EMD) er omfangsrik, kompleks og dynamisk. I det følgende gir vi kun et forenklet omriss av de mest sentrale aspektene ved denne rettspraksisen som har relevans for mandatpunkt 4.[149]

Det er for det første viktig å understreke at forholdet mellom EMK artikkel 8 og artikkel 10 gjelder likeverdige rettigheter. Ytringsfrihet etter artikkel 10 har ikke høyere normativ status enn personvern etter artikkel 8; den ene får med andre ord ikke presumptiv forrang over den andre. Eller som Europarådets Parlamentarikerforsamling (Parliamentary Assembly) uttrykker det, ”these rights are neither absolute nor in any hierarchical order, since they are of equal value”.[150]

Hovedspørsmålet gjelder da hvorvidt det er nødvendig at den ene rettigheten begrenses for å ivareta de underliggende verdiene som den andre rettigheten beskytter. I vurderingen av dette spørsmålet legger EMD til grunn de samme momentene uavhengig av om vurderingen tar utgangspunkt i artikkel 10 (dvs. en vurdering av hvilke inngrep i ytringsfrihet myndigheter kan gjøre av hensyn til personvern uten å krenke ytringsfrihet) eller artikkel 8 (dvs. en vurdering av hvilke inngrep i personvern myndigheter kan gjøre av hensyn til ytringsfrihet uten å krenke personvernet). Alt dette kommer særlig frem av den såkalte ”Caroline”-dommen som er omtalt nedenfor.

Brorparten av EMDs praksis i denne sammenheng dreier seg om pressens virksomhet. Domstolen anerkjenner for det første at pressens virksomhet utgjør en vesentlig del av den ytringsfriheten som faktisk finner sted. Slik virksomhet utøver ytringsfrihet og er en sentral formidler av andres ytringer. Samtidig blir pressens rolle som ”public watchdog” fremhevet. Pressen skal avsløre hendelser – maktmisbruk, diskrepans mv. – som har betydning for et demokratisk samfunns funksjonalitet:

> Whilst the press must not overstep the bounds set, inter alia, in the interest of 'the protection of the reputation and rights of others', it is nevertheless incumbent on it to impart information and ideas of public interest. Not only does the press have the task of imparting such information and ideas: the public also has a right to receive them. Were it otherwise, the press would be unable to play its vital role of 'public watchdog'. Although formulated primarily with regard to the print media, these principles doubtless apply also to the audiovisual media.[151]

I lys av denne rollen skal journalister ha stor frihet til selv å avgjøre hvordan de skal innhente og bearbeide personopplysninger og hvordan disse skal publiseres:

---

[149] For en mer utførlig analyse se særlig Eggen 2002 del IV.

[150] Jf. Resolution 1165 (1998) on the right to privacy, avsnitt 11 – sitert av EMD i dommen 24. juni 2004 *Von Hannover mot Tyskland* (Caroline-dommen) avsnitt 42. Jf. også House of Lords avgjørelsen i *Campbell v. Mirror Group Newspapers Ltd.* [2004] 2 AC 457, særlig avsnitt 55.

[151] Jf. dom 23. september 1994 *Jersild mot Denmark* avsnitt 31.

> [T]he methods of objective and balanced reporting may vary considerably, depending among other things on the media in question. It is not for this court, nor for the national courts for that matter, to substitute their own views for those of the press as to what technique of reporting should be adopted by journalists. In this context the court recalls that article 10 protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed.[152]

Dette betyr f.eks. at artikkel 10 i utgangspunktet overlater til journalister selv å avgjøre hvorvidt det er nødvendig å publisere materiale for å sikre troverdighet.[153] Journalister er også tillatt bruk av provoserende virkemidler.[154]

Disse prinsippene er i hovedsak utviklet av EMD i saker som angår etablerte massemedia. Det er imidlertid klart at prinsippene også har overføringsverdi i forhold til opinionsdannende ytringer fremsatt av folk som ikke er profesjonelle journalister. I en avgjørelse fattet i fjor uttalte EMD bl.a. følgende:

> The Government have pointed out that the applicants were not journalists, and should not therefore attract the high level of protection afforded to the press under Article 10. The Court considers, however, that in a democratic society even small and informal campaign groups … must be able to carry on their activities effectively and that there exists a strong public interest in enabling such groups and individuals outside the mainstream to contribute to the public debate by disseminating information and ideas on matters of public interest such as health and the environment ….[155]

> It is true that the Court has held that journalists are allowed 'recourse to a degree of exaggeration, or even provocation' …, and it considers that in a campaigning leaflet a certain degree of hyperbole and exaggeration is to be tolerated, and even expected.[156]

Samtidig er det viktig å være klar over at artikkel 10 i seg selv medfører visse forpliktelser for journalister og andre når de behandler personopplysninger. Bestemmelsen forutsetter bl.a. at journalister handler i god tro for å gi riktig og nøyaktig informasjon i samsvar med deres yrkeskodeks. Dette gjelder også reportasjer om saker av allmenn interesser:

> Article 10 of the Convention does not … guarantee a wholly unrestricted freedom of expression even with respect to press coverage of matters of serious public concern. Under the terms of paragraph 2 of the Article the exercise of this freedom carries with it 'duties and responsibilities' which also apply to the press. These 'duties and responsibilities' are liable to assume significance when … there is question of attacking the reputation of private individuals and undermining the 'rights of others'. […] By reason of the duties and responsibilities' inherent in the exercise of the freedom of expression, the safeguard afforded by article 10 to journalists in relation to reporting on issues of general interest is subject to the proviso that they are acting in good faith to provide accurate and reliable information in accordance with the ethics of journalism.[157]

Lignende forbehold gjelder for ytringer fremsatt av enkeltindivider og grupper utenfor de etablerte massemediene.[158]

---

[152] *Ibid.*

[153] Jf. dom 21. januar 1999 *Fressoz og Roire mot Frankrike* særlig avsnitt 54.

[154] Jf. bl.a. dom 24. februar 1997 *De Haes og Gijlsels mot Nederland* særlig avsnitt 48.

[155] Jf. dom 15. februar 2005 *Steel og Morris mot United Kingdom* avsnitt 89.

[156] *Ibid.* avsnitt 90.

[157] Jf. dom 20. mai 1999 *Bladet Tromsø og Stensaas mot Norge* avsnitt 65.

[158] Jf. *Steel og Morris* avsnitt 90 flg.

I avveiningen mellom hensynet til ytringsfrihet og personvernhensyn legger EMD vekt på en lang rekke momenter, deriblant ytringens karakter (er den f.eks. en verdivurdering ("value judgment") eller en faktisk påstand ("factual statement")?),[159] ytringens form og medium (er den f.eks. audiovisuelt eller ren tekst?),[160] ytringens kontekst (foreligger det eksempelvis et "climate of continual harrassment"?),[161] emnet for ytringen (gjelder den f.eks. omtale av en offentlig person eller privatperson?)[162] og ytrerens formål (har f.eks. ytreren til hensikt å fokusere på en sak av allmenn interesse eller kun å sjikanere andre?).[163] De samme momentene legges til grunn i norsk rettspraksis på feltet.[164] Vektlegging av momentene og deres samspill varierer naturligvis fra sak til sak. Likevel kommer det frem av EMDs praksis at det sentrale momentet er hvorvidt ytringen bidrar til en debatt av generell samfunnsinteresse. Jo mer en ytring bidrar i så måte desto mer vern vil den få på bekostning av personverninteresser.

Betydningen av dette er godt illustrert i en av de prinsipielt viktigste avgjørelsene som EMD har truffet i nyere tid om forholdet mellom ytringsfrihet og personvern: dom 24. juni 2004 *von Hannover mot Tyskland* ("Caroline-dommen). Dommen gjaldt tysk tabloidpressens trykking av fotografier av Prinsesse Caroline von Hannover i forskjellige daglige situasjoner utenom offisielle oppdrag. Dommen er prinsipielt viktig fordi EMD for første gang slo fast at EMK artikkel 8 medfører at konvensjonsstater har en positiv forpliktelse til å gi enkeltindivider en viss grad av person*opplysnings*vern overfor andre *private* rettssubjekter. Bestemmelsen får dermed såkalte tredjepartsvirkning i forbindelse med behandling av personopplysninger. Dommen er også prinsipielt viktig fordi den klart og tydelig bekrefter at de begrensningene som følger av nevnte forpliktelse også gjelder når opplysningene omhandler offentlig kjente personer. Kjendiser har med andre ord en rett til privatliv og skal dermed ikke være "fritt vilt" for massemedier. Domstolen understreket videre at pressens offentliggjøring av personopplysninger i hovedsak kun er berettiget når opplysningene bidrar til en debatt av generell samfunnsmessig interesse:

> the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of general interest.[165]

Når det gjelder hva som er av samfunnsmessig interesse trakk domstolen i det vesentlige det samme skillet som Lord Wilberforce gjorde i hans berømte uttalelse om at "… there is a wide difference between what is interesting to the public and what it is in the public interest to make known".[166] I følge EMD vil ikke formidling av personopplysninger om en persons privatliv for å tilfredsstille nysgjerrighet kunne anses å bidra til en debatt av samfunnsmessig interesse:

> The Court considers that a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private

[159] Jf. bl.a. dom 8. juli 1986 *Lingens mot Østerrike* særlig avsnitt 46.
[160] Jf. bl.a. *Jersild* avsnitt 31.
[161] Jf. bl.a. *Von Hannover* avsnitt 59 og 68.
[162] Jf. f.eks. dom 23. mai 1991 *Oberschlick mot Østerrike* særlig avsnitt 59.
[163] Jf. f.eks. dom 25. juni 1992 *Thorgeirson mot Island* særlig avsnitt 66.
[164] Jf. bl.a. Rt. 2002 s. 764, Rt. 2003 s. 928, Rt. 2003 s. 1190, Rt. 2004 s. 510, RG 2004 s. 618, Rt. 2005 s. 1677.
[165] *Von Hannover* avsnitt 76.
[166] Jf. *British Steel Corporation v. Granada Television Ltd.* [1981] AC 1096, 1168G.

> life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of 'watchdog' in a democracy by contributing to 'impart[ing] information and ideas on matters of public interest …' it does not do so in the latter case.[167]
>
> As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.[168]
>
> Furthermore, the Court considers that the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public. Even if such a public interest exists, as does a commercial interest of the magazines in publishing these photos and these articles, in the instant case those interests must, in the Court's view, yield to the applicant's right to the effective protection of her private life.[169]

Caroline-dommen fastslår som nevnt at artikkel 8 får tredjepartsvirkning i forhold til behandling av personopplysninger. Det nøyaktige omfanget av denne virkningen er imidlertid noe usikkert. At den medfører begrensninger på pressens trykking og annen offentliggjøring av personopplysninger er på det rene, men hvorvidt den medfører begrensninger på eksempelvis innsamling og lagring av opplysninger forut publisering går ikke helt klart frem av dommen. Det er blitt reist spørsmål om ikke visse avsnitt i dommen peker mot sistnevnte begrensninger, jf. særlig følgende:

> The Court finds another point to be of importance: even though, strictly speaking, the present application concerns only the publication of the photos and articles by various German magazines, the context in which these photos were taken – without the applicant's knowledge or consent – and the harassment endured by many public figures in their daily lives cannot be fully disregarded ....[170]
>
> Furthermore, increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data .... This also applies to the systematic taking of specific photos and their dissemination to a broad section of the public.[171]

Det er likeledes blitt reist spørsmål om dommen – sammen med flere andre dommer som er avsagt i nyere tid[172] – signaliserer at EMD nå vektlegger personverninteresser sterkere enn tidligere i forhold til massemedia. Etter vår mening et det utvilsomt at EMD i de avsnittene vi har sitert ovenfor oppstiller momenter som er generelt relevante i avveiningen mellom de konkurrerende hensyn som fremkom i Caroline-saken. Det er likevel høyst tvilsomt at domstolen her (eller i dommen for øvrig, eller i de avgjørelsene henvist til i fotnote 56) krever økt regulering av pressens behandling av personopplysninger forut publisering. Dette ville i så fall bryte med domstolens tradisjonell tilbakeholdenhet mot å gripe inn (eller la andre domstoler og myndigheter griper inn) i journalisters arbeidsmetoder. Vi kan heller ikke se at EMD gjennom disse avgjørelsene signaliserer at den nå vektlegger personverninteresser

---

167 *Von Hannover* avsnitt 63.

168 *Ibid*. avsnitt 65.

169 *Ibid*. avsnitt 77.

170 *Ibid*. avsnitt 68.

171 *Ibid*. avsnitt 70.

172 Jf. særlig dom 30.3.2004 *Radio France mfl. mot Frankrike*, dom 29. juni 2004 *Chauvy mfl. mot Frankrike*, og dom 17.12.2004 *Cumpana og Mazare mot Romania*.

sterkere enn tidligere overfor media.[173] Avgjørelsene tydeliggjør derimot rekkevidden av disse interessene sterkere, bl.a. ved å gjøre det klart at artikkel 8 beskytter offentlige personers personverninteresser mot overgrep fra private aktører. Vi kan følgelig ikke se at avgjørelsene setter et alvorlig spørsmålstegn ved den regulatoriske ordningen som er lagt til grunn i personopplysningsloven § 7, og som langt på vei begrenser tilsyn med pressens behandling av personopplysninger til "etterfølgende ansvar for det ferdige og publiserte produktet".[174]

Ut i fra en vurderingen av EMDs samlede praksis på feltet, finner vi ikke holdepunkter for å hevde at det må eller bør skje en justering av personopplysningsloven § 7. Den avveiningen mellom hensynet til ytringsfrihet og personvernhensyn som § 7 uttrykker – og som Personvernnemnda så langt har lagt til grunn (jf. klagesak 2005 nr. 3) – er fullt ut forsvarlig i henhold til EMK.

## 5.5 Beskyttelse i forhold til nettpublisering

Behandling av personopplysninger som faller inn under unntaket etter personopplysningsloven § 7 vil som påpekt ovenfor kunne reguleres av flere regler i annen lovgivning samt visse yrkesetiske regler. I det følgende gir vi en kort drøftelse av hvorvidt disse reglene vil kunne anvendes i tilfeller der personverninteresser (i vid forstand) blir skadelidende pga. at personopplysninger blir lagt ut på offentlig tilgjengelige steder på internettet.

En rekke regler vil i utgangspunktet kunne komme til anvendelse, men anvendelsen vil ikke nødvendigvis føre til sanksjoner. Akkurat hvilke regler som vil være mest relevante vil naturligvis avhenge av ytringens innhold og formål mv., og dermed av hvilke personverninteresser ytringen truer. Er det f.eks. personers omdømme og/eller selvaktelse som står på spill, er det primært straffelovens bestemmelser om ærekrenkelser som vil være relevante (jf. §§ 246 og 247). Skjer det offentliggjøring av privatsensitive opplysninger, vil straffelovens bestemmelse om krenkelser av privatlivets fred være relevant (jf. § 390). Publisering av personbilder vil kunne vurderes etter åndsverkloven § 45c. Driver et nettsted med trakassering av personer vil straffeloven § 390a muligens komme til anvendelse. Skjer trakasseringen på grunnlag av etnisitet, religiøs tilhørighet mv. vil den kunne rammes av straffeloven § 135a.

Disse bestemmelsene er supplert av ulovfestede regler om vern for personligheten som på enkelte punkter vil kunne gå lenger enn lovgivningen. I tillegg vil visse yrkesetiske kodekser kunne komme til anvendelse. Pressens Vær Varsom-plakat håndheves av Pressens faglige utvalg også i forhold til nettpublisering som forestås av det etablerte massemedia (inklusive kringkastingsselskapene). Det finnes dessuten et sett med "etiske regler for Internett", samt mer spesifikke retningslinjer for god nettskikk vedrørende henholdsvis personvern og informasjonskontroll, som er utformet av Nettnemnda – et selvreguleringsinitiativ igangsatt 2001 av bransjeorganisasjonen IKT-Norge.[175] Meningen var at nemnda skulle behandle klager på brudd på disse reglene. Nemnda er imidlertid nå lagt ned og angjeldende kodekser hadde derfor primært verdi i de to årene nemnda var i funksjon.

[173] Jf. også førstvoterende i Rt 2005 s. 1677 avsnitt 70.
[174] Jf. Ot.prp. nr. 92 (1998–1999) s. 107.
[175] Se videre <http://www.nettnemda.no>.

Brorparten av reglene er blitt utformet i tiden forut internettets gjennombrudd som allmenn kommunikasjonskanal. Deres rekkevidde i forhold til spredning av opplysninger via nettet er dermed beheftet med betydelig usikkerhet. Det er dessuten svært lite rettspraksis som direkte angår nettpublisering. Ett nevneverdig unntak er kjennelsen av Høyesteretts kjæremålsutvalg i den såkalte "Teazer.tv"-saken.[176] Kjæremålsutvalget kom her enstemmig til at åndsverkloven § 45c forhindret at bilder av to tidligere deltakere i et TV-program ble lagt ut uten de avbildede personenes samtykke. Bildene var tatt under et moteshow og det aktuelle nettstedet (<Teazer.tv>) hadde fokus på sex.

De aller fleste av reglene – både lovfestede, ulovfestede og ikke-rettslige – er formulert på en såpass teknologi-nøytral måte at de vil kunne anvendes på tilfeller med nettpublisering. Enkelte regler hviler imidlertid på formuleringer og forutsetninger som vanskeliggjør (men ikke nødvendigvis umuliggjør) anvendelse i internettsammenheng. Straffeloven § 390 er hovedeksempelet i så måte. En forutsetning for anvendelse av bestemmelsen er at det skjer en "offentlig meddelelse" av visse typer personopplysninger. Siden en meddelelse er en type handling, må spørsmålet om hva som er en "offentlig meddelelse" avgjøres i lys av definisjonen av hva som er en "offentlig handling" i strl § 7 nr. 2. Meddelelsen må da anses å være offentlig dersom den er fremsatt ved "Udgivelse af trykt Skrift", "i Overvær af et større Antal Personer" eller "under saadanne Omstændigheder, at den let kunde iagttages fra et offentlig Sted og er iagttaget af nogen der eller i Nærheden værende". Spørsmålet om hva flere av disse delkriteriene betyr, må i tur avgjøres i lys av definisjoner i andre bestemmelser (jf. §§ 7 nr. 1 og 10) som igjen ikke byr på entydige løsninger i forhold til realitetene ved nettvirksomhet. Om § 390 kan anvendes i forhold til spredning av opplysninger via nettet reiser dermed vanskelige tolkningsspørsmål. Innen rettsvitenskapen er det uenighet om løsningene av spørsmålene.[177] Det er dessuten mangel på rettspraksis som er direkte relevant. De lege ferenda mener vi det foreligger gode grunner for å anse spredning via internettet som "offentlig meddelelse".[178] Sett hen til legalitetsprinsippet og Grunnloven § 96 er likevel holdbarheten av dette synspunktet tvilsomt de lege lata.

Om anvendelse av de nevnte reglene fører til sanksjoner eller ikke, avhenger av en nærmere avveining. Ikke sjelden vil dette være proporsjonalitetsvurderinger tilsvarende de som må gjennomføres i forhold til EMK artikkel 8 og 10. For eksempel er det et vilkår for anvendelse av strl § 390 at meddelelsen "krenker" privatlivets fred. Vilkåret betyr at kun meddelelser uten "påviselig aktverdig grunn" vil kunne rammes av § 390.[179] Vurderingen av om det foreligger en slik krenkelse, beror på en helhetsvurdering som innebærer en konkret avveining mellom personvernhensyn og hensynet til ytringsfrihet.[180] Tilsvarende gjelder f.eks. åndsverkloven § 45c:

> Det nærmere innhold i bestemmelsen må fastlegges ved en interessavveining der i første rekke allmennhetens informasjonsbehov veies mot den avbildedes interesse i vern mot bruk i sammenhenger som er urimelig belastende.[181]

[176] Rt. 2001 s. 1691.

[177] Sml. eksempelvis Tokvam 1995 med Mæland 1998 (særlig s. 220); Brække 1991 (særlig s. 107–111); NOU 1992:23 (særlig s. 66 og 326).

[178] Jf. også Tokvam 1995 s. 77–79; Schartum og Bygrave 2004 s. 240.

[179] Jf. Indst. O. I (1901–02) s. 51.

[180] Jf. bl.a. Mæland s. 222.

[181] Jf. Rt. 2001 s. 1691, 1694–95. Videre om bestemmelsen, se bl.a. Jordahl 1996 s. 44flg.

Med hensyn til forutberegnelighet er det problematisk at reglenes gjennomslagskraft avhenger av slike avveininger som er kompliserte og krever kunnskap om andre rettsregler. Slike avveininger er imidlertid neppe til å unngå.

Det siste punktet som det er grunn til å fremheve her er at alle de nevnte reglene i utgangspunktet kun vil få *ex post facto* virkning, dvs. at de i utgangspunktet vil komme til anvendelse kun etter at publisering finner sted. Dette er til forskjell fra personopplysningsloven som i betydelig grad er rettet mot tidligere stadier i informasjonsbehandlingssyklusen. Det er likevel klart at i den grad deres anvendelse fører til ileggelse av sanksjoner som både "svir" og blir allment kjent, vil reglene kunne få en preventiv virkning. Dessuten er det grunn til å anta at en slik virkning lettere vil kunne springe ut av yrkesetiske adferdskodekser i forhold til angjeldende bransje – forutsatt naturligvis at reglene her håndheves på årvåken vis.

## 5.6 Avsluttende betraktninger

Vi mener at den avveiningen mellom personvernhensyn og hensynet til ytringsfrihet som personopplysningsloven § 7 representerer, ligger trygt innenfor de grenser satt av EMK (og dermed SP). Det samme gjelder i forhold til personverndirektivet artikkel 9.

Vi mener dessuten at personopplysningsloven § 7 er ellers hensiktsmessig utformet. Det ville naturligvis vært ønskelig at bestemmelsen ga større veiledning om innholdet i de angitte formålskategoriene, men det er svært vanskelig å gjøre dette uten å øke bestemmelsens kompleksitet. De begrepene som brukes for å betegne slik behandling som inngår i § 7 er ord som er mye brukt i dagligtale, men som er særdeles vanskelig å få definert på en måte som både er konsis og klargjørende uten å bli sirkulær. Utdypingen av ordet "journalistiske" ved tilføyelse av "opinionsdannende" må i så måte anses å være et kunststykke, fordi sistnevnte ord også peker i riktig retning mot det sentrale momentet i avveiningen mellom personvern og ytringsfrihet.

En annen grunn til at vi ikke anbefaler videre utdyping av formålskategoriene er at en dermed beholder fleksibiliteten i bestemmelsens rekkevidde. Noe fleksibilitet er nok påkrevd siden EMK og EMDs praksis innebærer en dynamisk rettsutvikling. Bestemmelsens kjernebegreper "kunstneriske", "litterære", "journalistiske" og "opinionsdannende" er diffuse nok til at anvendelse av bestemmelsen kan justeres noe i henhold til en proporsjonalitetsvurdering slik som direktivet artikkel 9 og EMK legger opp til. En eventuell justering vil da skje gjennom tolkning av hva angjeldende formålsangivelse dekker i det konkrete tilfellet.

Med hensyn til Datatilsynets rolle er det på det rene at § 7 innebærer klare begrensninger av tilsynets kompetanse og myndighet. Som forarbeidene til personopplysningsloven påpeker, er tilsyn med medienes behandling av personopplysninger i hovedsak avgrenset til et "etterfølgende ansvar for det ferdige og publiserte produktet".[182] Vi kan ikke se at det er behov for å endre denne situasjonen. På dette punktet slutter vi oss til konklusjoner og begrunnelser i forarbeidene.[183]

Vi oppfatter det slik at Datatilsynet har vært lite villige til å teste grensene for dets kompetanse i forhold til behandling av personopplysninger i grenselandet mellom

[182] Ot.prp. nr. 92 (1998–1999) s. 107.
[183] *Ibid.* særlig avsnitt 11.6.

ytringsfrihet og personvern. Datatilsynet mener at det i dette grenselandet mangler klar nok lovhjemmel til å gi vurderinger av hva som er "opinionsdannende" virksomhet mv. i henhold til pol § 7. Som påpekt i avsnitt 5.2 ovenfor mener vi at tilsynet har tilstrekkelig hjemmel her. For å sørge for en hensiktsmessig dynamikk rundt § 7 vil det imidlertid være på plass at også departementet vurderer tilsynets kompetanse i forhold til § 7, og hvis nødvendig tydeliggjør denne kompetansen bedre. Det er svært viktig at tilsynet skal kunne vurdere om en behandling er omfattet av § 7 for å sikre at bestemmelsen ikke blir brukt til urettmessig omgåelse av loven. Dessuten er det viktig at tilsynet er villig til å klargjøre bestemmelsens grenser. Forarbeidene forutsetter jo at unntakskategoriene som er angitt i pol § 7 i noe grad vil bli definert gjennom praksis.

Når det gjelder regler som kan bidra til bekjempelse av bruk av nettet som på uakseptabel måte krenker personlig integritet mv., viser drøftelsen ovenfor at det finnes flere regler med et slikt potensial. Bestemmelsene er imidlertid plassert nokså spredt i lovverket, og det er knyttet usikkerhet til anvendelsen av enkelte av dem. Det er særlig problematisk at denne usikkerheten gjelder straffeloven § 390, fordi denne bestemmelsen vil kunne fylle et viktig behov for å verne privatliv i samband med nettbruk. Vi har dessverre ikke hatt kapasitet til å utarbeide konkrete forslag til endring av bestemmelsen, men anbefaler departementet å vurdere om bestemmelsen bør revideres for å gjøre den mer anvendelig i forhold til offentlig meddelelser om personlige eller huslige forhold på nettet. Det kunne være hensiktsmessig å frikoble bestemmelsen fra de definisjonsmessige føringer som ligger skjult i formuleringen "offentlig meddelelse" (jf. strl §§ 7 og 10) og som ikke helt samsvarer med alminnelige intuitive oppfatninger av hva offentliggjøring av opplysninger innebærer. En mer teknologi-nøytral formulering kunne vurderes innført eksempelvis etter mønster av strl § 204 første ledd bokstav a ("utgir ... eller på annen måte søker å utbre"). Vi anbefaler videre at departementet tar opp straffelovens struktur til vurdering, med henblikk på å oppnå bedre sammenheng mellom de forskjellige bestemmelsene som angår personvern (inklusive vern av omdømme). Dette vil for eksempel kunne skje ved å gruppere bestemmelser med betydning for personvern, eller ved i større grad å gjøre bruk av henvisninger.

Avslutningsvis mener vi at det mest effektive personvernfremmende tiltak på sikt for bekjempelse av "overtramp på nettet" vil være systematisk skolerings- og opplysningsarbeid for å få nettbrukere og andre til å innse betydningen av "nettvett" i vid forstand.[184] Hvis det skal satses riktig langsiktig, bør hovedstøtet settes inn i de vanlige skolene, inklusive grunnskolen. Her er det er stort behov for undervisning i de etiske (og til en viss grad rettslige) sidene ved bruken av IKT. Og det er her at Datatilsynet kan og bør spille en aktiv rolle – først og fremst med bistand i utviklingen av skolekurs i informasjonsetikk. Det er allerede utarbeidet én læringshefte om personvern myntet på ungdomsskolene,[185] men det er et klart behov for mer satsing her.

[184] Et eksempel er SAFT-prosjektet (Safety awareness facts tools) som har som siktemål å motvirke skadelig bruk av internett ved å skolere barn og foreldre slik at de kan gjøre kunnskapsrike, kritiske og trygg bruk av nettet, se <http://www.saftonline.no/>.

[185] Jf. <http://www.skolenettet.no/templates/Page.aspx?id=11812&epslanguage=NO>.

# Kapittel 6

## Vilkår for å behandle personopplysninger, personopplysnings-loven §§ 8 og 9

### 6.1 Om mandatet

I rammen gjengir vi mandatets punkt 5 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Personopplysningsloven §§ 8 og 9*

Bestemmelsen i § 8 gjennomfører EU-direktivet artikkel 7 og oppstiller generelle og uttømmende vilkår for når behandling av personopplysninger kan finne sted. Personopplysninger kan bare behandles når den registrerte har samtykket eller det er lovhjemmel for behandlingen, eller behandlingen er nødvendig av grunner som er opplistet i § 8 bokstav a til f. Vilkårene i bokstav a til f inneholder skjønnsmessige begreper og krever derved en konkret vurdering i hvert enkelt tilfelle. Dette overlater et visst skjønn til den behandlingsansvarlige. Skjønnet kan igjen overprøves av Datatilsynet. For å behandle sensitive personopplysninger oppstilles det tilleggsvilkår i § 9.

I praksis har det vist seg at personopplysninger ofte behandles med hjemmel i § 8 bokstav f. Bestemmelsen er generell og angir en avveining av den behandlingsansvarliges interesser i å gjennomføre behandlingen mot den registrertes personverninteresse i at behandlingen ikke gjennomføres. Bokstav f var i utgangspunktet ment som en sikkerhetsventil og ikke tiltenkt den store rollen den har fått i praksis.

I lys av praksis bes utrederne **vurdere om det kommer klart nok fram i loven at de to førstnevnte vilkårene i § 8, samtykke og lovregulering, skal være de primære behandlingsgrunnlag, mens bokstav a til f skal være sekundære behandlingsgrunnlag etter at samtykke er forsøkt innhentet men ikke gitt og adgangen ikke følger av lov**. Det bes vurdert om det er nødvendig eller hensiktsmessig å presisere dette i loven med en klarere prioritering eller gradering av vilkårene.

Utrederne bes også **vurdere om § 8 bokstav f er hensiktsmessig utformet** blant annet sett i sammenheng med hvilken vekt de ulike interessene skal eller bør ha i avveiningen. Det vises her til merknader til bestemmelsen om avveiningen av interessene, Ot.prp. nr. 92 (1998–1999) s. 109:

> På begge sider må både fordeler og ulemper med behandlingen tas i betraktning. Generelt må hensynet til privatlivets fred tillegges betydelig vekt i avveiningen mot kommersielle interesser. Dersom en registrert gir den behandlingsansvarlige beskjed om at han eller hun ikke vil at behandlingen skal gjennomføres eller fortsette, bør dette tillegges vesentlig vekt.

Eventuelle forslag til endringer må være i samsvar med EU-direktivet.

Selv om spørsmålene i mandatet kun er direkte knyttet til § 8, forstår vi det slik at også § 9 kan trekkes inn. Disse bestemmelsene er uansett så tett vevet sammen, at det vil være umulig å foreta et klart skille mellom dem. Vi vil imidlertid legge vekt på strukturelle forhold mellom

de to bestemmelsene, snarere enn å foreta en detaljert innholdsmessig analyse. Hoveddelen av drøftelsen vil gjelde § 8. Fordi § 8 bokstav f er ett av 6 "nødvendighetsalternativer" i denne bestemmelsen, finner vi også grunn til en viss grad å trekke inn de øvrige nødvendighetsgrunnene.

Vi gjør oppmerksom på at §§ 8 og 9 også vil bli drøftet under avsnitt 12.5.2.2. Denne drøftelsen er plassert der fordi den mest gjelder strukturelle spørsmål vedrørende forholdet til § 11 første ledd bokstav c.

## 6.2 Generelt om pol §§ 8 og 9

### 6.2.1 Oversikt over §§ 8 og 9 og forholdet til omkringliggende bestemmelser

Pol §§ 8 og 9 står i kapittel II i loven om "Alminnelige regler for behandling av opplysninger". Kapittelet har en noe uensartet innhold, men §§ 8 – 12, §§ 13 – 15 (informasjonssikkerhet og internkontroll) og §§ 16 og 17 (tidsfrister og betaling) kan sies å høre sammen i tre grupper. Paragraf 8 gjelder vilkår for å behandle personopplysninger uansett opplysningenes innhold, og § 9 gjelder vilkår for å behandle sensitive personopplysninger, jf. definisjonen i § 2 nr. 8. De vilkår som stilles opp blir ofte omtalt som *krav til rettslig grunnlag*, og begge bestemmelser opererer med grunnlagene lov, samtykke og "nødvendig grunn", se de grunner som er angitt i bestemmelsene. I tillegg opererer § 9 bokstav d med grunnlaget at det "utelukkende behandles opplysninger som den registrerte frivillig har gjort alminnelig kjent". Dette vilkåret er ikke stilt opp som alternativ etter § 8, men det er neppe grunn til å ha strengere regler her enn for sensitive personopplysninger.

For opplysninger som er klassifisert som sensitive er vilkårene i §§ 8 og 9 kumulative, se § 9 første ledd. I slike tilfeller må den behandlingsansvarlige først finne et grunnlag for å behandle opplysningene i § 8, og deretter finne et særskilt grunnlag i § 9 for å behandle sensitive personopplysninger.

Poenget med §§ 8 og 9 er at behandlingsansvarlige må forsikre seg om at de har et tilstrekkelig rettslig grunnlag for å behandle personopplysninger, *før* behandlingen tar til. Dersom det ikke foreligger et slikt grunnlag, må behandlingsansvarlig – eventuelt – ta initiativ til å skaffe seg slikt grunnlag. I så fall er det kun to rettslig grunnlag som er mulig å gjøre bruk av: For det første kan behandlingsansvarlig forsøke å innhente samtykke i samsvar med kravene til samtykke i § 2 nr. 7, eventuelt kan det bli tatt initiativ til å få vedtatt en lovhjemmel som grunnlag for behandlingen. I praksis vil imidlertid alternativet lovhjemmel primært være en mulighet for offentlige myndigheter.

Loven angir ikke noen prioritering mellom de tre typene grunnlag. Dersom det finnes lovhjemmel oppstår det ingen prioriteringsproblemer. Her er problemene primært knyttet til hva som må kreves av en hjemmel for at den skal anses å være tilstrekkelig, se avsnitt 6.3. Når lovhjemmel ikke finnes, er det kun samtykke og en av de nødvendige grunner loven regner opp som kan være aktuelle grunnlag. Etter lovteksten er det imidlertid uklart i hvilken grad behandlingsansvarlig kan velge å se bort fra samtykkealternativet og i stedet velge en passende "nødvendig grunn" som grunnlag. Siste nødvendige grunn som angis i § 8 innebærer krav til en interesseavveining, og kan derfor fremstå som et tjenlig grunnlag. Se nærmere om dette i avsnitt 6.6.

Uten et rettslig grunnlag i samsvar med §§ 8 og 9 er behandlingen av personopplysninger ulovlig. Brudd på disse bestemmelsene er imidlertid ikke gjort straffbart etter § 48. Sett i lys av lovens formålsbestemmelse, må manglende rettslig grunnlag likevel regnes som et grunnleggende og alvorlig brudd på loven.

Personopplysningsloven § 8 gjelder for alle personopplysninger, dvs. også for opplysninger der det ikke er noen konsesjonsplikt. Dette innebærer at vurderinger av det rettslige grunnlaget for behandling normalt foretas av den behandlingsansvarlige, uten Datatilsynets medvirkning. For vurderingen etter § 9 vil det ikke sjelden skje en vurdering i Datatilsynet fordi behandling av sensitive personopplysninger ofte er konsesjonspliktige etter pol § 33, jf. forskriftens kapittel 7. I punkt 8 av mandatet for dette utredningsarbeidet (se kapittel 9, nedenfor), er det stilt spørsmål ved hensiktsmessigheten ved den ressursbruken som i dag skjer i tilknytning til konsesjonsbehandlingen. En eventuell reduksjon av konsesjonsplikten, vil innebære at enda flere behandlinger enn i dag skjer på et rettslig grunnlag som ikke er vurdert av andre enn den behandlingsansvarlige, dvs. av en aktør som har klar interesse av å finne et slikt grunnlag.

Personopplysningsloven § 10 innebærer en innskrenkning i retten til å behandle personopplysninger i form av "fullstendig register over straffedommer", og innebærer et unntak fra vilkårene i § 9. Slike opplysninger kan med andre ord ikke behandles på grunnlag av samtykke, "nødvendig grunn" eller frivillig avgivelse. Derimot er det selvsagt mulig at annen lovbestemmelse må anses å gå foran forbudet i § 10, for eksempel ut i fra anvendelse av prinsippet om lex specialis. Vi kommer ikke nærmere inn på denne bestemmelsen.

Paragraf 12 gjelder fødselsnumre og andre entydige identifikasjonsmidler. Biometriske identifikasjonsteknikker kommer inn under denne bestemmelsen som både inneholder innskrenkninger i adgangen til å bruke slike opplysninger, og hjemmel for Datatilsynet til å gi pålegg om bruk av fødselsnummer mv. Fødselsnummer er ikke definert som sensitiv personopplysning, men opplysninger knyttet til biometri kan være det, jf. § 2 nr. 8 bokstav c. Uansett kan § 12 leses som en særregel om en viss kategori personopplysninger, som legger begrensinger på hva som kan behandles på grunnlag av samtykke mv. Kommentaren ovenfor knyttet til lovhjemmel er imidlertid også relevant her.

§ 11 inneholder det som blir betegnet "grunnkrav" til behandling av personopplysninger. De fleste kravene i bestemmelsen er ikke mer "grunnleggende" enn §§ 8 og 9, men § 11 bokstav a inneholder en påminnelse om at §§ 8 og 9 må etterleves, og § 11 fremstår derfor som en bestemmelse som inneholder oversikt over hvilke grunnleggende krav som stilles. Det er derfor lite logisk at bestemmelsen står *etter* §§ 8 og 9 som den viser til, noe vi kommer tilbake til i avsnitt 12.5.2.1. Paragraf 11 bokstavene b og c gjelder krav til formål for behandling av personopplysninger. Det er neppe mulig å ta stilling til rettslig grunnlag i samsvar med §§ 8 og 9, uten først å ha tatt stilling til formålet.

### 6.2.2 Forholdet til personverndirektivet

Den norske lovens §§ 8 og 9 tilsvarer langt på vei artiklene 7 og 8 i personverndirektivet. Særlig er det stor grad av samsvar mellom § 8 og artikkel 7. I artikkel 7 er ikke lovhjemmel angitt som et mulig rettslig grunnlag. Samtykke og nødvendige grunner (tilsvarende de i § 8), er regnet opp i bokstavene a – f, med samtykke som første alternativ. Det er imidlertid neppe holdepunkter for å mene at det i direktivet forutsettes at samtykke skal ha forrang fremfor

tilfeller der behandling av personopplysninger er "necessary for" et av de formålene som er angitt i bokstavene b – f.[186]

Personopplysningsloven § 9 og personverndirektivet artikkel 8 er ulikt bygget opp. Artikkel 8 er plassert i en annen del av direktivet (section III, mens artikkel 7 står i section II), og omhandler "Special categories of processing". Det som i den norske loven er tatt inn som definisjoner i § 2 nr. 7, er del av denne bestemmelsen (nr. 1) i form av en oppregning av opplysninger som det skal gjelde spesielle begrensninger for. Direktivet setter her opp forbud som utgangspunkt: "Member States shall *prohibit* the processing of personal data revealing […]" (vår kursiv). Forbudet gjelder ikke for visse medisinske formål (nr. 3). I nr. 2, bokstavene a – e, regner direktivet opp tilfeller der behandling av slike sensitive opplysninger likevel skal være tillatt; og disse omfatter samtykke (a) og nødvendige grunner (b – e). Det enkelte medlemsland kan innenfor visse rammer vedta unntak (nr. 4) i tillegg til disse. I artikkel 8 nr. 5 er det bestemmelse om opplysninger i straffedommer og i visse avgjørelser i sivile saker, og denne er grunnlaget for pol § 10 om "register over straffedommer". På lignende måte er artikkel 8 nr. 7 om nasjonale identifikasjonsnumre kommet til uttrykk i pol § 12 om bruk av fødselsnummer mv. Direktivet angir imidlertid ikke noe materielt innhold på dette punktet, men henviser spørsmålene til løsning i det enkelte land.

Det er et poeng at samkjøringen av pol §§ 8 og 9 avviker fra oppbygging av direktivet. Det er stort samsvar mellom pol § 8 og direktivets artikkel 7. I tillegg er det innholdsmessige likheter mellom pol § 9 og direktivet artikkel 8, men de rettslige sammenhengene de to bestemmelsene står i, er markert forskjellige. Dessuten har den norske loven tatt ut og plassert enkeltelementer i artikkel 9 i egne paragrafer (§§ 2 nr. 8, 10 og 12). Vi mener direktivet ikke er til hinder for å gjøre ytterligere strukturelle endringer. Dersom §§ 8 og 9 kan klargjøres ved å endre på forholdet mellom disse bestemmelsene og/eller andre omkringliggende bestemmelser, bør slike endringer i denne delen av regelstrukturen vurderes.

## 6.3 Lovhjemmel som rettslig grunnlag

Samtykke er det rettslige grunnlaget som nevnes først i § 8 og § 9. Her velger vi å behandle lovhjemmel først fordi dette grunnlaget har størst trinnhøyde. Formuleringene vedrørende lovgrunnlag er lik i begge bestemmelser: "det er fastsatt i lov at det er adgang til slik behandling". I begge tilfeller kan forskrift i medhold av lov tilfredsstille kravene til lovhjemmel. Det sentrale spørsmålet gjelder hvor eksplisitt slike hjemler skal være.

I forarbeidene uttaler departementet at: "Hjemmelskravet er relativt, slik at det kreves klarere hjemmel jo større personvernmessige konsekvenser behandlingen kan få". Etter dette kan det med andre ord ikke stilles opp noen klar grense. Dette innebærer imidlertid ikke at det i mange tilfeller klart foreligger lovhjemmel.

En stor gruppe lovgivning som klart tilfredsstiller kravet til lovhjemmel, er "registerlover", dvs. lover som fastsetter at det skal etableres registre med personopplysninger. I samband med kravet til rettslig grunnlag er hvorvidt lovgiver har vurdert om behandling av personopplysninger skal skje eller ikke. Går lovvedtaket ut på å opprette et register som skal omfatte bestemte opplysningstyper, har denne vurderingen alltid skjedd. Det samme må etter vår mening i utgangspunktet gjelde i tilfelle der lovgiver har vedtatt forvaltningsordninger

[186] Oppregningen i pol § 8 a – f, tilsvarer oppregningen i direktivet artikkel 7 b – f. Alternativ e i direktivet er i den norske loven delt inn i to alternativer (d og e).

som krever at visse personopplysninger blir behandlet, for eksempel for å treffe et enkeltvedtak eller for å yte tjenester til borgerne. Dersom lovgiver for eksempel behandler en endring i folketrygdloven eller skatteloven som gjør at involverte myndigheter må behandle personopplysninger, kan det neppe være tvil om at disse lovvedtakene også er tilstrekkelig grunnlag for å behandle opplysningene. Det betyr ikke at en med hjemmel i slik lovgivning kan behandle alle opplysninger som kan tenkes å være relevante innen saksområdet. Hjemlene dekker bare de opplysningstyper som er nevnt eller tydelig fremgår av det underliggende lovvedtaket. En slik forståelse av hjemmelskravet innebærer innfortolkning av et slags nødvendighetskriterium lignende de som gjelder for § 8 første ledd, bokstavene a – f og § 9 første ledd, bokstavene c – h.

Kravet til lovhjemmel må ses i sammenheng med nødvendighetskriteriet i § 8 første ledd bokstav e; når behandling av opplysningene er "nødvendig for å utøve offentlig myndighet". Dersom det er tale om myndighetsutøvelse, har det liten praktisk betydning dersom en gjør hjemmelskravet så strengt at "implisitte hjemler" faller utenfor; Er behandlingen nødvendig for myndighetsutøvelse, kan den likevel skje, også uten lovhjemmel. Forholdet mellom de to alternativene krever i alle fall to kommentarer.

For det første innebærer selvsagt ikke § 8 første ledd bokstav e at offentlig myndighet kan skje uten lovhjemmel dersom legalitetsprinsippet innebærer krav til slik hjemmel. Når personopplysninger skal behandles for å utøve offentlig myndighet, foreligger det altså ikke (alltid) valgfrihet mellom å påberope lovhjemmel eller å identifisere en passende "nødvendig grunn". I slike tilfeller vil det være *krav* om lovhjemmel, og legalitetsprinsippet må avgjøre styrken av hjemmelskravet.

For det andre kan ikke "nødvendig for å utøve offentlig myndighet" alltid avhjelpe behovet for rettslig grunnlag i offentlig sektor, der lovgrunnlag ikke anses å foreligge. All behandling som skjer ut i fra andre formål enn offentlig myndighetsutøvelse, faller utenfor dette alternativet i § 8 første ledd bokstav e. Dette gjelder for eksempel tilfeller vedrørende offentlig tjenesteytelse.

Det er etter vår mening behov for å gjøre tydeligere at lovhjemmel går foran samtykke og nødvendig grunn, og at prioriteringsproblemet gjelder disse to grunnlagene. Det bør dessuten klart angis tilfeller der lovhjemmel alltid kan sies å foreligge, dvs. de skjønnsmessige vurderingene knyttet til hjemmel bør gjøres så begrenset som mulig. Med en klargjøring av kravene til lovhjemmel, kan det også være grunn til å spørre om alternativet i § 8 første ledd bokstav e er hensiktsmessig, fordi slike tilfeller av myndighetsutøvelse nesten alltid vil kunne dekkes av kravene til lovhjemmel.

## 6.4 Samtykke som rettslig grunnlag

Samtykke kan sies å fremstå som et ideologisk utgangspunkt for personopplysningsloven, og flere av lovens bestemmelser tar nettopp sikte på å sikre stor grad av selvbestemmelse for den enkelte. I valget mellom samtykke fra den registrerte og "nødvendig grunn" har departementet uttrykt dette i form av en begrunnet anbefaling:

> Behandling av personopplysninger bør i størst mulig utstrekning baseres på samtykke fra den registrerte, selv om den også kan hjemles i de grunnlagene som oppstilles i bokstavene a-f. For det første vil dette styrke den registrertes muligheter til å råde over opplysninger om seg selv. For det annet vil man ved å basere behandlingen på samtykke unngå mulig tvil om de mer skjønnsmessige vilkårene i bokstavene a til f er oppfylt.

Denne uttalelsen har ikke bidratt til å klargjøre prioriteringen mellom de to typene rettslig grunnlag, og har derfor neppe demmet opp for omfattende bruk av den brede skjønnsmessige vurderingen i § 8 første ledd bokstav f, framfor innhenting av samtykke fra registrerte personer. En åpenbar grunn til at samtykke ofte ikke brukes, er at det krever innsats i form av tid og penger, mens vurderingen etter bokstav f kan gjøres formfritt, og uten strenge og klare krav til innholdsmessige elementer.

Personvernnemnda har i klagesak 2004 nr. 1 avgjort at hensynet til den enkeltes autonomi representerer et hovedprinsipp etter personverndirektivet og den norske implementeringen av direktivet, og uttaler at:

> For at man skal kunne gjøre et avvik fra hovedprinsippet, må det derfor foreligge en begrunnelse. Denne begrunnelsen kan, som nevnt ovenfor, ikke bare være en ren hensiktsmessighetsbetraktning, f eks å unngå kostnader, spare tid eller lignende – selv om slike begrunnelser selvsagt også må vurderes konkret i forhold til den enkelte sak.[187]

Vi forstår denne avgjørelsen slik at bruk av "nødvendig grunn" som rettslig grunnlag, fremfor samtykke, bare kan skje når dette er begrunnet. I begrunnelsen bør en konkret forholde seg til de personvernmessige konsekvensene av å velge den ene fremfor den andre fremgangsmåten, jf. departementets begrunnelse for hvorfor samtykke bør foretrekkes i størst mulig utstrekning (se første sitat i dette avsnittet). Det kan da særlig være grunn til aktivt å trekke inn lovens formålsbestemmelse. Argumenter vedrørende kostnader og praktiske forhold er relevante men ikke tilstrekkelige.

Personvernnemndas avgjørelse skaper noe større klarhet om forholdet mellom samtykke og "nødvendig grunn". I virkeligheten har nemnda innført et krav til bred avveining mellom hensyn. Dette er imidlertid ikke synlig for den enkelte leser av loven. En løsning kan derfor være å formulere en slik avveiningsregel som lovtekst. Uansett vil selve gjennomføringen av avveiningen være krevende. I de tilfeller der avveiningen av om en "nødvendig grunn" kan benyttes som grunnlag framfor samtykke, skjer ved at nødvendighetsalternativet i § 8 første ledd bokstav f) blir brukt, vil de to avveiningene lett smelte sammen til én: Dersom konklusjonen er at samtykke ikke er påkrevet, mener vi med andre ord sannsynligheten er stor for at behandlingsansvarlige anser § 8 første ledd bokstav f for å gi tilstrekkelig rettslig grunnlag for behandling. Etter vår mening ville den beste løsningen derfor være å gjøre avveiningen mellom samtykke og nødvendighet mindre skjønnsmessig.

## 6.5 Nødvendig grunn som rettslig grunnlag

Her vil vi ikke gå inn på hvert enkelt alternativ i § 8 første ledd bokstav a – f og § 9 første ledd bokstav c – h, men nøye oss med noen generelle kommentarer, i tillegg til en nærmere analyse av § 8 første ledd bokstav f. Først skal det understrekes at det ikke er vanntette skott mellom de ulike typene rettslig grunnlag. Blant grunnlagene i § 8 første ledd bokstavene a – f ("nødvendig for å …"), er det i alle fall to alternativer som kan sies å ha elementer som er sterkt beslektet med samtykke (bokstav a vedrørende avtaler, og bokstav c vedrørende "vitale interesser", jf. presumert samtykke). Slike samtykkeelementer kan ha klar betydning for vurderingen om behandlingsansvarlige kan unnlate å innhente samtykke etter § 8 første ledd og § 9 første ledd bokstav a, jf. diskusjonen i forrige avsnitt.

[187] Samme standpunkt er også lagt til grunn i senere praksis av nemnda, jf. særlig sakene 2004 nr. 4 og 2005 nr. 8.

For det andre er det en viktig erfaring at formuleringene i nødvendighetsalternativene kan ha lett for å bli oppfattet i samsvar med dagligspråket, dvs. uten at de særskilte hensyn som ligger bak hver bestemmelse blir kommunisert til den som leser lovteksten. "[N]ødvendig for å utføre en oppgave av allmenn interesse" (§ 8 bokstav d), kan for eksempel forstås som en generell henvisning til samfunnsmessig nytte mv, mens det i virkeligheten er "arkivering eller i forbindelse med statistisk, historisk eller vitenskapelig virksomhet"[188] departementet hadde i tankene. Etter vår mening er det derfor et behov for å tydeliggjøre de særlige forhold som skal ha betydning for anvendelsen av nødvendighetsalternativene.

Alternativet i § 8 første ledd bokstav f avviker fra de andre alternativer ved at det ikke er knyttet opp til noe bestemt formål, og er derfor spesielt anvendelig. Det finnes ikke noe tilsvarende alternativ nødvendig grunn i § 9 for å behandle sensitive personopplysninger. Bestemmelsen lyder:

> behandling er nødvendig for
>
> […]
>
> f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Bestemmelsen er langt på vei en oversettelse av personverndirektivet artikkel 7 bokstav f. Norge kan imidlertid også implementere dette elementet på andre måter. Hovedpoenget med direktivets bestemmelse er å unngå at fullt ut legitim behandling av personopplysninger blir ulovlig fordi den ikke er dekket av ett av de foregående spesifikke alternativene.

Bestemmelsen gir anvisning på en enkel interesseavveining mellom – på den ene side – interesser knyttet til behandlingsansvarlig og eventuelle aktører som skal motta opplysningene, og – på den annen side – den registrertes personvern. Det er ikke krav om annet enn simpel interesseovervekt, og det stilles ikke noen formelle krav eller krav til bestemte fremgangsmåter mv. I merknadene til bestemmelsen gjør departementet oppmerksom på at "[d]et vil kunne være vanskelig for den behandlingsansvarlige i det enkelte tilfelle selv å avgjøre om egeninteressen i å behandle opplysningene veier tyngre enn hensynet til den registrertes personvern". Det vises så til Datatilsynets spesielle veiledningsoppgave slik den kommer til uttrykk i pol § 42 nr. 6, jf. fvl § 11. Så vidt vi kan se, har ikke Datatilsynet utferdiget noen generell veiledning om dette spørsmålet. Personvernnemnda hadde i begynnelsen av jaunar 2006 drøftet anvendelsen av § 8 første ledd bokstav f i fire saker.[189] Etter det vi kan se, inneholder imidlertid ingen av avgjørelsene uttalelser av mer generell interesse.

Etter vårt syn er det med utgangspunkt i direktivet artikkel 7 vanskelig å tenke seg en annen løsning enn at konkrete nødvendighetsgrunner knyttet til formål, kombineres av en bestemmelse som kan gi rettslig grunnlag til å behandle personopplysninger ut i fra en bred interesseavveining. Bestemmelsen slik den nå står, er imidlertid paradoksal: Den er basert på eksistensen av en (sannsynlig) interessekonflikt mellom behandlingsansvarlig (m.fl.) og den registrerte. Konflikten går ut på om det skal etableres en ny rett for den behandlingsansvarlige overfor enkeltpersoner. Lovgiver har gitt den parten som ønsker å

[188] Se Ot.prp. nr. 92 (1998–99) s. 109.

[189] Sakene 2004 nr. 3, 2004 nr. 7, 2004 nr. 9 og 2005 nr. 10.

oppnå en slik ny rett kompetanse til å avgjøre saken. Fordi beslutningen ikke er lagt til et forvaltningsorgan, er den behandlingsansvarlige likevel en habil beslutningstaker.[190]

På den annen side, er det lite praktisk å overlate avgjørelsen i slike saker til Datatilsynet eller annen myndighet. Dessuten har Datatilsynet en generell inngrepskompetanse i § 46, og kan derfor gripe inn mot ulovlig anvendelse av § 8 første ledd bokstav f. Fordi behandlingsansvarlige ikke treffer "enkeltvedtak", gjelder ingen klagerett for de registrerte,[191] men det er heller ingen innskrenkninger i Datatilsynets adgang til å omgjøre den behandlingsansvarliges bestemmelse.[192]

Etter vår mening er § 8 første ledd bokstav f en alt for åpen og løs bestemmelse. Uten nærmere begrensninger kan bestemmelsen tenkes å begrunne interesseovervekt for den behandlingsansvarlige i nesten ethvert tilfelle. Etter vår mening er det derfor behov for å stramme inn bestemmelsen. Innstramning kan tenkes ved hjelp av flere teknikker:

- Kreve klarere interesseovervekt enn i dagens bestemmelse;
- Kreve at visse fremgangsmåter skal følges;
- Kreve at avgjørelsen skal fremkomme på bestemte måter;
- Knytte rettigheter for de registrerte til den behandlingsansvarliges avgjørelse av rettslig grunnlag.

Etter vår mening kan alle nevnte regulatoriske elementer tenkes å ha god effekt, eventuelt i kombinasjon. Vårt hovedperspektiv er at det kan være fruktbart å se på anvendelsen av § 8 første ledd bokstav f som utøvelse av en beslutningskompetanse, og knytte rettssikkerhetsgarantier til utøvelsen av denne kompetansen. I avsnitt 6.8 (nedenfor) fremmer vi forslag om omfattende endringer av nåværende §§ 8 og 9. Forslaget inngår i vårt radikale lovutkast.

## 6.6 Nærmere om prioriteringen mellom de rettslige grunnlagene

Det er etter vår mening viktig å klargjøre forholdet mellom samtykke og "nødvendighetsgrunnene", og i hvilken utstrekning det er mulig å behandle personopplysninger uten lovhjemmel eller samtykke. Etter vår mening er det grunn til å skjelne mellom to situasjoner:

1. Tilfeller der samtykke ikke er forsøkt innhentet, og behandlingsansvarlig ønsker å anvende ett av nødvendighetsalternativene direkte; og
2. Tilfeller der samtykke er forsøkt innhentet men nektet av så mange personer at behandlingsansvarlig ikke kan basere seg på dette grunnlaget.

I sist nevnte tilfellet, er det etablert en slik konflikt som gjør det problematisk å akseptere at behandlingsansvarlig skal kunne "overkjøre" registrerte personer som har nektet samtykke, ved å påberope seg nødvendig grunn, for eksempel § 8 første ledd bokstav f.

[190] Jf. fvl § 6 første ledd bokstav a.
[191] Jf. fvl § 28.
[192] Jf. fvl §§ 35.

Det er også grunn til å gi klarere begrensinger av muligheten til å unnlate innhenting av samtykke. Dette kan både oppnås ved å stille opp konkrete vilkår i loven, og ved å stille krav til å følge bestemte fremgangsmåter mv. I avsnitt 6.8 fremmer vi forslag til endret regulering.

Diskusjonen vedrørende samtykke kontra andre rettslige grunnlag baserer seg på en enten – eller oppfatning som forutsetter at det enten er behandlingsansvarlig eller de registrerte som skal ta stilling til spørsmålet om rettslig grunnlag uten innblanding fra andre. Vi vil gjøre oppmerksom på muligheter for mellomløsninger, dvs. løsninger som ikke er basert på én aktørs enekompetanse. Blant mulighetene er krav til varsel og informasjon til registrerte personer, og rett for registrerte personer til å reservere seg mot behandling av opplysninger som skjer på grunnlag av rettslige grunnlag tilsvarende § 8 første ledd bokstav f.

## 6.7 Vurderinger av forholdet mellom §§ 8, 9 og 11 første ledd bokstav a

Som tidligere nevnt i avsnitt 6.2.1 virker det lite logisk at bestemmelsen i § 11 første ledd bokstav a som viser til §§ 8 og 9, er plassert etter disse bestemmelsene. Samtidig mener vi det er en god idé å ha en slik "regibestemmelse". Særlig er det et behov for en bestemmelse som klart formidler den prosedyren som må følges for at de alminnelige bestemmelsene i lovens kapittel II, kan anses å være etterlevet. Det kan herunder også være grunn til å gi en veiledende bestemmelse som dekker alle viktige punkter i kapittel II, og som klarere plasserer §§ 10 og 12 i sammenheng med de øvrige bestemmelsene.

I dag skal rettslig grunnlag først vurderes i forhold til de alminnelige reglene i § 8, og deretter i forhold til reglene for sensitive opplysninger i § 9. Det er etter vår mening grunn til å gjennomføre større grad av integrasjon mellom disse bestemmelsene, eventuelt ved å slå sammen bestemmelsene. Spørsmålet om forholdet mellom §§ 8 og 9, avhenger imidlertid til en viss grad av hvilken løsning som vil bli valgt for den fremtidige konsesjonsplikten. I dag gjelder konsesjonsplikt for behandling av sensitive personopplysninger. Skulle denne konsesjonsplikten bli redusert eller falle helt bort, vil spørsmålet om sensitivitet slik det er definert i § 2 nr. 8, primært få konsekvenser i forhold til rettslig grunnlag og overføring av personopplysninger til utlandet. Redusert beskyttelse i tilknytning til konsesjonsordningen, kan begrunne økt beskyttelse i tilknytning til andre deler av loven, for eksempel i relasjon til bestemmelsene om rettslig grunnlag i § 9.

## 6.8 Endringsforslag

På bakgrunn av drøftelsene i dette kapittelet, har vi formulert en alternativ regulering av spørsmålet om rettslig grunnlag for behandling av personopplysninger. Forslaget bryter med tidligere tilnærminger ved at vi ikke skjelner mellom ikke-sensitive og sensitive opplysningstyper. Vår forutsetning er at forslaget ikke skal gi vesentlige endringer i kravene til rettslig grunnlag i andre tilfeller enn de som i dag vurderes ut i fra § 8 første ledd bokstav f. Blant annet gjelder dette innskrenking av adgangen til å påberope seg slike skjønnsmessige rettslige grunnlag som basis for å behandle opplysninger om små barn, se forslaget til § 8c første ledd bokstav c. Forslaget har grunnlag i drøftelser som er plassert i kapittel 11, og er for helhetens skyld tatt med her. Bestemmelsene har henvisningsstruktur som er tilpasset vårt samlede radikale lovutkast.

**§ 8 Generelt om krav til rettslig grunnlag for å behandle personopplysninger**

For å være lovlig, må behandling av personopplysninger alltid ha et rettslig grunnlag i medhold av bestemmelsene i §§ 8 – 8d i denne loven. Det rettslige grunnlaget skal vurderes og fastsettes ut i fra ett eller flere formål, se § 9.

**§ 8a Primære rettslige grunnlag for behandling av personopplysninger**

Personopplysninger (jf. § 2 nr. 1) kan behandles dersom:

a) det klart er fastsatt i lov eller med hjemmel i lov at det er adgang til slik behandling, eller

b) etterlevelse av lovgivning gjør det nødvendig at opplysningene blir behandlet, eller

c) behandlingen bare gjelder opplysninger som de registrerte personene selv frivillig har gjort alminnelig kjent, eller

d) den registrerte har gitt sitt samtykke til behandlingen i samsvar med kravene i § 6 annet ledd, og samtykket ikke er trukket tilbake.

**§ 8b Sekundære rettslige grunnlag for behandling av personopplysninger**

Dersom vilkårene i § 8a ikke kan oppfylles, eller vilkåret i § 8a bokstav d er umulig eller uforholdsmessig vanskelig eller ressurskrevende å legge til grunn for behandlingen, kan den behandlingsansvarlige likevel behandle de opplysninger som er nødvendig for:

a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, eller

b) å vareta den registrertes vitale interesser og den registrerte ikke er i stand til å samtykke, eller

c) å utføre forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling, eller for forvaltning av helsetjenester, når opplysningene behandles av helsepersonell med lovbestemt taushetsplikt, eller

d) at den behandlingsansvarlige skal kunne fastsette, gjøre gjeldende eller forsvare et gyldig rettskrav eller oppfylle en rettslig forpliktelse, eller

e) at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter, eller

f) å fremme kulturelle, historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for de registrerte.

**§ 8c Behandling av personopplysninger på grunnlag av skjønnsmessige avveininger**

Dersom et av vilkårene i §§ 8a og 8b ikke kan oppfylles, kan den behandlingsansvarlige beslutte å igangsette behandling av personopplysninger som er nødvendig for å ivareta egne eller medkontrahenters berettigede interesser. Slik beslutning kan bare treffes dersom:

a) hensynet til personvern ikke overstiger de hensyn som taler for at behandling av personopplysninger skal skje, og

b) det ikke inngår noen sensitiv opplysningstype i den planlagte behandlingen, og

c) det ikke i overveiende grad inngår personopplysninger om barn under 12 år, og

d) behandlingsansvarlig har gjort en systematisk kartlegging av mulige ulemper for den enkeltes personvern.

Forbudet mot å behandle sensitive personopplysninger (bokstav b) gjelder ikke for ideelle organisasjoners behandling av opplysninger om medlemmer og andre personer som frivillig er i regelmessig kontakt med organisasjonen på grunn av organisasjonens ideelle formål. Adgangen til å behandle sensitive personopplysninger gjelder bare opplysninger som blir samlet inn direkte fra de registrerte. Disse opplysningene kan ikke utleveres til andre uten samtykke fra den registrerte, jf. § 6 annet ledd.

**§ 8d Datatilsynets adgang til å tillate behandling av personopplysninger som mangler rettslig grunnlag etter §§ 8a – 8c**

Dersom viktige samfunnsinteresser tilsier det, kan Datatilsynet treffe enkeltvedtak om at personopplysninger kan behandles også i andre tilfeller enn som nevnt i §§ 8a – 8c. I vedtaket skal det fastsettes hva som skal anses å være tilfredsstillende krav til opplysningskvalitet (jf. § 9a) og sikkerhetstiltak (jf. § 13).

# Kapittel 7

# Elektroniske spor

## 7.1 Om mandatet

I rammen gjengir vi mandatets punkt 6 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Særlig om elektroniske spor*

Lagring og bruk av personopplysninger som den enkelte legger igjen ("elektroniske spor") reiser særlige spørsmål i forhold til personvernet. Ikke minst gjelder dette muligheten for at slike opplysninger senere kan bli brukt som ledd i en generell kartlegging av og kontroll med kortinnehaverens handlinger og disposisjoner. Justisdepartementet og Datatilsynet har gitt Norsk Regnesentral i oppgave å kartlegge ulike typer elektroniske spor og hva disse blir brukt til.

Teknologirådets prosjekt IKT og personvern har avgitt rapport 1 – 2005 *Elektroniske spor og personvern* hvor det viser hvordan dagens og morgendagens teknologi endrer betingelsene for personvernet. Rapporten beskriver også annen utvikling i samfunnet som er viktig for personvernet. Norsk Regnesentral har på oppdrag av Datatilsynet og Justisdepartementet utarbeidet en tilsvarende rapport som supplerer rapporten fra Teknologirådet.

Departementet ber utrederne **vurdere Teknologirådets og Regnesentralens rapporter, og ta stilling til om reglene i personopplysningsloven gir den enkelte et tilstrekkelig vern mot uønsket behandling (innsamling, lagring, bruk) av elektroniske spor**.

Vi har valgt å forstå dette punktet i mandatet slik at de to rapportene vedrørende elektroniske spor skal utgjøre en viktig bakgrunn for dette utredningsarbeidet, og at spørsmål knyttet til elektroniske spor skal gis spesiell oppmerksomhet ved evalueringen av loven. Vi finner imidlertid ingen grunn til å gå systematisk og konkret gjennom de to rapportene. Oppgaven med å evaluere personopplysningsloven krever dessuten at vi forholder oss konkret til lovens systematikk mv. enn det de to rapportene har funnet det nødvendig å gjøre. Dette innebærer en forholdsvis selvstendig og lite refererende bruk av rapportene. Flere av de muligheter for lovtiltak som vi i de følgende avsnitt vil peke på, er særlig beslektet med konklusjoner og anbefalinger i Teknologirådets rapport. De teknologisk baserte kategoriseringene og beskrivelsene i NRs rapport, er i mindre grad hensiktsmessige som direkte grunnlag for diskusjon av lovmessige tiltak. Rapporten er imidlertid viktig fordi den inneholder teknologiske beskrivelser som motiverer en alvorlig diskusjon av spørsmål knyttet til elektroniske spor.

## 7.2 Generelt om elektroniske spor

I Teknologirådets rapport er elektroniske spor omtalt på følgende kortfattet og omtrentlig vis:[193]

> Nye informasjons-og kommunikasjonsteknologier (IKT) introduseres i høyt tempo. Mange av disse lager elektroniske spor som kan føres tilbake til oss som brukere og som således kan utnyttes til å overvåke vår atferd…

Heller ikke Norsk Regnesentral definerer "elektroniske spor" men angir innholdet i begrepet ved å beskrive informasjonsbehandling som kan klassifiseres som behandling av elektroniske spor ("sporing"). Vi kan langt på vei slutte oss til de forutsetninger og beskrivelser som finnes i begge rapporter, og som innebærer en beskrivelse – om enn ikke en definisjon – av elektroniske spor.

Etter vår mening tyder den manglende definisjonen av "elektroniske spor" på at denne betegnelsen trolig omfatter så mange, omfattende og varierte fenomener at det er problematisk å benytte én felles betegnelse. Vi har derfor lagt vekt på å "dekomponere" den bekymring vi mener er inkorporert i begrepet "elektroniske spor", og ønsker ikke å gjøre forsøk på å introdusere én altomfattende definisjon. Snarere enn å gi et autorativ beskrivelse av "elektroniske spor", ønsker vi å formidle noen viktige og typiske elementer som kan sies å passe inn under dette uttrykket.

Det er også grunn til å peke på at betegnelsen "elektroniske spor" er en metafor og et populær-retorisk, mer enn et systematisk begrep. Elektroniske spor kan vekke riktige assosiasjoner og følelser, men er vanskelig å benytte direkte i rettslig regulering. Etter vår mening er det viktig å alminneliggjøre spor-problematikken, og vise berøringspunktene mellom disse spørsmålene og den nåværende personopplysningslovgivningen. For å kunne gjøre dette, er det nødvendig å trekke frem enkelte aspekter som kan sies å være integrert i spørsmålene knyttet til elektroniske spor. I de følgende avsnitt vil vi trekke frem i alt seks aspekter som vi mener er viktige/typiske for elektroniske spor, og som kan aktualisere lovgivningsmessige tiltak innenfor rammene av personopplysningsloven og/eller relevant særlovgivning.

## 7.3 Identifikasjons- og autentiserings-aspektet

For det første er det grunn til å understreke – det selvfølgelige – at "elektroniske spor" kun kommer opp som et problem dersom det er mulig å identifisere en eller flere personer som kan knyttes til sporene. Dette er i og for seg bare en understrekning at "sporene" er en betegnelse på, og forutsetter eksistensen av, personopplysninger, se § 2 nr. 1. Dette innebærer også at jo svakere og/eller dårlig tilgjengelig forbindelsen mellom sporene og de personer som har avsatt sporene er, desto mindre alvorlige kan spørsmålene knyttet til "elektroniske spor" anses å være. Er opplysningene anonyme, foreligger det ikke "elektroniske spor" i personvernrettslig forstand, og er opplysningene kun knyttet til pseudonymer som er godt beskyttet, er de personvernmessige implikasjonene klart mindre alvorlige enn med åpen identitet og full autentisering.

[193] Jf. Teknologirådet 2005 s. 15.

Med dette som utgangspunkt, er det grunn til å anta at situasjonen vedrørende "elektroniske spor" kan endres ved å endre bestemmelser knyttet til krav om identifisering og autentifisering. Vi viser her særlig til § 2 nr. 1 ("personopplysning") og § 12 om entydige identifikasjonsmidler.

For det første kan det være grunn til å oppmuntre behandlingsansvarlige til å unngå å behandle personopplysninger i større grad enn nødvendig. Dette gjelder både valg av teknologier som over hodet ikke gjør bruk av slike opplysninger, og opplegg for å behandle personopplysninger, som innebærer at opplysningene raskt kan anonymiseres eller pseudonymiseres. En åpenbar mulighet er å gi lettelser for behandling som ikke gjelder direkte identifiserbare personopplysninger, for eksempel ved at deler av loven/enkeltbestemmelser ikke gjelder slik behandling.

For det andre kan det være grunn til å legge begrensninger eller stille krav til bruk av midler for entydig autentisering av personer. Det kan for eksempel ha virkning å innføre begrensninger i adgangen til bruk av skjult eller ufravikelig (obligatorisk) innsamling av personopplysninger når denne skjer ved hjelp av hjelpemidler som virker automatisk. Bak de særlige reglene om fjernsynsovervåking (pol kap. VII) ligger for eksempel vektlegging av at slik overvåking er automatisk eller fjernstyrt, se § 36. Dette gir i sin tur begrunnelse for å stille opp særskilte begrensninger i adgangen til å fjernsynsovervåke bestemte områder, se de særlige grunnkravene i § 38.

## 7.4 Bruk av personopplysninger for kontrollformål

En annen grunn til å ta spor-metaforen på alvor, er at personopplysninger kan brukes til å ettergå enkeltpersoner, dvs. i ettertid finne ut noe om deres bevegelser, disposisjoner, tilstander osv. Elektroniske spor kan derfor i stor grad sies å gjelde en viss type formål med behandling av personopplysninger, dvs. *kontrollformålet* står sentralt. Selv om etterkontroll med handlinger, bevegelser mv. også kan være primærformålet med å behandle personopplysninger, kommer spørsmålene vedrørende slike spor på spissen når sporing og kontroll ikke har vært blant de formål som er angitt ved oppstart av behandlingen, men er et sekundærformål som kan bli utløst av mistanker om uønsket adferd, straffbare forhold osv. Dette gjelder ikke bare spørsmål om politiets tilgang til opplysninger, men også for eksempel arbeidsgiveres mulighet til bruk for sporing og kontroll som sekundærformål: For eksempel i forbindelse med bruk av opplysninger fra internett-logger mv. i tilknytning til mistanke om brudd på arbeidsgivers IKT-reglement eller lignende.

Det er grunn til å tro at endringer i den rettslige reguleringen vedrørende formål med behandling av personopplysninger (jf. § 11 første ledd bokstavene b og c), kan brukes for å få bedre grep om spor-problematikken. Særlig er det grunn til å se nærmere på forholdet mellom kravet til formålsangivelse og kravet til rettslig grunnlag for behandling av personopplysninger i §§ 8 og 9. I dag står den enkelte fritt mht. hvorledes formål skal angis. Det vil for eksempel være mulig å innføre krav om at kontrollformål skal angis direkte for at kontrollen skal være lovlig, og det vil være mulig å knytte særskilte prosessuelle og/eller materielle regler til slike formål. En slik lovendring vil tydeliggjøre og kan tenkes å redusere bruk av personopplysninger for å kontrollere den enkelte. Når det gjelder politiets bruk av elektroniske spor, er det på tilsvarende måte viktig å tydeliggjøre betydningen av legalitetsprinsippet og stille krav til klare hjemler som angir og avgrenser retten til å skaffe til veie og sammenstille personopplysninger.

## 7.5 Graden av selvbestemmelsesrett ved innsamling og bruk av personopplysninger

For det tredje er det grunn til å legge vekt på spor-metaforens fortelling om at sporene representerer noe ufrivillig, dvs. at folk uunngåelig setter igjen elektroniske spor på lignende måte som en person som setter foten på mykt underlag. Slik sett handler ønsket om å begrense innsamling og bruk av elektroniske spor om å beskytte personopplysninger som alle må avgi for å leve normale liv med omfattende IKT-basert informasjonsbehandling. Sagt på en annen måte kan det sies å eksistere et ønske om å være fullstendig deltaker i informasjonssamfunnet og gjøre bruk av elektroniske tjenester i stort monn, uten derfor å komme i en situasjon der tilknyttede personopplysninger blir brukt på måter som den enkelte ikke ønsker.

Dette frivillighets-aspektet er nært knyttet til spørsmålet om den enkeltes autonomi, og mer generelt om rettslig grunnlag for å behandle personopplysninger. I dag realiseres den enkeltes selvbestemmelsesrett ved at det ofte vil være nødvendig å innhente samtykke til å behandle opplysninger. Selvbestemmelsesretten blir imidlertid ofte satt til side fordi (i) det eksisterer lovhjemmel eller "nødvendig grunn" som overstyrer den enkeltes valg, og (ii) fordi det kan være lite realitet i at samtykke er frivillig. I flere og flere situasjoner forutsettes det bruk av IKT-baserte tjenester dersom en skal leve det som oppfattes og forventes som et normalt liv. Betalingstjenester, adgangskontrollsystemer og bompengesystemer betegner enkelte slike områder der muligheten til å nekte samtykke kun foreligger som en teoretisk mulighet. Slik "strukturell tvang" kan komme til å minske området for selvbestemmelse og samtykke, og tilsvarende øke området for "nødvendig grunn", jf. særlig § 8 første ledd bokstavene a (avtaler mv.) og f (vid interesseavveining).

Ut i fra nevnte betraktninger kan det være aktuelt å se nærmere på lovens krav til rettslig grunnlag, for eksempel vurdere den vide adgangen til å bruke "nødvendig grunn" som rettslig grunnlag for å behandle "elektroniske spor". En mulig tilnærming kan være at dersom et reelt samtykke er umulig å innhente pga. strukturell tvang, bør spørsmålet i stedet lovreguleres og ikke overgis vurderinger vedrørende "nødvendig grunn". En del av slik lovregulering kan også være vurdering av behov for ytterligere personvern- og rettssikkerhetsgarantier knyttet nærmere bruk av slike opplysninger.

## 7.6 Sammenstilling av personopplysninger

Det fjerde aspektet gjelder de kilder som anvendes for å finne frem til elektroniske spor. I utgangspunktet kan ikke bruk av én enkel kilde ekskluderes fra spor-problematikken. Det typiske for truende bruk av elektroniske spor er imidlertid at det blir anvendt og kombinert spor fra ulike kilder, dvs. at det skjer en *sammenstilling* av personopplysninger. Dette indikerer for det første at det primært er opplysninger som hentes fra maskinlesbare kilder som er av interesse.

Mange "spor-opplysninger" er personopplysninger som en ikke tenker over at en legger igjen fordi avgivelsen er triviell og integrert i en rekke dagligdagse handlinger, jf. forrige punkt. Fordi opplysningene er preget av trivielle og hyppige innsamlingssituasjoner, kan de fremstå som fordekte og vanskelige å kontrollere, og derfor mer truende enn opplysninger som en sjelden gang avgir med full informasjon og full bevissthet om avgivelsen.

Dette fjerde punktet aktualiserer særlig spørsmålet om rettslig regulering av adgangen til å sammenstille personopplysninger. I dag finnes ingen særskilt regulering av kopling/sammenstilling av personopplysninger. Etter personregisterlovens bestemmelser var det frem til 1. januar 2001 begrensninger i denne adgangen.

Det kan dessuten være grunn til å rette søkelyset mot forhold/mekanismer som kan åpenbare at personopplysninger fra dagliglivets mange trivielle situasjoner blir sammenstilt, jf. informasjonsplikten ved bruk av personprofiler (jf. også neste punkt) samt bruk av personvernøkende teknologi.

## 7.7 Elektroniske spor og personprofiler

Det femte aspektet gjelder spørsmålet om hvilke slutninger som typisk kan bli trukket på grunnlag av "elektroniske spor". Vi mener det er et karakteristisk trekk at slike spor ikke bare oppfattes som en trussel mot personvernet på grunn av det informasjonsinnehold hvert enkelt spor har direkte. Minst like viktig er den informasjonen som utledes ut i fra mange spor. Således er det for eksempel ikke bare den enkelte betalingstransaksjon, men forbruksmønstre som er viktigst i tilknytning til bruk av betalings- og kredittkort mv., og reisevaner/-mønstre snarere enn enkeltreiser i tilknytning til lokasjonsbaserte tjenester.

Også dette aspektet kan gi grunn til å se nærmere på reglene for lagring av personopplysninger, særlig spørsmål om tidspunkt for sletting, eventuelt blokkering og anonymisering. Desto kortere "hukommelse" informasjonssystemene har, desto mer begrenset vil muligheten for å sammenholde opplysninger være. Det er også grunn til å vurdere om bestemmelsen i § 21 om personprofiler er tilstrekkelig vidtfavnende og hensiktsmessig formulert.

## 7.8 Elektroniske spor som "ugjendrivelige bevis"

Det siste punktet gjelder aspekter som er knyttet til tid og hukommelse. I flere spor-situasjoner er sporene personopplysninger om den enkelte ikke selv har tilgang til, eller kun har tilgang til i det omfang og på de måter som den behandlingsansvarlige fastsetter/tilbyr. Banken fastsetter for eksempel hvilke transaksjonsopplysninger som skal være tilgjengelige fra bankens nettside, hvor lenge opplysningene skal være tilgjengelige osv. Å bli konfrontert med elektroniske spor, kan derfor innebære konfrontasjon med saksforhold som den enkelte har liten kunnskap om, og har liten beredskap/mulighet til å forholde seg til. Den behandlingsansvarlige som "motpart", kan på den annen side nettopp ha bestrebet seg på å dokumentere forhold knyttet til den registrerte, og vil således ha en spesialisert og pålitelig "hukommelse" om disse utvalgte elementene. Den behandlingsansvarlige kan i slike tilfeller sies å ha en slik grad av dokumentasjon og "regi" at den enkelte uforberedte registrerte person står hjelpeløse.

Dersom en ønsker å innføre lovgivning som kan ha effekt på problemer knyttet til elektroniske spor, kan det være grunn til å ta utgangspunkt i misforholdet mellom behandlingsansvarliges og de registrertes situasjoner:

- På den ene side behandlingsansvarlige med "full regi" vedrørende behandlingen av spor, herunder utvalget av hva som skal dokumenteres for eventuell fremtidig bruk;

- På den andre side de registrerte med liten kunnskap om sporene og normalt med små muligheter for å skaffe til veie dokumentasjon mv. som kan imøtegå sporene.

Dette peker i retning av behov for bestemmelser som kan gi en reell kontradiksjon *før* slike opplysninger legges frem, for eksempel som bevis for regelbrudd.[194] Misforholdet mellom behandlingsansvarliges og registrertes mulighet til å forholde seg til innholdet i logger mv., kan et stykke på vei repareres ved hjelp av bestemmelser om varsling av den registrerte om ufordelaktig innhold i logger. Det bør også være aktuelt å gi registrerte tilgang til egen logginformasjon, dvs. uten forutgående innsynsbegjæring (jf. tanken bak "Min Side", nettbankløsninger mv. som gir den enkelte direkte tilgang til egne opplysninger, herunder vedrørende transaksjoner). Slike ordninger kan særlig være aktuelt når behandlingsansvarlig og registrerte personer inngår i faste relasjoner, for eksempel i et arbeidsforhold, i en utdanningssituasjon eller i et fast kundeforhold. Det kan herunder tenkes regler som innebærer begrensinger i adgangen til å legge vekt på opplysninger som i dominerende grad er basert på elektroniske spor.

## 7.9 Lovregulering av elektroniske spor?

Som nevnt innledningsvis i dette kapittelet, representerer uttrykket "elektroniske spor" et litterært virkemiddel som gir mange riktige assosiasjoner, men som neppe er egnet som grunnlag for en nærmere lovregulering. Vi tror derfor ikke det er mulig å lovregulere elektroniske spor direkte. Etter vår mening kan imidlertid flere av de aspekter som ofte karakteriserer elektroniske spor, danne et fruktbart utgangspunkt for rettslige reguleringer som er relevante for dette problemområdet. Vi viser her til gjennomgangen i avsnittene 7.3 til 7.8. Flere uheldige sider ved elektroniske spor, kan med andre ord dempes ved hjelp av flere mindre lovgivningsmessige grep, jf. skissemessige angivelser i de foregående avsnittene.

Dersom en skal gi anvisning på hvor slike "spor-relevante" lovendringer kan plasseres, vil vi særlig nevne kravene til formålsangivelse (jf. § 11 første ledd bokstavene b og c), rettslig grunnlag (jf. §§ 8 og 9), bestemmelser om innsyn (jf. § 18) og bestemmelser om varsling ved bruk av personprofiler (jf. § 21). Det er imidlertid ikke sikkert at all rettslig regulering som er relevant for elektronisk sporing mv. skal plasseres i personopplysningsloven. I noen situasjoner er bruk av elektroniske spor særlig aktuelt og kontroversielt. Dette gjelder for eksempel i forholdet til politimyndigheter og arbeidsgivere. Det er derfor mulig at straffeprosessloven og arbeidsmiljøloven er kandidater for en mer eksplisitt og konkret regulering av spørsmål vedrørende det som ofte betegnes elektroniske spor.

I denne utredningen avgrenser vi oss til å foreslå endringer i personopplysningsloven. Vi har i denne sammenheng festet oss ved to mulige lovendringer som lett lar seg innpasse i den eksisterende loven. Dette gjelder nye bestemmelser i tilslutning til någjeldende bestemmelser i §§ 11 (grunnkrav) og 19 (informasjon til registrerte personer). Når det gjelder § 21 om personprofiler, mener vi at denne i utgangspunktet kan ha en god dempende effekt på spørsmål vedrørende elektroniske spor. Vi har imidlertid ikke sett eksempler på at bestemmelsen i særlig grad er brukt. I stedet for å foreslå endringer/suppleringer av denne bestemmelsen, kan det derfor være grunn til å vurdere om Datatilsynet gjennom sin tilsynspraksis kan bidra til at bestemmelsen får større praktisk betydning enn i dag. Dette kan

[194] Vi anser det imidlertid som uaktuelt å fravike prinsippet om fri bevisvurdering ved å fastsette nærmere regler om bevisfremleggelse.

bl.a. skje gjennom informasjons- og kontrolltiltak overfor bransjer og forvaltningsmyndigheter der en antar at spor-problematikken er spesielt aktuell.

Forslagene til ny lovtekst (nedenfor) er innarbeidet i vårt radikale lovutkast, noe som innebærer at nummereringen når det gjelder nåværende §§ 11 og 19 er endret til henholdsvis §§ 9 og 18.

Forslag til (ny) § 9 annet ledd:

> Dersom behandlingsansvarlig planlegger å sammenstille personopplysninger for å utføre kontroll med den registrerte eller noen i hans husstand, skal dette eksplisitt angis som formål.

Forslag til (ny) § 18 første ledd bokstav b:

> [§ 19. Informasjonsplikt når det samles inn opplysninger fra den registrerte
>
> Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om
>
> …
>
> b) formålet med behandlingen,] herunder om opplysningene skal benyttes for å kontrollere den registrerte eller noen i hans husstand, (Någjeldende tekst i klammeparantes)

Forslaget til ny § 18 får også effekt i forhold til ny § 19 om innsamling av opplysninger fra andre enn den registrerte, se § 19 første ledd i vårt radikale lovforslag.

# Kapittel 8

## Overføring av personopplysninger til utlandet

### 8.1 Om mandatet

I rammen gjengir vi mandatets punkt 7 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Overføring av personopplysninger til utlandet*

Overføring av personopplysninger til utlandet reguleres av personopplysningsloven kapittel V. Det framgår av Ot.prp. nr. 92 (1998–99) s. 75 at den

stadig økende internasjonaliseringen nødvendiggjør en regulering som knesetter enkelte grunnleggende vilkår for slike overføringer, med det formål å ivareta sentrale personvernhensyn. Samtidig er det viktig at reguleringen åpner for fleksibilitet.

Ved overføring av opplysninger til utlandet kan den registrerte, den behandlingsansvarlige og tilsynsmyndighetene miste kontroll over behandlingen av opplysningene, og det er derfor oppstilt vilkår for slik overføring: Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater innenfor EØS-området som har gjennomført EU-direktivet, oppfyller kravet til forsvarlig behandling og opplysninger kan utveksles fritt, jf. personopplysningsloven § 29. Ved overføring til andre stater fra et EØS-land, såkalt tredjelandsoverføring, beror avgjørelsen i utgangspunktet på om EU-kommisjonen har truffet beslutning om tilstrekkelig beskyttelsesnivå i tredjelandet, jf. personvernforskriften § 6-1. Datatilsynet skal gjennomføre kommisjonens beslutninger. Det er gjort unntak fra krav til beskyttelsesnivå i tredjeland i personopplysningsloven § 30 blant annet når den registrerte samtykker i overføringen.

Datatilsynet har mottatt få henvendelser og meldinger om overføring av personopplysninger til utlandet og har behandlet svært få saker om dette. Det gjør at det er vanskelig å si noe konkret om hvilke eventuelle implikasjoner reglene om overføring vil ha for personvernet.

**Utrederne bes vurdere om krav til samtykke etter § 30 første ledd bokstav a bør være et tilstrekkelig vilkår for overføringer av opplysninger til et tredjeland som ikke oppfyller krev til forsvarlig behandling av opplysninger**. Det kan reises spørsmål om et slikt samtykke vil være basert på tilstrekkelig informasjon hos den registrerte. **I denne forbindelse bes utrederne kartlegge praksis og undersøke hvordan spørsmålet er løst i andre EØS-stater og vurdere om erfaringer fra andre land tilsier endringer i Norge.**

**Departementet ber videre utrederne vurdere om det er grunn til å endre personopplysningsloven eller forskriften slik at betydningen av EU-kommisjonens avgjørelser om hvilke land som har tilstrekkelig beskyttelsesnivå kommer klarere fram enn i dag, eventuelt om brukerne av loven på andre måter kan informeres om dette bedre enn i dag.**

**Til sist bes utrederne vurdere om overføring av personopplysninger til tredjeland bør være meldepliktig behandling** slik at Datatilsynet får bedre muligheter til å føre tilsyn.

## 8.2 Samtykke til overføring av personopplysninger til tredje land

Reglene i personopplysningsloven kapittel V bygger direkte på personverndirektivet artikkel 25 og 26. Sistnevnte bestemmelse åpner for at EU-/EØS-medlemsland tillater overføring av personopplysninger til tredjeland uten forsvarlig personvernbeskyttelse når bl.a. den registrerte samtykker til overføringen. Angjeldende del av artikkel 26 lyder:

> 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
>
> (a) the data subject has given his consent unambiguously to the proposed transfer ….

Det fremgår av bestemmelsens innledning at medlemsland ikke behøver å fastsette samtykke som vilkår for overføring, jf. "save where otherwise provided by domestic law governing particular cases". Dette er et punkt som er lite tydeliggjort i enkelte språkversjoner av direktivet.[195] Det er likevel utvilsomt at bestemmelsen gir medlemsland et visst spillerom.[196] Hvor stort dette spillerommet er, kan imidlertid diskuteres. Det at artikkel 26 nr. 1 refererer til "particular cases" kan tyde på at medlemsland skal være tilbakeholdne i å ikke benytte seg av de angitte unntaksmulighetene, inklusive vilkåret om samtykke. Det kan f.eks. argumenteres for at i den grad samtykke ikke nedfelles som overføringsvilkår, skal dette gjelde kun for nærmere bestemte situasjoner eller typer opplysninger som innebærer særlige personvernmessige risikoer (eksempelvis for arbeidstakers overføring av opplysninger om arbeidstakere, eller overføring av sensitive opplysninger generelt). Holdbarheten av dette argumentet er imidlertid usikker. Vi finner ingen direkte støtte for argumentet i fortalen eller forarbeidene til direktivet eller i teori. Visse bemerkninger fra artikkel 29 arbeidsgruppen gir noe men ikke entydig støtte til argumentet:

> Member States may provide in domestic law for the exemptions not to apply in particular cases. This might be the case, for example, where it is necessary to protect particularly vulnerable groups of individuals, such as workers or patients.[197]

Imidlertid har arbeidsgruppen for øvrig den klare oppfatning at alle unntak etter artikkel 26 nr. 1 skal tolkes og anvendes restriktivt.[198]

Det overveldende flertallet av EU-/EØS-medlemsstater – inklusive alle nordiske land – har valgt å fastsette samtykke som et tilstrekkelig vilkår for overføring etter artikkel 26 nr. 1. Det er med andre ord stor grad av sammenfall på dette punktet, til tross for betydelige ulikheter ellers i medlemsstatenes implementering av dataoverføringsreglene.[199] Det finnes imidlertid visse unntak. Ungarns lovgivning om personopplysningsvern tillater bruk av samtykke kun i tilfeller overføring til tredje land med et beskyttelsesnivå som EU-kommisjonen har godkjent som tilstrekkelig.[200] I Frankrike har datatilsynsmyndigheten (Commission Nationale de

---

[195] For eksempel lyder den svenske versjonen "om det inte finns tvingande regler om detta i deras lagstiftning" – en formulering som ikke samsvarer med den engelske, den franske, den tyske og den danske språkversjonen, jf. også bemerkninger dertil i SOU 1997: 39 s. 156 fotnote 84.

[196] Jf. eksempelvis NOU 1997:19 s. 102, Artikkel 29 arbeidsgruppen 1998 s. 24, og Blume 2006 s. 95 som alle nevner at medlemsland ikke er forpliktet til å gjennomføre alle unntakene etter artikkel 26 nr. 1.

[197] Artikkel 29 arbeidsgruppen 1998 s. 24.

[198] *Ibid.*

[199] Mer om ulikhetene, se bl.a. Korff 2002 avsnitt 14.3, Europa-kommisjonen 2003 s. 18–19.

[200] Jf. Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest, section 9(1).

l'Informatique et des Libertés – CNIL) valgt å innta en restriktiv holdning til bruk av samtykke som overføringsvilkår. I følge CNIL skal samtykke kun brukes i forhold til enkelte sporadiske overføringer av begrenset omfang. Samtykke skal ikke brukes i forhold til regelmessige og omfattende overføringer ("transferts répétitifs, massifs ou structurels"); slike overføringer skal snarere underlegges andre beskyttelsesvilkår (så som avtaler og bindende konsernregler ("Binding Corporate Rules")). I utgangspunktet skal heller ikke arbeidsgiveres overføring av opplysninger om arbeidstakere kunne skje på grunnlag av samtykke fordi et slikt samtykke – i følge CNIL – vanligvis vil mangle tilstrekkelig grad av frivillighet.[201]

Prinsipielt er vi i det vesentlige enige med resonnementet til CNIL. Overføring av personopplysninger med basis i samtykke – eller med basis i flere av de øvrige unntak nevnt i artikkel 26 nr. 1 – har svært betydningsfull virkning for den enkeltes personvern: Etter at opplysninger overføres til tredjeland som ikke har et tilstrekkelig beskyttelsesnivå, forsvinner langt på vei den registrertes mulighet for å verne om opplysningene, selv om samtykket blir tilbakekalt. Når overføring skjer kun på grunnlag av samtykke, bør dette derfor få spesiell oppmerksomhet av lovgiver og/eller tilsynsmyndigheten.

Selv om bruk av samtykke som overføringsvilkår er problematisk, er det dermed ikke sagt at samtykke bør forsvinne fra listen over overføringsvilkår etter personopplysningsloven § 30 første ledd. Vi mener at det er gode grunner for å opprettholde samtykke som mulig overføringsvilkår. For det første tilsier hensynet til regelharmonisering og forutberegnelighet innen EU/EØS – og til en viss grad forutberegnelighet for tredje land[202] – at Norge opprettholder et vilkår som finnes i de aller fleste andre EU-/EØS-landenes lovgivning. Hvis samtykkealternativet ikke blir beholdt, ville det for det andre bryte med et av lovens (og direktivets) prinsipielt viktige ideologiske utgangspunkter, nemlig personers selv-bestemmelsesrett. For det tredje er det mulig å tydeliggjøre i personopplysningsloven og i Datatilsynets praksis at bruken av samtykke som overføringsvilkår forutsetter kumulativ tilfredsstillelse av flere delvilkår (dvs. samtykke skal være frivillig, uttrykkelig og informert, jf. pol § 2 nr. 7).

Kravet om at samtykke skal være informert kan tydeliggjøres og utdypes i personopplysningsloven i forhold til overføringer til tredje land. Det viktigst elementet i dette kravet er at den registrerte er gjort oppmerksom på de særlige risikoer som overføring kan innebære.[203] Dette betyr at den registrerte blir informert om hvilket land mottakeren av opplysningene er basert i, det generelle beskyttelsesnivået for opplysningene i dette landet og risiko for personvernkrenkelser dersom opplysningene overføres. For å sikre at informasjonskravet her ikke blir for omstendelig må detaljeringsgraden tilpasses styrken i de aktuelle personvernmessige behov. Jo mer sensitive opplysningene er, desto større krav må stilles til informasjonen som skal danne grunnlaget for et samtykke. Likeledes vil kravet til frivillighet variere i takt med opplysningenes sensitivitet mv. og øvrige personvernmessige behov i det enkelte tilfellet.

---

Vi har imidlertid fått opplyst fra den ungarske datatilsynsmyndigheten at regelen snart skal endres slik at samtykke blir et tilstrekkelig overføringsvilkår uavhengig av mottakerlandets antatt beskyttelsesnivå.

201 Jf. CNIL 2006 s. 28–30.

202 Som Blume påpeker "[d]er er som nævnt adgang til i de nationale love at fastsætte fravigelser, hvilket i og for seg er problematisk, fordi sådanne kan forvirre omverdenens opfattelse af EU", jf. Blume 2006 s. 95.

203 Jf. også artikkel 29 arbeidsgruppen 1998 s. 24: "The requirement for information is particularly relevant in that it requires that the data subject be properly informed of the particular risk that his/her data are to be transferred to a country lacking adequate protection".

Det nevnte informasjonskravet kunne enten inngå som tilføyelse til den generelle bestemmelsen om informasjonsplikt i pol § 19 eller plasseres i § 30. Vi mener at kravet vil få størst signaleffekt i forhold til dets tiltenkte målgruppe hvis det plasseres i § 30 første ledd, som del av selve vilkåret om samtykke:[204]

> § 30 Unntak
>
> Personopplysninger kan også overføres til stater som ikke sikrer en forsvarlig behandling av opplysningene dersom
>
> a) den registrerte har samtykket i overføringen (jf. § 6 annet ledd), og den registrerte forut for avgivelsen av samtykket er gjort oppmerksom på den særlige risiko som overføringen kan innebære,
>
> b) […].

## 8.3 EU-kommisjonens avgjørelser om beskyttelsesnivået i tredje land

EU-kommisjonen har kompetanse til å bestemme om et tredje land tilbyr tilstrekkelig personopplysningsvern, jf. personverndirektivet artikkel 25 nr. 6. Denne kompetansen innebærer at Kommisjonen kan overprøve medlemsstaters (og dermed nasjonale datatilsynsmyndigheters) egne vurderinger av spørsmålet om tilstrekkelighet. Ved inngangen til 2006 har Kommisjonen vedtatt at Sveits, Argentina, Canada, Guernsey, Isle of Man og 2 særskilte ordninger for dataoverføring til USA tilbyr tilstrekkelig vern.

Det følger av EØS-avtalen at Norge skal etterleve Kommisjonens beslutninger om beskyttelsesnivå.[205] Avtalen gir samtidig Norge en reservasjonsadgang, men det er svært usannsynlig at den kommer til å bli benyttet i særlig grad. Betydningen av Kommisjonens beslutninger om tredje lands beskyttelsesnivå går frem av personopplysningsforskriften § 6-1. Bestemmelsen er klar og tydelig i sin formulering og er den første av forskriftsbestemmelsene som angår overføring av personopplysninger til utlandet.

Kommisjonen har hittil truffet relativ få beslutninger om beskyttelsesnivå, og vi tror ikke at det på kort sikt blir en markant økning i antall beslutninger. I lys av dette samt at forskriftsbestemmelsen om betydningen for Norge av Kommisjonens beslutninger ikke er vanskelig å forstå eller finne, ser vi ikke særlige grunner til at bestemmelsen blir "oppgradert" og satt inn i selve loven.

Det er verdt å merke seg at den finske personopplysningsloven fikk i 2000 en ny bestemmelse som synliggjør Kommisjonens beslutninger:[206]

> Personuppgifter får översändas till stater utanför Europeiska unionens medlemsstaters territorium eller Europeiska ekonomiska samarbetsområdet, till den del Europeiska gemenskapernas kommission i enlighet med artiklarna 3 och 25.6 i Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, nedan personuppgiftsdirektivet, har konstaterat att staten i fråga tryggar en tillräcklig dataskyddsnivå.

[204] Forslaget nedenfor har henvisning som er tilpasset moderat lovforslag, se avsnitt 13.3.

[205] Jf. EØS-komiteens beslutning 25.6.1999 nr. 83/1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI.

[206] Jf. 22 a § tilføyd ved lov 22.11.2000 nr. 986.

> Personuppgifter får inte översändas till stater utanför Europeiska unionens medlemsstaters territorium eller Europeiska ekonomiska samarbetsområdet, om kommissionen i enlighet med artiklarna 3 och 25.4 i personuppgiftsdirektivet har konstaterat att staten i fråga inte tryggar en tillräcklig dataskyddsnivå.

Det ville vært forholdsvis enkelt å sette inn en lignende bestemmelse som tredje og fjerde ledd i pol § 29. De fleste andre EU-lands lovgivning mangler imidlertid en tilsvarende bestemmelse. Det er viktig å understreke at dette har ingen rettslig betydning siden landene – som Norge – uansett er forpliktet til å følge Kommisjonens avgjørelser. Den finske bestemmelsen har dermed mest verdi som "folkeopplysning".

## 8.4 Meldeplikt?

Etter personopplysningsloven § 32 første ledd bokstav h (jf. § 31) skal behandlingsansvarlige underrette Datatilsynet om planlagt overføring av personopplysninger til tredje land. En rekke kategorier av personopplysningsbehandlinger er imidlertid unntatt meldeplikten etter personopplysningsforskriften kapittel 7. Vi har foreslått en vesentlig endring i dagens meldeplikt, og den følgende diskusjonen forutsetter derfor at en velger å beholde hovedtrekkene i dagens ordning. Spørsmålet blir da om disse unntak fra meldeplikt skal avgrenses når opplysninger skal utleveres til tredje land uten tilstrekkelig beskyttelsesnivå.

I prinsippet ville det vært hensiktsmessig at Datatilsynet fikk meldinger om all planlagt utlevering av opplysninger til tredje land som ikke tilbyr tilstrekkelig beskyttelse for opplysningene. Gitt grunnleggende trekk ved dagens teknologiske og organisatoriske virkelighet er det høyst sannsynlig at det foregår en storskala overføring av personopplysninger til tredje land i strid med personopplysningsloven. Samtidig mangler Datatilsynet detaljerte kunnskaper om omfanget av disse dataoverføringene. Dette er ikke nytt: Også i forhold til personregisterloven ble det antatt at det forelå "et stort mørketall" av meldepliktige overføringer som ikke ble meldt.[207] Dette er heller ikke et særnorsk problem: De fleste datatilsynsmyndigheter i EU/EØS sliter tydeligvis med mørketallsproblemet.[208]

Det er imidlertid tvilsomt om en mer omfattende meldepliktsordning ville rette opp situasjonen i nevneverdig grad. Meldepliktsordningen i henhold til personregisterloven var forholdsvis omfattende, men klarte trolig ikke å fange opp flertallet av meldepliktige overføringer. Det ble antatt at dette mørketallet først og fremst skyldtes manglende kjennskap til meldepliktsordningen snarere enn bevisst overtredelse av loven.[209] Det er grunn til å anta at det samme uvitenhet også ville ramme en eventuell omfattende meldepliktsordning etter personopplysningsloven. Med dagens teknologiske utvikling – særlig bruken av internett – og de generelle globaliseringstrekk i alle sektorer av samfunnsliv, er det stor sannsynlighet for at det vil oppstå et enda større misforhold enn på 1970, -80 og -90-tallet, mellom antall meldinger til Datatilsynet om overføringer og det faktiske antallet overføringer.

Vi er videre usikre på om en mer omfattende meldepliktsordning vil gi noen nevneverdig personvernmessige gevinst. Datatilsynet synes nå i liten grad å analysere og ta aktiv stilling

---

[207] Jf. Djønne, Grønn og Hafli 1987 s. 159. Samme sted skrives det at i perioden fra 1980 til 1987 mottok Datatilsynet kun 300 meldinger om overføring til utlandet. Jarbekk skriver at i perioden fra 1990 til november 1995 var antall meldinger litt i underkant av 200, jf. Jarbekk 1996 s. 4.

[208] Jf. EU-kommisjonen 2003 s. 19.

[209] Jf. Djønne, Grønn og Hafli 1987 s. 157.

til innkomne meldinger. Det kan vanskelig tenkes at denne situasjonen vil endre seg etter innføring av en mer omfattende meldepliktsordning for dataoverføringer til tredje land.

Vårt "radikale" forslag til § 33a kan etter vår mening fange opp en del av de problemer som gjelder overføring av personopplysninger til tredjeland, se avsnitt 13.2. Bestemmelsen innebærer at personer som vil bli berørt av overføring til slike land, på nærmere bestemte vilkår kan kreve at Datatilsynet konsesjonsbehandler saken. Det er grunn til å tro at dette (i) kan medvirke til at behandlingsansvarlige foretar samvittighetsfull vurdering for å unngå at berørte personer skal protestere, og (ii) kan innebære at vanskelige og viktige saker kommer på Datatilsynets bord til avgjørelse.

Også vårt forslag til ordning med personvernombud, vil innebære at spørsmålet får særlig oppmerksomhet. Uten slikt ombud vil overføring til tredjeland inngå i forpliktelsen til å gjennomføre internkontrollrutiner, se § 14. For å styrke dette punktet, vil en kunne tydeliggjøre spørsmålstypen i forskriften til § 14 (forskriftens kapittel 3).

# Kapittel 9

## Melde- og konsesjonsplikten

### 9.1 Om mandatet

I rammen gjengir vi mandatets punkt 8 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Melde- og konsesjonsplikten*

Erfaringer fra Datatilsynet tilsier at dagens konsesjonsplikt er for omfattende og fører til en lite hensiktsmessig bruk av tilsynets ressurser. **Departementet ber om at det utformes ett eller flere forslag som fører til en klar reduksjon av antallet konsesjonssaker.** Det må vurderes om en mer målrettet tilnærming kan gi en bedre løsning enn dagens konsesjonsplikt. For eksempel bør det vurderes om det er mulig å utforme konsesjonsplikten slik at den bare gjelder for nærmere bestemte behandlingsformer som typisk lett kan krenke personvernet. Et eksempel på en behandling som ikke bør være undergitt informasjonsplikt, kan være en type behandling som foregår i alle kommuner, men som neppe truer personvernet i nevneverdig grad, slik som for eksempel kartlegging av boligbehov og opplysninger som behandles i forbindelse med utstedelse av ledsagerbevis.

Det må legges vekt på at de nye reglene skal rette seg mot saker der personvernhensyn tilsier at behovet for en forhåndskontroll er størst, samtidig som reglene må gi en tilstrekkelig forutberegnlighet for de behandlingsansvarlige. **Det bør også vurderes om endringer av reglene om konsesjonsplikt bør føre til at reglene om meldeplikt bør endres for å oppnå best mulig sammenheng i regelverket.**

Konsesjonsordningen var hjørnesteinen i personregisterloven av 1978, og ordningen ble videreført i redusert omfang i personopplysningsloven. Samtidig ble meldeplikten innført, til en viss grad som en kompensasjon for redusert konsesjonsplikt. Det er med andre ord en historisk betinget kopling mellom konsesjons- og meldeplikt, noe som også gjenspeiles i mandatet. Disse to ordningene er sentrale og må ses i sammenheng. Likevel vil vi minne om at den bakenforliggende problemstillingen er bredere: Hvilke virkemidler skal Datatilsynet råde over for å sikre ivaretakelsen av personvernet?

Grunnleggende sett gjelder spørsmålet helt generelt om hvilket virkemiddelapparat som kan/bør tas i bruk for å sikre en balansert avveining mellom hensynet til personvern og andre hensyn, og for å sikre etterlevelse av de bestemmelser som gjelder for behandling av personopplysninger. Konsesjons- og meldeordningen bør ikke eksistere uavhengig av andre virkemidler, heller ikke uavhengig av virkemidler som direkte ligger i hendene på andre aktører enn Datatilsynet. Det er således behov for å se mange virkemidler i sammenheng, og etter vår mening bør mandatpunkt 8 særlig ses i sammenheng med punkt 9 i mandatet vedrørende frivillige ordninger, dvs. ordninger som kan supplere Datatilsynets innsats. Likevel har vi valgt å fremstille disse spørsmålene i tråd med punktene i mandatet. Vurderinger og forslag i dette kapittelet, må imidlertid ses i sammenheng med vurderinger og forslag i neste kapittel.

## 9.2 Generelt om konsesjons- og meldeplikt

Understrekningen av behovet for å se mange virkemidler i sammenheng er ikke ny, men ble sterkt fremhevet av Skaugeutvalget:

> Personregisterloven gjør i dag bruk av flere reguleringsformer, ved at den kombinerer en omfattende konsesjonsplikt med materielle normer, rådgivning og etterfølgende kontroll (se nærmere ovenfor 12.2 om gjeldende rett). Utvalget foreslår at man også i fremtiden benytter flere ulike reguleringsmåter. Konsesjonspliktordningen foreslås videreført, men blir mindre omfattende enn i dag (se 12.5.5) og avløst av en rekke tiltak som bl a er fundert på en meldeplikt (12.5.4) i kombinasjon med mer vidtrekkende tilsynsoppgaver fra Datatilsynet. Utvalget foreslår dessuten at Datatilsynet som i dag skal ha rett og plikt til å gi råd til dem som planlegger å behandle eller allerede behandler personopplysninger, samt til å gjennomføre etterfølgende kontroller (12.5.6). Også materielle regler bør stå sentralt i reguleringen, og utvalget foreslår at denne reguleringsformen benyttes i større grad enn i dagens lov (12.5.7). Det vil dessuten som i dag være behov for regulering i forskrift (12.5.3). Videre foreslås regler om internkontroll (12.5.8), og endelig har utvalget vurdert bransjevise atferdsnormer (dvs. retningslinjer vedrørende personvern som er utarbeidet av de behandlingsansvarlige selv), se 12.5.9. […] Utvalget vil understreke behovet for å se de ulike typene reguleringsformer i sammenheng.[210]

Det er i utgangspunktet grunn til å understreke at vi ikke har gjort noen systematisk undersøkelse av Datatilsynets arbeidsmetoder og prioriteringer, og at dette heller ikke inngår i mandatet for denne utredningen. Vi har likevel valgt å understreke behovet for en (fortsatt) brede tilnærmingen slik sitatet ovenfor uttrykker. Representanter fra Datatilsynet har overfor oss gitt uttrykk for at ordningen med meldeplikt er til meget begrenset nytte, og dette bekreftes bl.a. av en studentoppgave fra 2005.[211] Etter vår mening er det av avgjørende betydning å ha et velfungerende meldesystem. Et svakt eller ikke-fungerende meldesystem bør gjøre det mindre aktuelt å redusere omfanget av konsesjonsplikten. Årsaken er primært at konsesjonsplikt særlig bør erstattes av økt kontrollvirksomhet. Kontrollvirksomheten er uansett begrenset og må styres ut i fra noen prioriteringskriterier. Slike prioriteringer krever et faktisk grunnlag som meldesystemet kan generere.

I Skaugeutvalgets forslag til meldeplikt ble det formulert fire målsettinger for den foreslåtte ordningen:[212]

1. Etablere en kontakt mellom Datatilsynet og den behandlingsansvarlige.
2. Gi grunnlag for å formidle regelinformasjon til de meldepliktige og bidra til å høyne bevissthetsnivået om personvernspørsmål hos disse.
3. De samlede meldingene skal utgjøre en vesentlig del av Datatilsynets kunnskapsbasis for tilsynets prioritering av arbeidsoppgaver, særlig i relasjon til kontroll, veiledning og regelverk.
4. Sikre offentlighet med hensyn til de behandlinger som foretas.

Etter vår mening bør disse punktene ses som en felles målsetting for både konsesjons- og meldeplikten. Den samlede virkemiddelbruken bør i størst mulig grad støtte opp om disse målsettingene – eller snarere – *strategiene* for å etablere et effektivt personvernregime. Dette

[210] Jf. NOU 1997: 19 s. 78–79.

[211] Se Berg m.fl. 2005 s. 24 der de fremhever at Datatilsynet primært bruker meldesystemet i tilknytning til fjern-synsovervåking, og at systemet i liten grad er grunnlag for tilsynsvirksomhet ellers.

[212] Se NOU 1997: 19 s. 80.

synspunktet innebærer likevel ikke at andre strategier er unødvendige, og i neste kapittel vil vi fremme supplerende synspunkter på disse strategivalgene.

Konsesjons- og meldeplikt kan *potensielt* være nært beslektede tiltak. Begge ordninger kan foranledige enkeltvedtak fra Datatilsynet, og i dette vedtaket kan det innbefattes pålegg, forbud og vilkår mv. I tilfelle som er underlagt meldeplikt, er Datatilsynets kompetanse knyttet til § 46 og den lovlighetskontroll denne bestemmelsen hjemler. I konsesjonstilfellene kan Datatilsynet i tillegg "sette vilkår for behandlingen når slike vilkår er nødvendige for å begrense ulempene behandlingen ellers ville medføre for den registrerte", se § 35. I konsesjonstilfellene har Datatilsynet med andre ord kompetanse til å spille en mer konstruktiv rolle enn i meldetilfellene.

Konsesjonsordningen innebærer en situasjon der lovgiver har forhåndsdefinert noen generelle kjennetegn som gir Datatilsynet en plikt til saksbehandling. Meldeordningen er derimot innrettet slik at tilsynet til en hver tid selv kan bestemme hva som skal være bestemmende for deres innsats, og gir ingen plikt til å behandle andre saker enn de Datatilsynet finner nødvendig. I hvilken grad andre aktører, for eksempel registrerte personer og interesseorganisasjoner mv., kan foranledige saksbehandling og myndighetsutøvelse fra Datatilsynet er uklart etter loven.

En forskjell mellom konsesjons- og meldeplikt gjelder tidsperspektivet. Melding skal sendes minst 30 dager før behandling av personopplysninger starter, dvs. behandlingen kan starte etter 30 dager med mindre Datatilsynet har forbudt behandlingen i samsvar med § 46. Meldeplikten kan derfor ses som et 30 dagers forbud mot å behandle personopplysningene, og dette innebærer samtidig et visst press på Datatilsynet til å handle innen denne fristen. Konsesjonsplikten er ikke knyttet til noen særlige frister, men forvaltningslovens regler som saksbehandlingstider gjelder også for konsesjonssaker, dvs. saken skal forberedes og avgjøres "uten ugrunnet opphold" (fvl § 11a). Tredje ledd i samme bestemmelse innebærer at det skal gis foreløpig svar i konsesjonssaker dersom saken ikke er avgjort innen 30 dager etter at konsesjonssaken ble mottatt.

Beslutningsgrunnlaget som inngår i de to ordningene er også forskjellig. Når det gjelder meldeplikten, er det klart angitt i § 32 hva meldingene skal/kan inneholde. For konsesjonsordningen inneholder verken lov eller forskrift noen tilsvarende angivelse av hvilket beslutningsgrunnlag som skal foreligge. Årsaken er at konsesjonsbehandlingen er basert på en forestilling om at det her vil skje en genuint individuell vurdering av hver sak, og at det derfor er vanskelig å angi på forhånd hvilke opplysninger som må foreligge. I praksis er imidlertid standardiseringsbehovet stort også når det gjelder konsesjoner, og Datatilsynet har således utformet et skjema over 4 sider der det spørres etter opplysninger innen et forholdsvis vidt spektrum; for eksempel vedrørende hvordan informasjonsplikten etter §§ 19 og 20 planlegges etterlevet, utarbeidelse av internkontrollsystem, opplysningskvalitet og informasjonssikkerhet. Beslutningsgrunnlaget i meldesaker og konsesjonssaker overlapper et stykke på vei, men i konsesjonssaker er beslutningsgrunnlaget klart bredere enn i meldesaker. Meldinger som blir fulgt opp ved hjelp av saksbehandling, vil normalt foranledige ytterligere informasjonsinnsamling. Når konsesjonssøknad er sendt og saken tatt under behandling, vil det tilsvarende kunne være behov for utfyllende opplysninger. Den samlede informasjons-mengden i saker som er foranlediget av melding og konsesjonssøknad trenger med andre ord ikke være veldig forskjellig. Dersom en forutsetter at konsesjonssaker alltid må opplyses ut over det som følger av konsesjonsskjemaet, kan en med andre ord tenke seg at meldings- og

konsesjonssaker gjorde bruk av samme skjemaet, og at skillet primært kan gjelde *oppfølgingen* av sakene.

Vårt hovedpoeng her er at forskjellene mellom en fremtidig konsesjons- og meldeplikt ikke nødvendigvis trenger å være markerte. Det vil således være mulig å etablere/praktisere en meldeplikt der Datatilsynet aktivt plukker ut og behandler saker med tanke på å treffe enkeltvedtak. I så fall kunne saksbehandlingsinnsatsen i stor grad styres avhengig av skiftende prioriteringer, kapasitetsmessige forhold osv. Tidsfristen for meldeplikten kan også introduseres som del av bestemmelser om saksbehandling og enkeltvedtak, for eksempel slik at Datatilsynet må behandle saker innen en viss frist, og slik at fristoverskridelse begrenset tilsynets kompetanse til å gripe inn på et senere tidspunkt.

Vi mener det er grunn til å vurdere om det er hensiktsmessig å videreføre konsesjons- og meldeplikt som to atskilte ordninger. Som vår lille sammenlignende analyse ovenfor viser, er det fullt mulig å bygge elementer fra de nåværende konsesjons- og meldepliktordningene sammen til én integrert ordning. I avsnitt 9.5.2 kommer vi tilbake til et konkret forslag til hvorledes dette kan gjøres.

## 9.3 Nærmere om meldeplikten

### 9.3.1 Oversikt over fremstillingen og meldeplikt etter personverndirektivet

I det følgende gjennomgår vi bestemmelsene i § 31 om plikten til å gi melding til Datatilsynet (avsnitt 9.3.2) og kravet til innholdet av meldinger i § 32 (avsnitt 9.3.3). I hvert av disse avsnittene gjør vi kun enkelte lovgivningstekniske vurderinger. I avsnitt 9.3.4 ser vi kort på den praktiske gjennomføringen av meldepliktordningen. Når det gjelder hensiktsmessigheten og effektiviteten av en så vid meldeplikt som etter § 31, velger vi å se dette spørsmålet i sammenheng med innholdet av meldeplikten og den praktiske gjennomføringen av ordningen og den mulige bruken av meldingene. Vi har derfor valgt å gi en samlet vurdering i avsnitt 9.3.5. Forslag til endrede bestemmelser gis i avsnitt 9.5, der forslagene er ment å erstatte alle bestemmelser vedrørende melde- og konsesjonsplikt.

Melding til tilsynsmyndigheten er et viktig element i personverndirektivet, se artikkel 18 og 19. Den norske meldepliktordningen ligger klart innenfor den ordningen som er skissert i direktivet, men kan sies å representere en av de mest omfattende løsninger som direktivet gir rom for. Direktivets utgangspunkt er at det er helt eller delvis elektronisk behandling av personopplysninger som skal meldes, men åpner også for at manuell behandling av personopplysninger kan meldes.[213] Direktivet åpner for en forenklet meldeplikt eller unntak fra meldeplikt, og angir vilkårene for at dette kan skje, men angir ikke hva forenklingen kan gå ut på. I Norge er adgangen til å gjøre unntak benyttet i flere tilfelle, se avsnitt 9.3.2. Direktivet åpner videre for unntak fra meldeplikten for visse allment offentlige opplysninger,[214] og for visse opplysninger som behandles av ideelle organisasjoner mv.[215] Disse sist nevnte unntaksalternativene er ikke benyttet i den norske loven og forskriften.

Krav til innholdet av meldingene er angitt i artikkel 19 nr. 1 bokstavene a – f og tilsvarer i meget stor grad de innholdsmessige kravene i pol § 32, se avsnitt 9.3.3 nedenfor.

[213] Se artikkel 18 nr. 1 og nr. 5.
[214] Se artikke 18 nr. 3.
[215] Se artikkel 18 nr. 4, jf. artikkel 8 nr. 2 bokstav d.

### 9.3.2 Omfanget av meldeplikten

Personopplysningsloven § 31 etablerer en generell meldeplikt for det store flertallet av behandlinger som faller inn under loven. Dette fremgår ved å sammenligne § 31 første ledd bokstavene a og b, med § 3 første ledd bokstavene a og b som beskriver lovens saklige virkeområde. Sammenholdt er det to avvik: I § 31 første ledd bokstav a er "behandling av personopplysninger med elektroniske hjelpemidler", angitt som meldepliktig. Presiseringen "som helt eller delvis skjer [med elektroniske …]" som inngår i § 3 første ledd bokstav a, er utelatt. Dette har imidlertid ikke betydning fordi delvis elektronisk behandling uansett er den betegnelsen som passer i det store flertallet tilfellene der personopplysninger blir behandlet.

Når det gjelder (manuelle) personregistre gjelder meldeplikten for "opprettelse av manuelt personregister som inneholder sensitive personopplysninger". Det saklige virkeområdet omfatter "annen behandling [enn helt eller delvis elektronisk] av personopplysninger når disse inngår eller skal inngå i et personregister". Forskjellen er med andre ord at en ikke trenger å melde fra om innsamling av personopplysninger som skal inn i et register, og at det kun er registre som inneholder sensitive personopplysninger som skal meldes. Loven må forstås slik at det i registeret må forekomme opplysningstyper som er sensitive, og at forekomster av sensitive enkeltopplysninger ikke utløser meldeplikt, jf. diskusjonen i avsnitt 2.2.3.

Etter vår mening er det uheldig at en i loven benytter formuleringer som er nesten identiske med andre sentrale formuleringer i loven, uten at forskjellen har innholdsmessig betydning. Beskrivelsen av meldepliktige manuelle personregistre mangler presisjon. Dersom en ønsker å beholde denne delen av meldeplikten, kan den lett gjøres klarere.

Meldeplikten inntreffer på et tidspunkt som ligger minst 30 dager før den planlagte behandlingen av personopplysninger starter. Det inntrer også meldeplikt dersom det skjer endringer i de opplysninger som er gitt i tidligere meldinger, se tredje ledd første setning. Det fremgår ikke av loven eller forarbeidene om det i slike tilfeller skal sendes en helt ny melding, og av den elektroniske melderutinen fremgår det at fullstendig melding skal inngis selv om det kun er endringer i enkelte opplysningstyper.

Den tredje meldepliktige situasjonen oppstår når det har gått 3 år siden siste melding, selv om det ikke har skjedd endringer i meldingens innhold. Tidsangivelsen på 30 dager står i tilknytning til først nevnte meldeplikt, men det er nærliggende å forstå loven slik at også endringsmeldinger må sendes inn senest 30 dager før endringen får virkning. Dette er nødvendig for at Datatilsynet skal kunne gripe inn dersom endringen ikke kan godtas, f.eks. fordi et nytt formål klart kommer i konflikt med det opprinnelige formålet, jf. § 11 første ledd bokstav c. Dersom en ønsker å beholde denne delen av meldeplikten, bør en sørge for at 30-dagersregelen får en ordlyd eller plassering som viser at den gjelder generelt.

Paragraf 31 siste ledd gir hjemmel for å gjøre unntak fra meldeplikten, men det fremgår ikke om slike unntak er gitt, eller hvor de er gitt. Dette er etter vår mening lite tilfredsstillende. Vi viser her til tilsvarende spørsmål vedrørende unntak fra konsesjonsplikt, se avsnitt 9.4.6.

Personopplysningsforskriften kapittel 7 avsnittene II og III inneholder unntak fra meldeplikten. I avsnitt II er det kun gjort unntak fra meldeplikt, mens det i avsnitt III både er gjort unntak fra konsesjons- og meldeplikt. Sist nevnte tilfelle gjelder behandlinger som i utgangspunktet er underlagt konsesjonsplikt. I andre tilfelle innebærer unntak fra konsesjons-

plikt meldeplikt i stedet (se pof kapittel 7 avsnitt IV). Unntakene fra konsesjonsplikt og konsesjons- og meldeplikt, er nærmere presentert i avsnitt 9.4.2 (nedenfor), og her nøyer vi oss derfor med kun å omtale unntakene fra (bare) meldeplikten i kapittel 7 avsnitt II (§§ 7-6 til 7-12).

Følgende unntak fra meldeplikten er gjort i følgende tilfeller:

- Kunde-, abonnent- og leverandøropplysninger, § 7-7
- Opplysninger i boligforhold, § 7-8
- Aksjebok § 7-9
- Protokollføring av mekling § 7-10
- Aktivitetslogg i edb-system eller datanett § 7-11
- Personvernombud § 7-12.

De fem første unntakstilfellene er primært knyttet til bestemte formål med behandlingen som er angitt og presisert i hvert alternativ. For aktivitetslogger er det for eksempel et vilkår for unntak at opplysningene brukes til administrasjon av systemet, eller for å avdekke/oppklare sikkerhetsbrudd.

Det siste alternativet vedrørende personvernombud (§ 7-12), gjelder unntak som er knyttet til at den behandlingsansvarlige utpeker et uavhengig personvernombud. I slike tilfeller kan Datatilsynet gjøre unntak, dvs. unntaket krever en enkeltavgjørelse i tilsynet. Bestemmelsen stiller også krav til hva personvernombudet skal gjøre, og blant annet skal ombudet "føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32", dvs. de opplysninger som inngår i en ordinær melding. Unntaket innebærer derfor ingen praktisk lettelse for den behandlingsansvarlige; den eneste forskjellen er at opplysningene ikke sendes inn til Datatilsynet og inngår i den samlede basen over meldinger. I tillegg skal personvernombudet sikre at den behandlingsansvarlige etterlever personopplysningsloven med forskrifter.

Når det gjelder unntaket i pof § 7-12, er dette i realiteten en bestemmelse som etablerer en ordning med personvernombud. Teknisk sett burde bestemmelsen om vilkårene for å etablere personvernombud, ombudets oppgaver mv, være regulert adskilt fra bestemmelsen om unntak fra meldeplikten. I kapittel 10 kommer vi tilbake til spørsmålet om personvernombud med forslag til en fornyet ordning.

### 9.3.3 Innholdet av meldeplikten

Det som skal meldes til Datatilsynet er i alt 9 opplysningstyper som beskriver vedkommende behandling av personopplysninger. Disse opplysningstypene er for en stor del felles med de opplysningstypene som er angitt i personverndirektivet artikkel 19, men det er også viktige forskjeller. For det første inneholder direktivet krav om beskrivelse av hvem de registrerte er (se artikkel 19 nr. 1 bokstav c), men denne opplysningstypen mangler i den norske loven. Størst avvik fremkommer imidlertid ved at det i den norske loven spørres etter opplysningstyper som direktivet ikke har med. Dette gjelder alternativene:

b) når behandlingen starter;
c) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter;
f) hvor personopplysningene hentes fra;
g) det rettslige grunnlaget for innsamlingen av opplysningene.

Artikkel 19 angir minstekrav til innhold (”shall include at least”), noe som innebærer at de fire tilleggsopplysningene som er referert ovenfor, er uproblematisk i forhold til direktivet. Utelatelsen av å beskrive de registrerte personene (”the category or categories of data subject”) er formelt sett et irregulært avvik fra direktivet, men har neppe stor betydning.

De opplysninger som skal inngå i meldingene, er slike som en forventer vil gi et tilfredsstillende vurderingsgrunnlag for Datatilsynet, jf. tilsynets inngrepskompetanse (§ 46) og adgang til å pålegge konsesjonsplikt etter en konkret vurdering (§ 33 annet ledd, se avsnitt 9.4.3). Ytterligere opplysningstyper og detaljering av gjeldende krav til opplysninger, kunne selvsagt være nyttig i konkrete tilfelle. Samtidig er det imidlertid grenser for hvor omfattende og standardisert meldingenes innhold kan være før det blir uforholdsmessig arbeidskrevende for behandlingsansvarlige å fylle ut, sammenholdt med effekten av at opplysningene blir gitt. Det kan tvert i mot være aktuelt å undersøke muligheten for å innskrenke meldeplikten eller gjøre den ”indirekte”, uten Datatilsynet som adressat (jf. den beskrevne ordningen med personvernombud i henhold til pof § 7-12, se avsnitt 9.3.2). Vi kommer nærmere tilbake til disse mulighetene i avsnittene 9.4.8 og 9.5.

### 9.3.4 Datatilsynets behandling av meldinger

For Datatilsynet innebærer ikke innkomne meldinger noen plikt til å foreta realitetsbehandling av meldingenes innhold. Aktivitetsplikten begrenser seg til å registrere at meldingen har kommet frem og til å sende kvittering for at meldingen er mottatt. I forarbeidene til loven ble det imidlertid klart forutsatt at meldingene skulle brukes aktivt, se avsnitt 9.2 der vi har gjengitt de fire målsettingene med meldeplikten som Skaugeutvalget forutsatte, og som forutsetter at Datatilsynet etablerer flere rutiner, bl.a. for formidling av regelinformasjon, gjennomføring av analyser av det innkomne materialet for å ta stilling til hvorledes kontrollressurser skal disponeres, og etablering av rutiner for tilgjengeliggjøring og søking/gjenfinning av opplysninger i innkomne meldinger. Slike krav til Datatilsynets interne arbeid med meldingene ble imidlertid ikke lovfestet. I forarbeidene er det imidlertid uttalelser fra departementet som klart forutsetter en aktiv bruk av meldingene, bl.a:

> For at meldingene skal kunne benyttes som grunnlag for Datatilsynets kontrollvirksomhet, vil det være nødvendig å lagre dem elektronisk på en måte som gjør at man med enkle søkekriterier kan peke ut særlige områder eller bransjer for kontroll.[216]

Aktiv bruk av meldingene er selvsagt nødvendig for at en meldeordning skal kunne forsvares. Vi kommer nærmere tilbake til spørsmålet om praktiseringen av meldeplikten i neste avsnitt samt i kapittel 14 om administrative og økonomiske konsekvenser.

## 9.4 Nærmere om konsesjonsplikten

### 9.4.1 Oversikt over fremstillingen og utgangspunkter i personverndirektivet

Loven inneholder to typer konsesjon: en type for sensitive personopplysninger og en type etter Datatilsynets konkrete vurdering, se henholdsvis avsnittene 9.4.2 og 9.4.3. I tillegg blir konsesjonsplikten utvidet i personopplysningsforskriften. Fordi denne utvidelsen har nærmest sammenheng med konsesjon for behandling av sensitive personopplysninger, blir den behandlet i avsnitt 9.4.2 i sammenheng med gjennomgang av forskriftens bestemmelser

[216] Jf. Ot. prp. nr. 92 (1998–99) s. 56.

vedrørende konsesjonsplikt. Viktige felles regler som gjelder uavhengig av hva slags konsesjon det er tale om, blir omhandlet i avsnittene 9.4.4 til 9.4.6.

Personverndirektivet omtaler "prior checks", dvs. forhåndskontroll, og forutsetter ikke etablering av forbud mot å behandle visse opplysninger før det foreligger tillatelse i form av en forhåndsgodkjenning eller konsesjon:

> Article 20 Prior checking
>
> 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

Direktivet forutsetter heller ikke at det er tilsynsmyndigheten som skal gjennomføre kontrollen:

> 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

En "data protection official" kan for eksempel være personvernombud eller lignende, som på sin side skal ha en plikt til å rådføre seg med tilsynsmyndigheten i tvilstilfeller. Det er verd å merke seg at direktivet ikke knytter forhåndskontrollen til spesielle opplysningstyper, og bringer ikke inn spørsmålet om sensitive opplysninger. I stedet er det vist til en generell risikovurdering ("likely to present specific risks"), uten at momentene i en slik vurdering er angitt. I fortalen punkt 54 uttales det imidlertid at "the amount posing such specific risks should be very limited". Dette må forstås slik at omfanget av tilsynsmyndighetens eller personvernombudets forhåndskontroll forutsettes å være lite. Behandlingsansvarliges *egen* forhåndsvurdering av personvernrisiko omfattes imidlertid ikke av denne uttalelsen. Således kan lovgiver pålegge behandlingsansvarlige å gjennomføre forhåndskontroller selv, på lignende måte som for den norske ordningen med internkontroll, jf. pol § 14 og pof kapittel 3.

### 9.4.2 Konsesjonsplikt for behandling av sensitive personopplysninger (§ 33 første ledd), med unntak og tillegg i forskriften

Etter personregisterloven var utgangspunktet at det alltid var krav til konsesjon (forhåndstillatelse) fra Datatilsynet for at det skulle være lovlig å etablere personregistre som skulle gjøre bruk av elektroniske hjelpemidler eller behandle sensitive personopplysninger. Personopplysningsloven innebar en vesentlig innsnevring i forhold til dette. Lovens § 33 første ledd pålegger behandlingsansvarlige å søke konsesjon dersom det skal behandles sensitive personopplysninger, jf. § 2 nr. 8. Konsesjonsplikt oppstår med andre ord dersom (i) det skal behandles sensitive personopplysninger ved hjelp av elektroniske hjelpemidler, og (ii) det skal behandles sensitive personopplysninger som inngår i et personregister eller skal inngå i et personregister, jf. § 3 første ledd.

Når en skal ta stilling til om det foreligger konsesjonsplikt etter denne bestemmelsen, er hovedproblemet å ta stilling til hva som kan sies å være en "sensitiv personopplysning". Vi viser her til diskusjon og forslag i avsnitt 2.2.3. Dersom det er klart at det foreligger sensitive personopplysninger, blir neste oppgave å undersøke om det gjelder unntak. Et unntak som

fremgår direkte av loven er nedfelt i § 33 fjerde ledd.[217] For øvrig er det kun gitt hjemler til å gjøre unntak, se § 33 siste ledd. Her fremgår det bare at det *kan* gjøres unntak. Dette er etter vår mening lite tilfredsstillende. En behandlingsansvarlig som vil undersøke om han er underlagt konsesjonsplikt, bør kunne lese direkte i lovteksten at det *er* gjort unntak, og hvor unntakene er regulert, se for øvrig avsnitt 9.4.6 (nedenfor). Personopplysningsforskriften er etter vår mening så sentral og stabil, at det bør kunne gis generelle henvisninger fra loven til forskriften. Loven bør med andre ord kunne opplyse om at unntak *er* gjort i personopplysningsforskriften, og bør om mulig også kunne si noe om hvilke typer unntak som er gjort.

Unntakene fra § 33 første ledd er gjort i personopplysningsforskriftens kapittel 7, III og IV.[218] I kapittel 7, III er det gjort unntak som innebærer at behandling av personopplysninger som i utgangspunktet er underlagt konsesjonsplikt, er unntatt fra både konsesjons- og meldeplikt. Dette gjelder:

- Sensitive kundeopplysninger, § 7-14;
- Foreningers medlemsopplysninger, § 7-15;
- Personellregistre mv, § 7-16;
- Personopplysninger om offentlige representanter, § 7-17;
- Domstolenes behandling av personopplysninger, § 7-18;
- Tilsynsmyndighetens behandling av personopplysninger, § 7-19;
- Elev- og studentopplysninger ved skoler og universiteter mv, § 7-20;
- Opplysninger om barn i barnehager og skolefritidsordninger, § 7-21.

I flere av de tilfellene som er listet opp ovenfor (§§ 7-14 – 7-16, 7-20 og 7-21), blir det stilt nærmere vilkår for at unntak skal gjelde. I alle disse tilfellene er vilkår knyttet til det rettslige grunnlaget for behandlingen, og i de fleste tilfelle er unntaket betinget av at behandlingen er basert på samtykke. Også andre vilkår vedrørende formål og den saklige begrunnelsen for behandlingen er trukket inn.

I avsnitt IV er det gjort unntak fra konsesjonsplikten, og i stedet gitt en meldeplikt i samsvar med pol § 31. Dette gjelder:

- Klientregistre mv, § 7-23;
- Hvitvaskingsregistre og tilknyttet behandling av personopplysninger, § 7-24;
- Behandling av pasientopplysninger hos helse- og sosialpersonell som ikke er underlagt offentlig autorisasjon eller gitt lisens, § 7-25;
- Behandling av pasientopplysninger hos helsepersonell som er underlagt offentlig autorisasjon eller gitt lisens, § 7-26;
- Forskningsprosjekter, § 7-27.

I fire av de bestemmelsene som er listet opp ovenfor, er unntaket betinget av at nærmere angitte vilkår er oppfylt. For forskningsprosjekter (§ 7-27) er vilkårene spesielle ved at de bl.a. involverer tilråding fra personvernombud, eventuelt de medisinske forskningsetiske komiteene (REK), omfag og varighet av forskningsprosjektet og anvendt forskningsmetode.

---

[217] Unntaket gjelder behandlinger i organ for stat eller kommune når behandlingen har hjemmel i egen lov.

[218] I § 33 fjerde ledd er det gjort felles unntak for konsesjonsplikt etter både første og annet ledd. Dette unntaket blir omtalt senere i dette avsnittet.

I tillegg til unntakene fra konsesjonsplikten, er plikten til å søke konsesjon *utvidet* i forskriften kapittel 7 avsnitt I. Dette gjelder visse typer behandling av personopplysninger i telesektoren, forsikringsbransjen og i banker og finansieringsinstitusjoner, se §§ 7-1 – 7-3.

I samme del av forskriften er Datatilsynet gitt kompetanse til å dispensere fra unntakene fra konsesjons- og meldeplikten (jf. ovenfor) "dersom særlige grunner tilsier det". Datatilsynets kompetanse gjelder i forhold til de fleste av unntaksbestemmelsene som vi ovenfor har listet opp.[219] Kompetansen gjelder bare i forhold til enkeltsaker og forutsetter således en prosessledende enkeltavgjørelse. Det er ikke gitt en eksplisitt klagerett i forhold til slike avgjørelser, tilsvarende det som gjelder for forhåndsavgjørelse om konsesjonsplikt etter pol § 33 annet ledd, jf. § 42 siste ledd, se avsnitt 9.4.5 (nedenfor). Dersom hovedtrekkene i dagens regulering beholdes, mener vi det er grunn til å vurdere om det bør være klagerett også i forhold til Datatilsynets bruk av nevnte dispensasjonsadgang.

### 9.4.3 Konsesjonsplikt ut i fra en konkret vurdering

I tillegg til konsesjonsplikten for behandling av sensitive personopplysninger, er det i § 33 andre ledd gitt en mulighet for Datatilsynet til å kreve konsesjonsbehandling:

> Datatilsynet kan bestemme at også behandling av annet enn sensitive personopplysninger krever konsesjon, dersom behandlingen ellers *åpenbart vil krenke tungtveiende personverninteresser*. I vurderingen av om konsesjon er nødvendig, skal Datatilsynet bl.a. ta hensyn til personopplysningenes art, mengde og formålet med behandlingen. (vår kursiv)

Bestemmelsen hjemler bare at det ved *enkeltavgjørelse* kan bestemmes at en behandling skal underlegges konsesjonsplikt, og Datatilsynet kan ikke avgjøre at bestemte kategorier behandlinger skal omfattes.

Bestemmelsen sier ikke noe om til hvilket tidspunkt Datatilsynet kan treffe slik avgjørelse. På den ene side kan ikke Datatilsynet treffe slik avgjørelse før saken er tilstrekkelig opplyst, jf. prinsippet om forsvarlig saksbehandling og utredningsprinsippet. Kravet til *åpenlys* krenkelse av personvernet, innebærer her begrensninger. Datatilsynet kan ikke treffe avgjørelse om konsesjonsplikt ut i fra en forutanelse eller frykt om slike krenkende effekter. På den andre side, er det uklart hvor lenge Datatilsynet kan vente med å stille krav om konsesjonsbehandling. Spørsmålet må i utgangspunktet ses i sammenheng med meldeplikten. Siden melding må være gitt minst 30 dager før vedkommende behandling av personopplysninger begynner, innebærer dette trolig at Datatilsynet ofte vil ha minst 30 dager på seg for å vurdere om det skal stilles krav til konsesjon. Når 30 dager har gått, har den behandlingsansvarlige imidlertid rett til å starte behandlingen. Det er tvilsomt om Datatilsynet har kompetanse til å ilegge konsesjonsplikt etter dette tidspunktet. Det samme må trolig gjelde dersom behandlingen er fritatt fra meldeplikt, slik at Datatilsynet ikke får kjennskap til behandlingen før den har startet.

Ileggelse av konsesjonsplikt for en pågående behandling av personopplysninger, vil prinsipielt sett ikke gjelde en *forhåndstillatelse* slik loven legger opp til. Vi går ikke her nærmere inn på spørsmålene om hvor lenge Datatilsynet kan vente med å treffe avgjørelse med hjemmel i § 33 annet ledd. Dersom en skulle velge å beholde hovedtrekkene i dagens regulering, bør spørsmålet imidlertid avklares nærmere i loven.

[219] Dispensasjonsadgangen gjelder ikke §§ 7-18 til 7-20, 7-26 og 7-27.

Selv om en skulle komme frem til den konklusjon at konsesjonsplikten etter § 33 annet ledd ikke kan benyttes etter at behandlingen har kommet i gang, kan Datatilsynet uansett gi pålegg i medhold av pol § 46. Mulighetene for å sette vilkår i samsvar med § 35 om vilkår for konsesjon, er imidlertid videre enn kompetansen etter § 46, fordi § 35 hjemler mer enn en ren lovlighetskontroll.

Vilkåret for å etablere konsesjonsplikt etter § 33 annet ledd er at "behandlingen […] åpenbart vil krenke tungtveiende personverninteresser". Kravene er med andre ord strenge, men samtidig skjønnsmessige. I loven stilles det opp retningslinjer for hva det kan legges vekt på, og særlig trekkes art, mengde og formål inn som eksempler på relevante momenter. Om dette uttaler departementet i forarbeidene:

> […] bestemmelsen er ment å være en sikkerhetsventil for ekstraordinære tilfeller. […]. Blant annet skal det tas hensyn til formålet med behandlingen. Behandlingsformål som kan få direkte virkning for de registrerte, som f eks kontrollformål, kan tale for konsesjonsplikt. Det samme gjelder tilfeller der det samles inn og sammenstilles en stor mengde opplysninger om enkeltpersoner.[220]

Spørsmålet om Datatilsynets rett til å fastsette konsesjonsplikt etter § 33 annet ledd ble behandlet av Personvernnemnda i sak 2005 nr. 11 om bomstasjoner og veibetaling. Nemnda uttalte i denne sammenheng at

> Datatilsynet har valgt å se saken fra en prinsipiell synsvinkel som fremhever generelle rettspolitiske aspekter ved avgjørelsen, og som også griper langt utover den konkrete saken. I et slikt perspektiv finner Personvernnemnda det lite tvilsomt at Datatilsynet har hjemmel til ved enkeltvedtak etter personopplysningsloven § 33, 2.ledd å kvalifisere systemet som konsesjonspliktig.

Uttalelsen innebærer en vektlegging av at avgjørelsen om å fastsette konsesjonsplikt berører prinsipielt viktige spørsmål, noe som ikke klart kommer frem i forarbeidene til bestemmelsen.

I tillegg er det åpenbart at lovens formålsbestemmelse kan få betydning for forståelsen av hva som skal regnes som "personverninteresser" i § 33 annet ledd, jf. § 1. Til formåls-bestemmelsen er det i forarbeidene videre vist til domstolspraksis, rettsteori og administrative avgjørelser. Vi kommer ikke her nærmere inn på hvor grensene for Datatilsynets kompetanse til å fastsette konsesjonsplikt etter § 33 annet ledd må trekkes. Samtidig som terskelen for å benytte bestemmelsen er høy, mener vi at Datatilsynet uansett har et ikke ubetydelig manøvreringsrom ved anvendelsen av denne bestemmelsen. Det er imidlertid viktig at praksis er lojal i forhold til formålsbestemmelsen, og at det kan konstateres å være konsekvent praksis over tid.

### 9.4.4 Felles unntak fra konsesjonspliktene etter § 33 første og annet ledd

Loven gjør et felles unntak for konsesjonsplikt etter § 33 første og annet ledd, når den i fjerde ledd fastsetter at konsesjonsplikt ikke gjelder "for behandling av personopplysninger i organ for stat eller kommune når behandlingen har hjemmel i egen lov". Ovenfor i avsnitt 6.3 har vi diskutert hjemmelskravet i forhold til kravet om rettslig grunnlag i §§ 8 og 9. I forarbeidene uttalte Justisdepartementet seg om hjemmelskravet etter § 33 fjerde ledd:

[220] Jf. Ot.prp. nr. 92 (1998–99) s. 129.

> For at et personregister skal være fritatt for konsesjon i medhold av denne bestemmelsen, kreves det at det eksplisitt fremgår av loven at det skal eller kan føres et register. Det er ikke tilstrekkelig at en særlov hjemler en aktivitet som gjør opprettelse av et personregister nødvendig. Selv om et register et fritatt fra konsesjonsplikt i medhold av bestemmelsen her, vil personopplysningsloven supplere den aktuelle særloven hvis ikke noe annet uttrykkelig fremgår av denne, jf. § 5 i lovforslaget.[221]

Hjemmelskravet er med andre ord trolig noe strengere her enn etter § 8 første ledd og § 9 første ledd bokstav b. Det at departementet bruker benevnelsen "personregistre", har ikke betydning for forståelsen av lovens formulering av "for behandling av personopplysninger", og innebærer ingen innsnevring. Lovens ordlyd i § 33 fjerde ledd ble endret av Justiskomiteen og "behandling av personregistre" erstattet med "behandling av personopplysninger" for å markere at unntaket gjelder generelt og er uavhengig av hvorledes personopplysningene er organiserte.[222]

Unntaket for konsesjonsplikt for behandling av personopplysninger som har eksplisitt hjemmel i lov, er for så vidt overflødig, fordi lex spesialis-prinsippet vil føre til samme resultat. Likevel er det pedagogiske grunner til å holde på formuleringen. Prinsippet om spesielle lovers forrang framfor generelle lover, gjelder imidlertid allment, og er ikke begrenset til lover som gjelder "organ for stat eller kommune". Dersom det i lov for eksempel ble gitt hjemmel for å behandle personopplysninger innen en viss bransje, vil også denne hjemmelen innebære at den spesielle lovhjemmelen gikk foran konsesjonsplikten i henhold til pol § 33. Forsikringsselskaper er for eksempel pålagt å føre et livforsikringsregister i samsvar med § 17-1 i forsikringsavtaleloven.[223] Dersom slike registre skulle inneholde sensitive personopplysninger som dekkes av hjemmelen, kunne konsesjonsplikten ikke gjøres gjeldende uten forbehold. De fleste lovhjemler vedrørende behandling av personopplysninger gjelder imidlertid offentlig sektor, så formuleringen i § 33 fjerde ledd regulerer uansett de mest praktisk viktige tilfellene. Dersom en velger å beholde hovedtrekkene i dagens konsesjonsordning, er det grunn til å velge en formulering som mer generelt gir uttrykk for lex spesialis-prinsippet.

### 9.4.5 Forhåndsavgjørelse om konsesjonsplikt

Den behandlingsansvarlige kan kreve at Datatilsynet tar stilling til spørsmålet om det foreligger konsesjonsplikt eller ikke, se § 33, tredje ledd. I forarbeidene er det uttalt at slike avgjørelser skal regnes som enkeltvedtak, og er gjenstand for klage, se også § 42 siste ledd. Bestemmelsen er plassert etter første og annet ledd som fastsetter konsesjonsplikt, men før fjerde ledd som gjør unntak for behandling av personopplysninger i organ for stat eller kommune og har lovhjemmel. Loven må imidlertid trolig forstås slik at forhåndsavgjørelsen kan gjelde ethvert spørsmål om eksistensen av konsesjonsplikt, herunder spørsmål knyttet til unntak fra og tillegg til konsesjonsplikt i forskrift. Dette burde imidlertid vært klart uttalt i loven, og bestemmelsen om forhåndsuttalelse burde hatt en plassering som tydeligere knytter an til alle bestemmelser vedrørende konsesjonsplikt.

I forarbeidene har departementet understreket at saken må være tilstrekkelig opplyst for at forhåndsavgjørelse skal kunne gis, jf. fvl § 17 første ledd. Dette er særlig en utfordring i forhold til konsesjonsplikt etter konkret vurdering i samsvar med § 33 annet ledd. Etter § 33

---

[221] *Ibid.*

[222] Se Innst. O. nr. 51 (1999–2000) s. 16–17.

[223] Lov 16. juni 1989 nr. 69.

første ledd blir spørsmålet kun om det skal behandles sensitive personopplysninger som ikke er unntatt i forskriften,[224] mens vurderingen etter annet ledd er langt mer åpen og skjønnspreget.

Bestemmelsene om bindende forhåndsavgjørelse gjelder bare spørsmålet om det foreligger konsesjonsplikt eller ikke, og omfatter ikke spørsmålet om konsesjon skal gis, og eventuelle vilkår for konsesjonen. I den grad Datatilsynet gir ikke bindende uttalelser i spørsmål om *innholdet* av eventuelt konsesjonsvedtak, vil den behandlingsansvarlige som får uttalelsen likevel kunne oppfatte uttalelsen som så tungtveiende at den faktisk vil bli lagt til grunn som om det var tale om et vedtak. Det samme gjelder råd som Datatilsynet gir som ledd i sin veiledningsvirksomhet, jf. pol § 42 andre ledd nr. 6. Etter vår mening kan dette gi grunn til å stille nærmere krav til hvorledes uttalelser og veiledning skal skje, for eksempel ved å kreve at råd og uttalelser alltid skal være begrunnet i lov, forskrift eller autorativ praksis. Uttalelser og råd bør dessuten alltid kunne kreves skriftlig.

### 9.4.6 Hjemler for unntak fra og tillegg til konsesjonsplikten

Et viktig unntak fra konsesjonsplikten fremgår av pol § 33 fjerde ledd. Øvrige unntak og tillegg er gitt i forskrift. Forskriftens unntak fra konsesjonsplikten er hjemlet i pol § 33 siste ledd, første setning. Tilleggene til konsesjonsplikten er hjemlet i § 31 siste ledd, jf. § 3 siste ledd som hjemler virksomhets- og bransjevise bestemmelser.

Etter vår mening er det lite tilfredsstillende at unntak fra og tillegg til konsesjonsplikten er hjemlet i forskjellige bestemmelser som ikke viser til hverandre. Hovedproblemet er imidlertid at unntakene i forskriften er så mange, og tilleggene i forskriften er så viktige, at det er lite tilfredsstillende at dette kun fremgår av forskriften. Konsesjonsplikten er et av lovens kraftigste virkemidler, som det er straffbart å bryte, jf. § 48 første ledd bokstav b. Det bør da forventes at unntak og tillegg kommuniseres på en klar måte i selve loven. Dersom en ønsker å holde fast ved hovedtrekkene i den nåværende konsesjonsordningen, kan dette for eksempel skje ved at unntakene regnes opp (enkeltvis eller i grupper), og at det vises til nærmere bestemmelser i personopplysningsforskriften. Det er her fullt mulig å benytte henvisningsteknikker som ikke gjør det nødvendig å endre loven dersom forskriften endres.

### 9.4.7 Samlet vurdering av konsesjonsplikten

#### 9.4.7.1 Generelle betraktninger og skisse to hovedelementer i en ny konsesjonsordning

Innledningsvis er det grunn til å understreke at Norge ikke er forpliktet av personverndirektivet til å ha en konsesjonsordning. Norge er bundet til direktivets definisjoner av sensitive opplysninger, men trenger ikke å benytte disse som del av en konsesjonsordning.

Hovedregelen om konsesjonsplikt er knyttet til behandling av sensitive personopplysninger. Klassifikasjonen av noe som generelt sensitivt er avhengig av kultur og politikk, og holdningene vil derfor variere over tid og mellom land. I land med mange fagorganiserte og med forholdsvis svake motsetningsforhold i arbeidslivet, vil mange for eksempel ikke oppleve

[224] Jf. også muligheten for utvidelse av konsesjonsplikten for visse bransjer, se avsnitt 9.4.2.

opplysninger om fagforeningsmedlemskap som sensitivt, jf. pol § 2 nr. 8 bokstav e. Det er dessuten åpenbart normalt mindre belastende å være åpen om seksuelle forhold i dag enn tidligere.

Meningsmålinger viser at mange mennesker er uenige i den klassifiseringen av sensitive personopplysninger som er definert i loven,[225] og at opplysningstyper som ikke regnes som sensitive i henhold til loven, oppfattes som sensitive av mange mennesker. Det er imidlertid ikke gitt at sensitivitetsspørsmålet skal følge flertallsmeningen i befolkningen. Selv om få mener at opplysninger om religion eller seksualitet er sensitive, kan det være et viktig mindretall i befolkningen der slike opplysninger oppfattes som ekstremt sensitive, og beskyttelse av opplysningstypen blir essensielt. En konsesjonsordning basert på sensitive opplysninger bør derfor ikke ensidig bli vurdert ut i fra flertallets oppfatninger. På den annen side er det viktig for en konsesjonsordnings legitimitet og oppslutning at den fremstår som rimelig balansert i forhold til dominerende oppfatninger i befolkningen.

Når en mulig fremtidig revidert konsesjonsordning skal diskuteres, er det etter vår mening grunn til å fjerne den bastante koplingen mellom konsesjonsplikt og definisjonen av sensitive personopplysninger, jf. § 2 nr. 8. Samtidig er det ikke lett å peke på andre konkrete og forhåndsbestemte kriterier som alene vil være mer treffsikre enn dagens ordning er. Etter vår mening er det grunn til å tro at den mest treffsikre konsesjonsordningen kan etableres ved å *kombinere flere teknikker*, hvorav to er i bruk i dagens regulering:

- Konsesjonsplikt på grunnlag av konkret vurdering av Datatilsynet, jf. § 33 annet ledd i dagens ordning;
- Konsesjonsplikt for bestemte bransjer mv, jf. forskriftens kapittel 7 avsnitt I;
- Konsesjonsplikt som er styrt av oppfatninger hos sammenslutninger av berørte enkeltpersoner (nytt forslag, se avsnitt 9.5).

De tre nevnte teknikkene for fastsettelse av konsesjonsplikt, innebærer at konsesjonsplikten knyttes til vurderinger på tre ulike samfunnsplan. For det første på *regjeringsnivå*, ved at konsesjon for visse bransjer mv. bør være knyttet til forskriftsmyndighet lagt til Kongen i Statsråd. For det andre på *tilsynsnivå*, ved at Datatilsynet fortsatt får kompetanse til å fastsette konsesjonsplikt i det enkelte tilfelle. For det tredje mener vi konsesjonsplikt også bør kunne etableres på *"befolkningsnivå"*, dvs. som et resultat av initiativ fra personer som vil bli berørt av den planlagte behandlingen av personopplysninger. Avgjørende for om denne sist nevnte måten å etablere konsesjonsplikt på kan bli vellykket, er selvsagt de nærmere krav som stilles med hensyn til oppslutningen om konsesjonskrav. Det er bl.a. selvsagt nødvendig å stille så strenge krav at en stenger for "kverulanter" og mindre aksjonsgrupper.

Vi kommer tilbake til detaljer i en mulig "folkelig" etablering av konsesjonsplikt i avsnitt 9.5, der vi fremmer og kommenterer forslag til nye regler om melde- og konsesjonsplikt. Her vil vi imidlertid understreke betydningen av ordninger som viser at personopplysningsloven er til for folk flest, og et instrument for å ivareta personvernhensyn som folk konkret mener er viktige. En følelse av "eierskap" til loven, vil uansett styrke legitimiteten og oppslutningen om loven. Dessuten vil regler som innebærer at konsesjonsplikt kan etableres på et folklig nivå innebære en langt større grad av treffsikkerhet enn etter dagens ordning. Dette gjelder særlig dersom vilkårene for en slik ordning er så strenge at konsesjonsplikt krever bred oppslutning om at konsesjonsbehandling er ønskelig.

[225] Se Ravlum 2005a tabell 4.1.

#### 9.4.7.2 Spesielt om hensynet til rettssikkerhet og forutberegnelighet

I mandatet for denne utredningen blir hensynet til forutberegnelighet for den behandlingsansvarlige spesielt nevnt. Vi ønsker derfor å gjøre en tydelig vurdering av dette aspektet ved en fremtidig konsesjonsordning, og har valgt å drøfte de tre skisserte komponentene i vårt forslag til fremtidig endret konsesjonsordning spesielt med tanke på forutberegnelighet. Vi ser forutberegnelighet som et utslag av rettssikkerhetsidealet, og vil understreke behovet for generelt å vurdere om den totale myndighetsordningen knyttet til personopplysningsloven og -forskriften, kan sies å være tilfredsstillende vurdert ut i fra dette idealet. Siden mandatet ikke inneholder rettssikkerhetsspørsmål som et generelt punkt, vil vi imidlertid nøye oss med å gi enkelte synspunkter på rettssikkerheten knyttet til konsesjonsplikten.

Konsesjonsplikt som stilles opp ut i fra tilsynsmyndighetens konkrete vurdering har den fordelen at det kan gi stor grad av fleksibilitet og treffsikkerhet. På den annen side gir den i utgangspunktet lite forutberegnelighet for de behandlingsansvarlige. Dette problemet kan imidlertid etter vår mening reduseres klart over tid dersom Datatilsynet får en nærmere plikt til å *begrunne* hvorfor en behandling blir underlagt konsesjonsplikt, samtidig som avgjørelsene *publiseres* og blir allment tilgjengelige. Det vil da etter hvert kunne danne seg mønstre som tydeliggjør hvilke kriterier Datatilsynet har lagt vekt på i tidligere saker. Likevel kan det ikke unnslås at det uansett vil gjenstå en ikke ubetydelig usikkerhet, bl.a. fordi det stadig vil kunne legges nye kriterier til grunn for en avgjørelse om å pålegge konsesjonsplikt etter en konkret vurdering. En konsesjonsordning som *bare* er basert på Datatilsynets konkrete skjønn, vil derfor etter vår mening neppe tilfredsstille de krav som bør stilles til forutberegnelighet. Omfanget av en slik konsesjonsplikt bør derfor ikke være for stor, og antagelig ikke større enn etter dagens regler, jf. avsnitt 9.4.3 (ovenfor).

Konsesjonsplikt basert på en angivelse av hvilke bransjer, virksomhetsområder mv. som skal undergis konsesjonsplikt, vil lett gi stor grad av forutberegnelighet. Dette er i alle fall tilfellet dersom en i bestemmelsene evner å klart angi hvilke bransjer mv. det er tale om. Hensynet til forutberegnelighet tilsier at konsesjonsplikten går tydelig frem av selve *lov*teksten. Så lenge loven inneholder en klar hjemmel som også angir materielle rammer for nærmere bestemmelser, bør slike bestemmelser imidlertid kunne plasseres i forskriften til loven. Loven kan med andre ord bestemme at bestemte bransjer kan ilegges konsesjonsplikt i henhold til forskrift, og forskriften angir hvilke bransjer dette er.

En konsesjonsplikt som er basert på et folkelig initiativ, kan etter vår mening utformes på en måte som gir stor grad av forutberegnelighet. I det forslaget til ny lovtekst vi foreslår i neste avsnitt, inngår en bestemmelse som sikrer at berørte personer blir varslet om behandlingsansvarliges planer om å starte behandling av personopplysninger. Slikt varsel i kombinasjon med nevnte konsesjonsbestemmelse, kan bidra til at den behandlingsansvarlige innleder dialog med berørte personer før melding til Datatilsynet sendes. I så fall vil eventuelle innsigelser og argumenter komme for en dag, og den behandlingsansvarlige kan på forhånd bedømme sannsynligheten for at berørte personer vil mobilisere for å kreve konsesjonsbehandling. Slik vil en kunne oppnå en stor grad av forutberegnelighet samtidig som en legger til rette for lokale løsninger basert på forhandlinger mellom den behandlingsansvarlige og berørte personer (eventuelt ved deres representanter).

En konsesjonsordning basert på de tre nevnte teknikkene for etablering av konsesjonsplikt vil etter vår mening kunne gi en fullt ut tilfredsstillende forutberegnelighet. Dette gjelder i alle

fall så lenge ikke det relative antallet konsesjonsplikter basert på Datatilsynets konkrete vurderinger blir for stort.

I tillegg til forutberegnelighet er det etter vår mening grunn til generelt å legge større vekt enn i dagens lov på rettssikkerhet mer generelt. Dette gjelder både ved på viktige punkter å tydeliggjøre at forvaltningslovens bestemmelser kommer til anvendelse, og ved å stille opp særlige saksbehandlingsregler med garantier for den enkelte behandlingsansvarlig i bestemte sakstyper. Særlig bør det være aktuelt å ha nærmere saksbehandlingsregler knyttet til konsesjonsbehandling og Datatilsynets kontrollvirksomhet. Vi har allerede nevnt behovet for begrunnelse i saker der Datatilsynet etablerer konsesjonsplikt for konkrete behandlinger av personopplysninger. Vi mener dessuten det kan være grunn til å se nærmere på praksis vedrørende forhåndsvarsling av parter, jf. fvl § 16. Dette gjelder særlig varsling av personer som er eller vil bli "registrert" i den behandling det er søkt konsesjon for eller som på annen måte er berørt av vedtak Datatilsynet treffer i henhold til § 46, og deres anledning til å bli hørt før saken avgjøres, jf. fvl § 17.

## 9.5 Forslag til endrede bestemmelser vedrørende melde- og konsesjonsplikt

### 9.5.1 Innledning

Nedenfor fremmer vi to alternative forslag til endrede bestemmelser om konsesjons- og meldeplikt. Vi mener de beste grunner taler for vårt omfattende forslag i avsnitt 9.5.2. Det moderate forslaget i avsnitt 9.5.3 kan nok sies å innebære en forbedring i forhold til dagens situasjon, fordi ordningen trolig blir mer treffsikker også med denne løsningen. Det omfattende forslaget vil imidlertid etter vår mening ha langt bedre effekt fordi den innebærer at melde- og konsesjonsplikt blir en enhetlig ordning, og fordi konsesjonsplikten i en viss grad bli "demokratisert". Det demokratiske elementet gjør at konsesjonsordningen både kan "føle folk på pulsen", samtidig som andre elementer i forslaget som er basert på myndighetsvurderinger, også sikrer en prinsipiell holdning til når konsesjonsplikt skal inntre.

### 9.5.2 Omfattende forslag

I det følgende bruker vi henvisninger til paragrafer i samsvar med nummereringen i vårt omfattende forslag. Dette forslaget innebærer en integrering av melde- og konsesjonsplikten, på den måten at innsendt melding kan foranledige krav om konsesjonsbehandling i samsvar med § 33a. Meldeplikten har i tillegg en selvstendig og forsterket betydning. Dette skyldes at meldingens innhold endres og forenkles kraftig, slik at meldingen viser til dokumenter som inneholder de opplysningstyper som det i dag spørres om i gjeldende § 32. Samtidig blir dette en melding om at den behandlingsansvarlige har gjennomført sentrale forpliktelser i henhold til loven (se §§ 13 og 14). Forslaget gjør det imidlertid nødvendig å supplere kravene i §§ 13 og 14, slik at samspillet med meldepliktbestemmelsene blir tilfredsstillende.

Forslaget innebærer også at det innføres en enkel plikt for den behandlingsansvarlige til å varsle personer som vil bli berørt av den planlagte behandlingen, om at melding er sendt til Datatilsynet.

Forslaget innebærer en noe større lovtekst vedrørende melde- og konsesjonsplikt enn etter dagens lov. Samtidig reduseres imidlertid forskriftsreguleringen av melde- og konsesjonsplikt radikalt, noe som samlet sett innebærer en klart redusert tekstmengde.

Vi har lagt vekt på å utforme bestemmelsene som en oppskrift på hvorledes bestemmelsene skal ses i sammenheng, bl.a. ved at bestemmelsene står i riktig rekkefølge i forhold til kravene til riktig anvendelse, og ved at det gis tydelige henvisninger til andre bestemmelser, samt tydelige anvisninger på den vilkårstrukturen som skal prøves.

**§ 31 Plikt til å melde og varsle om ny behandling av personopplysninger**

Den behandlingsansvarlige skal gi melding til Datatilsynet om behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler.

Varsel om at meldingen er sendt, skal gis til personer som vil bli berørt av den behandlingen av personopplysninger som meldes. Gjelder behandlingen et stort eller ubestemt antall personer, skal varselet gis til relevante interesseorganisasjoner eller meddeles allmennheten på hensiktsmessige måter.

Melding og varsel skal gis senest 30 dager før behandlingen tar til. Datatilsynet skal gi den behandlingsansvarlige kvittering for at melding er mottatt.

Kongen kan gi forskrift om unntak fra melde- og varslingsplikt etter §§ 31 og 31a, og om innholdet i meldinger og varsler etter § 32. Datatilsynet kan gi nærmere regler vedrørende den praktiske gjennomføringen av melde- og varslingsplikten, jf. §§ 31 – 32.

**§ 31a Plikt til fornyet melding og varsel**

Ny melding og nytt varsel må gis dersom det skjer endringer i:

a) hvem som har behandlingsansvaret og på hvilken måte ansvaret eventuelt er delt (§ 7), eller
b) det rettslige grunnlaget for behandlingen (§§ 8 – 8d), eller

c) formålet med behandlingen (§ 9), eller

d) dersom opplysninger blir utlevert til andre enn det tidligere opplyst om.

Selv om det ikke har skjedd endringer, skal det gis ny fullstendig melding tre år etter at forrige melding ble gitt, jf. § 31.

**§ 32 Meldingens og varselets innhold**

Meldingen skal inneholde bekreftelse av at det foreligger dokumentasjon vedrørende behovet for å iverksette tiltak for å

a) sikre personopplysninger i samsvar med § 13, og

b) sikre etterlevelse av lov, forskrift mv. i samsvar med § 14 om internkontroll, jf. likevel § 27a om unntak fra krav om internkontroll for virksomheter med personvernombud.

Det skal videre opplyses om det er fremkommet protester mot den planlagte behandlingen fra organisasjoner som representerer de registrerte personene. Det skal eventuelt kort gjøres rede for slik uenighet, og hvem som har fremmet synspunktene.

Varselet skal gi opplysning om at:

a) melding er sendt til Datatilsynet, og

b) at det eksisterer rett til å kreve konsesjonsbehandling i samsvar med § 33a.

**§ 33 Datatilsynets rett til å kreve konsesjonsbehandling**

Datatilsynet kan etter en konkret vurdering bestemme at behandling av personopplysninger krever konsesjon. Konsesjonsplikt kan bare pålegges dersom det er fare for at behandlingen kan krenke tungtveiende personverninteresser, jf. § 1.

Avgjørelse om plikt til å søke konsesjon skal behandles etter reglene for enkeltvedtak, se forvaltningsloven (fvl) kapittel IV – VI.

Avgjørelse i samsvar med første ledd skal begrunnes, jf. fvl § 25. Ved vurdering av om konsesjonsplikt skal pålegges, kan Datatilsynet bl.a. ta hensyn til om det skal behandles sensitive personopplysninger (jf. § 2 annet ledd), om behandlingen gjelder en gruppe personer med spesielt behov for beskyttelse, om personopplysninger skal sammenstilles fra flere kilder, formålet med behandlingen og mengden personopplysninger.

Den behandlingsansvarlige kan kreve at Datatilsynet avgjør om en behandling vil kreve konsesjon.

Datatilsynet kan gi nærmere regler vedrørende den praktiske gjennomføringen av konsesjonsplikten, jf. §§ 33 – 33b.

**§ 33a Registrerte personers rett til å kreve konsesjonsbehandling**

Registrerte personer eller deres valgte representanter kan kreve at Datatilsynet fastsetter konsesjonsplikt for behandling av personopplysninger. Datatilsynet skal konsesjonsbehandle saken dersom:

a) det kan dokumenteres at minst 40% av de personene som det vil bli registrert personopplysninger om krever det, eller

b) en organisasjon der mer enn 60% av de registrerte er medlemmer treffer vedtak om det, eller

c) det kan dokumenteres at minst 5000 personer stiller seg bak kravet om konsesjonsbehandling.

Krav om konsesjon etter denne bestemmelsen må fremmes senest 30 dager etter at varsel fra den behandlingsansvarlige ble mottatt, jf. § 31 annet og tredje ledd. Dersom behandlingen omfatter sensitive opplysningstyper (jf. § 2 annet ledd) er fristen 60 dager. Datatilsynet skal gi den behandlingsansvarlige kvittering for at krav om konsesjonsplikt er mottatt.

Datatilsynet kan treffe vedtak om andre grenseverdier enn de som fremgår av første ledd, bokstavene a – c. Vedtaket kan bare gjøres for ett år ad gangen, og skal straks kunngjøres. Er det ikke kunngjort noe vedtak, gjelder lovens grenseverdier.

**§ 33b Konsesjonsplikt i henhold til forskrift**

Kongen kan ved forskrift fastsette at det skal kreves konsesjon for å behandle personopplysninger innen bestemte næringer, for bestemte formål, eller på bestemte måter.

Kongen kan gi utfyllende forskrifter om konsesjonsbehandling etter § 33a og unntak fra konsesjonsplikt etter § 33b.

**§ 33c Unntak fra konsesjonsplikt når behandlingen har hjemmel i lov**

Datatilsynet kan ikke nekte behandling av personopplysninger eller stille vilkår for at slik behandling kan skje dersom dette vil stride mot bestemmelse i særlov eller bestemmelse i medhold av slik lov. Det samme gjelder behandling av personopplysninger som er klart forutsatt i nevnte lover eller forskrifter.

Innenfor gjeldende lov- og forskriftsbestemmelser som nevnt i forrige ledd, kan Datatilsynet likevel treffe vedtak om supplerende tiltak som åpenbart er nødvendig for å ivareta personvernet, og som ikke hindrer realisering av lovens eller forskriftens formål.

**§ 34 Avgjørelsen av om konsesjon skal gis**

Ved avgjørelsen av om konsesjon skal gis, skal det klarlegges om behandlingen av personopplysninger kan volde ulemper for den enkelte som ikke kan avhjelpes gjennom bestemmelsene i kapitlene II-V og vilkår etter § 35. I så fall må det vurderes om ulempene blir oppveid av hensyn som taler for behandlingen.

**§ 35. Vilkår i konsesjon**

I konsesjonen skal det vurderes å sette vilkår for behandlingen når slike vilkår er nødvendige for å begrense ulempene behandlingen ellers ville medføre for den registrerte.

### 9.5.3 Moderate forslag

Vi innser at vårt forslag til demokratisering av konsesjonsordningen innebærer en uvant tilnærming. I mandatet har departementet dessuten anmodet om ett eller flere forslag som kan føre til et redusert antall konsesjonssaker. På denne bakgrunn diskuterer vi i dette avsnittet flere mulige endringsforslag. Samtidig vil vi understreke at Befolknings- og Virksomhetsundersøkelsen vedrørende personvern[226] gir grunn til radikal nytenkning, snarere enn å justere på det eksisterende konsesjonssystemet.

Den første alternative ordningen vi vil peke på, ble fremlagt som en idé på seminaret som markerte starten på dette arbeidet, se kapittel 1. Forslaget gikk ut på å kombinere elementene i dagens konsesjonsordning, dvs. ved å trekke sammen elementer fra § 33 første og annet ledd. Utgangspunktet er da:

> § 33. Konsesjonsplikt
>
> Det kreves konsesjon fra Datatilsynet for å behandle sensitive personopplysninger. Dette gjelder likevel ikke for behandling av sensitive personopplysninger som er avgitt uoppfordret.
>
> Datatilsynet kan bestemme at også behandling av annet enn sensitive personopplysninger krever konsesjon, dersom behandlingen ellers åpenbart vil krenke tungtveiende personverninteresser. I vurderingen av om konsesjon er nødvendig, skal Datatilsynet bl.a. ta hensyn til personopplysningenes art, mengde og formålet med behandlingen.

Forslaget gikk ut på å formulere vilkåret for konsesjonsplikt på lignende måte som i § 33 annet ledd, eventuelt justert slik at terskelen for konsesjonsplikt blir senket noe. En slik bestemmelse kunne lyde:

> **§ 33. Konsesjonsplikt**
>
> Det kreves konsesjon fra Datatilsynet dersom behandlingen [åpenbart] vil krenke tungtveiende personverninteresser. Dette gjelder likevel ikke for behandling av sensitive personopplysninger som er avgitt uoppfordret.[227]

Det kan virke overraskende dersom konsesjonsplikten skal avhenge av en skjønnsmessig vurdering som pliktsubjektet selv skal gjøre. På den annen side er det et typisk trekk ved loven at behandlingsansvarlige skal etterleve en rekke plikter uten forutgående kontroll fra noe tilsynsorgan. Nåværende lov inneholder dessuten bestemmelser som innebærer at plikten hviler på skjønnsmessige vurderinger med brede og åpne avveininger mellom ulike interesser. Et sentralt eksempel på dette er någjeldende § 8 første ledd bokstav f og vårt forslag til § 8c. Etter vår mening er det imidlertid avgjørende at konsesjonsplikten skal gjelde behandlinger der det eksisterer en særskilt trussel mot personvernet. Dersom denne forutsetningen blir tatt på alvor, er det neppe akseptabelt å overlate den nærmere vurderingen til den behandlingsansvarlige. Til sammenligning vil behandlingsansvarliges uholdbare vurderinger i henhold til § 8 første ledd bokstav f, nettopp kunne fanges opp av konsesjonsordningen. Slik lar øvrige skjønnsmessige vurderinger som foretas av behandlingsansvarlige seg delvis forsvare av at det i antatt alvorlige tilfelle som omfattes av konsesjonsordningen vil skje en vurdering av tilsynsmyndigheten.

---

[226] Se Ravlum (2005a) og (2005b).

[227] Mulig justering av terskelen for å kreve konsesjon er markert med klammeparentes.

Fra et administrativt (myndighets-)synspunkt, vil en konsesjonsbestemmelse som den skisserte også være uakseptabel fordi det blir helt uvisst hvor mange konsesjonssøknader en slik bestemmelse vil generere. Med det lave kunnskapsnivået som Virksomhetsundersøkelsen har gitt et bilde av,[228] ville dette trolig gi veldig få søknader. I tilfeller av nyhetssaker og "skandaler" (jf. sakene vedrørende Vinmonopolets og Redningsselskapets bruk av ansattes e-post), kunne Datatilsynet imidlertid risikere å få et ras av konsesjonssøknader. Vi anser den skisserte konsesjonsordningen, basert på § 33 første og annet ledd, som uaktuell.

En alternativ tilnærming til dagens konsesjonsordning, kan være å angi i lov og/eller i forskrift visse bransjer, institusjoner, formål eller situasjoner som skal utløse konsesjonsplikt.[229] En slik løsning gir åpenbart forutberegnelighet. Samtidig vil det åpenbart være mulig å fange opp problemstillinger som ofte vil ha særlig stor personvernmessig betydning. På den annen side vil det også med en slik tilnærming være vanskelig å fortløpende dekke alle områder som faktisk oppleves som viktige og vanskelige, i lys av den teknologiske og samfunnsmessige utviklingen. I den grad konsesjonsplikten blir angitt i forskrift, ville det kunne være mulig å oppdatere konsesjonsordningen etter hvert, men det er etter vår mening lite realistisk å tro at dette kan skje så hyppig og så raskt at det vil kunne gi en tilfredsstillende ivaretakelse av personvernet. Vi ønsker derfor å gi klart uttrykk for at en ordning som bare er basert på positiv angivelse av konsesjonsplikt, ikke innebærer en tilstrekkelig fleksibel og treffsikker ordning.

I den grad en velger konkret og positiv angivelse av konsesjonsplikt, mener vi dette bør kombineres med en bestemmelse av samme type som dagens § 33 annet ledd. Vi tror den beste løsningen vil være å angi noen få og åpenbare kategorier av konkret angitt konsesjonsplikt, som kombineres med en kompetanse for Datatilsynet til å treffe vedtak om konsesjonsplikt i enkelttilfelle. Dersom en velger å være tilbakeholdene og ikke spesifisere et større antall positivt angitte konsesjonsplikter, bør Datatilsynets kompetanse utvides noe i forhold til dagens § 33 annet ledd. Vi har ikke kunnet prioritere en kartlegging og gjennomtenkning av hvilke bransjer mv. som kan være aktuelle for konsesjonsplikt, og begrenser oss derfor til å vise hvorledes annet ledd om Datatilsynets kompetanse kan lyde, og samspille med et første ledd som inneholder forskriftshjemmel for positiv angivelse av behandlinger som er underlagt konsesjonsplikt:

> **§ 33. Konsesjonsplikt**
>
> Det kreves konsesjon fra Datatilsynet for å behandle slike personopplysninger som er omfattet av personopplysningsforskriften kapittel [xx] (forskrift av 15. desember 2000 nr. 1265). Slike forskrifter fastsettes av Kongen.
>
> Dersom behandlingen vil krenke tungtveiende personverninteresser, eller behandlingen gjelder spørsmål av stor prinsipiell betydning (jf. § 1), kan Datatilsynet bestemme at også behandling av andre personopplysninger må ha konsesjon. Slike avgjørelser kan bare treffes som enkeltvedtak, jf. forvaltningsloven § 2 første ledd, bokstav b, jf. bokstav a.

Utformingen av første ledd er spesiell ved at den direkte sier hvor bestemmelser vedrørende konkrete konsesjonsplikter finnes. Hjemmelen til å gi slike forskrifter er plassert i direkte

[228] Se Ravlum 2005b.

[229] Se f.eks. personuppgiftslag (1998:204) 41 §.

samband med dette, for å sikre god saklig sammenheng mellom angivelsen av hvor konsesjonsplikter skal være plassert og hjemmelen til å gi forskrifter om konsesjonsplikt.

Første del av annet ledd er ment å dekke de konkrete vurderingene vedrørende effekter for registrerte personer. Annet ledd er ment å dekke tilfeller der behandlingen kan ha konsekvenser ut over den konkrete saken, for eksempel fordi den kan ha en uønsket smitteeffekt, fordi den representerer introduksjon av ny og kontroversiell teknologi eller lignende. Etter vår mening er det ikke grunn til å angi hva Datatilsynet skal vektlegge, på en måte som er så detaljert som i dagens lov ("skal Datatilsynet bl.a. ta hensyn til personopplysningenes art, mengde og formålet med behandlingen"). Ved å vise til lovens formålsbestemmelse gir en etter vår mening tilstrekkelig informasjon om hvilken vurdering Datatilsynet foretar, samtidig som det ikke legges føringer eller skjer innskrenkninger med hensyn til de vurderinger som kan skje.

Etter vår mening er det ikke store betenkeligheter knyttet til en utvidelse av Datatilsynets kompetanse på området. Datatilsynet vil uansett ha en presset arbeidssituasjon der de må gjøre klare prioriteringer mellom ulike oppgaver. Konsesjonsbehandling vil derfor neppe bli krevet i utrengsmål. Konsesjonsplikt vil trolig etableres i saker der Datatilsynet ofte vil avslå konsesjon eller stille strenge vilkår for å gi forhåndstillatelse. En videre kompetanse for tilsynet til å kreve konsesjonsbehandling, kan derfor hevdes å gi stor makt til Datatilsynet. Personvernnemnda kan imidlertid overprøve alle vedtak Datatilsynet treffer. Uansett vil en restriktiv praksis i Datatilsynet og Personvernnemnda kunne stimulere til igangsetting av politiske prosesser og endret lovgivning.[230] Slik uenighet og demokratisk debatt må uansett ses på som positivt.

[230] Det er f.eks. gitt politiske signaler om en mulig lovregulering etter at Datatilsynet ikke tillot dopingkontroll på treningsentre, jf. sak 05/01598-6 /RVB, 2. mars 2006.

# Kapittel 10

## Frivillige ordninger – personvernombud, bransjevise atferdsnormer

### 10.1 Om mandatet

I rammen gjengir vi mandatets punkt 9 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

*Frivillige ordninger – personvernombud, bransjevise atferdsnormer*

Personopplysningsforskriften § 7-12 gir regler om personvernombud. Datatilsynet kan gjøre unntak fra lovens meldeplikt dersom den behandlingsansvarlige utpeker et uavhengig personvernombud som skal sikre at loven med forskrift blir fulgt. Ordningen vurderes som positiv og bidrar til å styrke personvernet hos den behandlingsansvarlige og bør styrkes. Utrederne bes vurdere **om lovverket kan utformes slik at det i større grad enn i dag oppmuntrer den behandlingsansvarlige til å ta personvernombudsordningen i bruk**. Et virkemiddel som kan vurderes i denne forbindelse, er unntak fra konsesjonsplikten. **Personvernombudets rettslige stilling** og hva slags rettslig forhold det skal eller bør være mellom ombudet og Datatilsynet må også vurderes.

Departementet ber utrederne **vurdere om det kan etableres andre frivillige tiltak eller ordninger som tilsier at det gjøres unntak fra lovens meldings- eller konsesjonsplikt**. Et aktuelt tiltak kan være bransjevise adferdsnormer som sikrer at lov og forskrift følges opp av behandlingsansvarlige.

Vi forstår mandatet slik at den nåværende ordningen med personvernombud skal være utgangspunkt for drøftelsen, samtidig som forslag til endringer ikke nødvendigvis skal bygge direkte på den ordning som i dag gjelder. Mandatet gir også rom for å foreslå flere ombudsmannsordninger som er parallelle. Som tidligere understreket, mener vi dessuten det er viktig å skape så gode sammenhenger mellom de ulike ordningene som mulig. Særlig gjelder dette forholdet mellom meldeplikt, konsesjonsplikt, personvernombud og bransjenormer.

### 10.2 Dagens ordning med personvernombud

Viktige aspekter ved dagens ordning med personvernombud er beskrevet i avsnitt 2.5.8. For å ivareta sammenheng og lesevennlighet, har vi imidlertid valgt å gjenta (justerte) deler av denne teksten her, samtidig som den er supplert og presisert i forhold til de behov som drøftelsen i dette avsnittet begrunner.

Ordningen med personvernombud er introdusert i pof § 7-12, dvs. i det kapittelet av forskriften som gjelder unntak fra meldeplikt (kapittel 7 avsnitt II). Oppnevning av ombudet er her satt inn som et mulig alternativ til meldeplikt:

§ 7-12

Datatilsynet kan samtykke i at det gjøres unntak fra meldeplikt etter personopplysningsloven § 31 første ledd, dersom den behandlingsansvarlige utpeker et uavhengig personvernombud som har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet skal også føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32.

Som det fremgår av pof § 7-12 er det ingen automatikk i at oppnevning av personvernombud skal gi lettelse i meldeplikten (”kan samtykke”). Forskriften stiller som krav at personvernombudet skal være ”uavhengig”, men det går ikke frem av selve forskriften hva som ligger i dette, og det gis heller ingen nærmere beskrivelse av ombudets arbeidsområde og funksjon. I kgl. res. 15. desember 2000 nr. 1265 (om personopplysningsforskriften) er det gitt kommentarer til den enkelte forskriftsbestemmelse, herunder § 7-12. Det er her sagt at ombudet skal være en fysisk person, og skal ha ansvar på et ”bestemt og begrenset område”. Det heter videre at ombudet skal ”føre fortegnelser over behandlinger og behandlingsansvarlige, kontrollere den behandlingsansvarliges behandlinger og bistå de registrerte med å ivareta sine rettigheter etter personopplysningsloven og forskrifter …”.

Det er vanskelig å ha noen sikker formening om hva som ligger i ”bestemt og begrenset område”, når dette står sammen med ”føre fortegnelser over … behandlingsansvarlige”. Dette åpner tilsynelatende for fag- eller bransjespesifikke ombud, dvs. ombud som er felles for flere behandlingsansvarlige. Forskriften må imidlertid forstås slik at ombudet også kan omfatte én behandlingsansvarlig. Det sier seg selv at ombud kun er aktuelt når den behandlingsansvarlige er en virksomhet (juridisk person), og i praksis vil det være behandlingsansvarlige med et viss omfang og kompleksitet i sin behandling av personopplysninger som særlig vil være aktuelle. Dette kan innebære at aktuelle behandlingsansvarlige har mange ansatte, men det trenger ikke å være tilfellet. Det kan også være aktuelt å ha personvernombud i virksomheter med mange registrerte (og – eventuelt – få ansatte).

I mars 2006 var det i følge Datatilsynets hjemmeside i alt 21 personvernombud. Av disse var 19 interne, dvs. ombudet var ansatt hos den behandlingsansvarlige. I to tilfelle var det eksterne ombudsordninger, dvs. ombudet var knyttet til en annen organisasjon enn den behandlingsansvarlige. Størst av disse er Norsk Samfunnsvitenskapelige Datatjeneste A/S (NSD) som var personvernombud for mer enn 100 forskningsinstitusjoner.[231] Et annet eksternt ombud er en person i firmaet It-Con A/S, et selskap som selger spill og tilbehør til mobiltelefoner.[232] Hos NSD er selve ombudsrollen formelt knyttet opp til en bestemt person (direktøren), men det fremgår av annen informasjon at det er NSD som sådan som har denne funksjonen. Hos It-Con er det ikke publisert noen informasjon om hvem som fungerer som personvernombud, og det er heller ikke gitt annen informasjon om ordningen.

Det samlede antallet virksomheter som er knyttet til en ombudsordning, var ca. 130. De langt fleste av disse var forskningsinstitusjoner knyttet til NSD (mer enn 100). Andre virksomhetsområder av betydning utenfor det som hører til NSD, gjelder helsestell og et mindre antall kommuner. Bortsett fra Statistisk sentralbyrå, sykehus og universiteter, var det ingen store virksomheter som hadde personvernombud, verken i offentlig eller privat sektor.

---

[231] Se <http://www.nsd.uib.no/personvern/index.cfm>.

[232] Se selskapets hjemmeside, der det kun reklameres forprodukter, men ikke står noe om selskapet: <http://www.It-Con.no/>.

Vi har ikke undersøkt hvorledes hvert personvernombud er finansiert, men antar at alle interne ombud er ansatt hos den behandlingsansvarlige. Ombudsordningen ved NSD er spesiell fordi dette ombudet er eksternt i forhold til de behandlingsansvarlige forskningsinstitusjoner mv. som ordningen betjener. Her er det etablert en finansieringsmodell for medlemsorganisasjoner hos Universitets- og høgskolerådet, bestående av en basisbetaling og betaling per prosjekt.[233]

Ordningen med personvernombud er etter vår mening uklar. Slik den i dag praktiseres kan slike ombud både være eksterne i forhold til behandlingsansvarlige (NSD og It-Con A/S) og knyttet til én enkelt behandlingsansvarlig (de øvrige). I sin veileder for personvernombud, åpner Datatilsynet for både interne og eksterne ordninger, men anbefaler de interne.[234] De to typetilfellene fremstår som vidt forskjellige. For eksterne personvernombud fremstår ombudet som en ytre kontrollinstans, noe som gjør rollen som uavhengig aktør langt lettere å ha tiltro til enn dersom personvernombudet er ansatt hos den behandlingsansvarlige.

Det er også vanskelig å forestille seg hvorledes et ombud som har så mange "kunder" som NSD i Bergen kan "kontrollere den behandlingsansvarliges behandlinger og bistå de registrerte med å ivareta sine rettigheter". Dette er i alle fall urealistisk dersom ombudet skal være én person.[235] Kontrollen må uansett primært være basert på skriftlig materiale, og for at registrerte personer skal ha særlig hjelp fra ombudet med å realisere sine rettigheter, må det være opplysning om ombudets funksjon i informasjon som gis av den enkelte behandlingsansvarlig. Dernest må registrerte personer kunne ha tillit til ombudets faglige dyktighet vedrørende personvernspørsmål. En ansatt hos et firma som It-Con A/S, som ikke har noen informasjon om ombudsrollen på sine hjemmesider, kan selvfølgelig inneha betydelig kompetanse innen personopplysningsrett. Det er imidlertid et spørsmål om innbyggerne i de kommuner der personen hos dette firmaet er personvernombud kan stole på at kompetansen er tilstrekkelig. Vi har ikke gjort noen systematisk undersøkelse av hvilken informasjon som blir gitt fra behandlingsansvarlige, men i de kommuner som vi undersøkte og som hadde personvernombud knyttet til It-Con A/S, forekom ikke ordet "personvern" på kommunens hjemmeside, og ingen informasjon var gitt om ombudsordningen. I én kommune, var det informasjon om ombudsordningen i et nyhetsoppslag, og firmaet ble nevnt, men uten at det var gitt kontaktinformasjon av noe slag.

Både avstand og antall kan gjøre det vanskelig å etablere et slikt nært forhold mellom et eksternt ombud og daglig ansvarlige personer hos den behandlingsansvarlige. Det er imidlertid grunn til å tro av avstand/omfang primært vil være et problem for god kontakt mellom ombud og ansatte hos behandlingsansvarlige og – ikke minst – for kontakten mellom ombudet og personer som behandlingsansvarlige har registrert opplysninger om.

Slik personvernombudene kan være innrettet, er de dels en del av behandlingsansvarliges organisasjon, og fyller således en rolle i denne organisasjonen på linje med andre roller som loven foreskriver (daglig ansvarlig, daglig leder, sikkerhetsrevisor). De andre rollene er imidlertid ikke uavhengige, men forutsetter under- og overordningsforhold. Personvernombudet blir dermed en "frispiller" i spørsmål vedrørende arbeidsgiverens behandling av

---

[233] Etter hva vi har fått opplyst fra NSD var gjennomsnittlig kostnad per prosjekt i 2004, kr. 3200,- til 3500,-.

[234] Se Veileder for personvernombud, Datatilsynet 1. mars 2006, <http://www.datatilsynet.no/templates/Page____431.aspx>.

[235] I 2005 behandlet NSD 1917 nye meldinger om nye prosjekter og et nesten like stort antall meldinger om endring, utvidelse, og forlengelse av konsesjon. Av disse ble 1764 prosjekter ferdigbehandlet av personvernombudet, og 153 prosjekter (8 %) ble videresendt til Datatilsynet som konsesjonssøknader. Hos personvernombudet ved NSD er det referert til i alt 6 saksbehandlere knyttet til ordningen.

personopplysninger, og har alle aspekter ved personopplysningsloven og forskriften som arbeidsområde. Ordningen er imidlertid ikke bundet opp til at ombudspersonen faktisk skal ha tid/arbeidsforhold som tillater effektiv kontroll og assistanse.

Etter vår mening er forskriftens ordning med personvernombud uklar, meget mangelfullt integrert i loven og uensartet praktisert. I avsnitt 10.4 (nedenfor) foreslår vi en endret ombudsmodell. Uansett hvilken modell en velger, er det viktig å etablere ombudsmannen på en måte som klart definerer forholdet til andre aktører og roller etter loven (se avsnitt 2.5), og med klart definerte arbeidsområder og fullmakter mv.

## 10.3 Personvernombud og forholdet til personverndirektivet

Direktivet nevner mulighet for at behandlingsansvarlige kan oppnevne personvernombud ("data protection official") i artikkel 18 nr. 2. Ordningen er i denne sammenheng nevnt som et mulig vilkår for lemping eller forenkling av meldeplikt etter artikkel 18 nr. 1:

> Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
>
> – …
>
> – where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
>
> > – for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
> >
> > – for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),
>
> thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

Som påpekt i avsnitt 9.4.1 er ordningen også nevnt i forbindelse med forhåndskontroll ("prior checking") av behandlinger som innebærer særlige personvernmessige risikoer, jf. artikkel 20 nr. 2. En "data protection official" kan foreta slik forhåndskontroll og er i den forbindelse forpliktet til å rådføre seg med tilsynsmyndigheten i tvilstilfeller.

Direktivet inneholder ingen påbud om å oppnevne personvernombud, men understreker at i den grad ordningen tas i bruk, må ombudet kunne fungere uavhengig av den behandlingsansvarlige:

> such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence.[236]

Direktivet fastsetter ingen øvrige krav til ordningen.

Det er verdt å merke seg at det er stor forskjell mellom EU-/EØS-medlemsland – også innenfor Norden – når det gjelder hvorvidt de benytter seg av muligheten for en slik ordning forankret i sine respektive regelverk. Ordningen er f.eks. lite utviklet i både Finland og

[236] Fortalen punkt 49.

Danmark, men er blitt en forholdsvis viktig del av Sveriges politikk innen personopplysningsvern. Etter den svenske personuppgiftslagen faller meldeplikt helt bort dersom den behandlingsansvarlige oppnevner "ett personuppgiftsombud" (jf. 37 §, jf. 3 §).[237]

## 10.4 Vurdering av fremtidige ordninger vedrørende personvernombud

### 10.4.1 Hvem skal personvernombudet være til for?

Det er etter vår mening først nødvendig å avklare hvem en personvernombud skal være til for å bistå, og hva slags nærmere funksjon vedkommende derfor bør ha. En mulighet er å ha personvernombud som primært er Datatilsynets forlengede arm, dvs. som primært trer i stedet for myndigheten ved å påta seg oppgaver som Datatilsynet har. Registrering av meldinger, samt lovlighetskontroll av pågående behandling, er blant slike roller en kan tenke seg å gi personvernombudet. En annen mulighet er primært å se på personvernombudet som en "serviceperson" for registrerte personer, dvs. som er kontaktpunktet i kommunikasjonen med utenverdenen, og den som videreformidler og målbærer spørsmål fra registrerte og andre interesserte. En tredje mulig funksjon, er personvernombud som primært utfører interne servicefunksjoner hos den behandlingsansvarlige, for eksempel ved å ha spesielt ansvar ved kjøp og utvikling av informasjonssystemer med personopplysninger, utforming av personvernpolicy, internkontroll- og informasjonssikkerhetsrutiner, og som kan bistå enkelte ansatte i konkrete spørsmål vedrørende personvern. Disse rollene kan selvsagt kombineres, og det er prinsipielt sett mulig å la personvernombudet fylle alle tre roller. Etter vår mening er det imidlertid de to sist nevnte rollene som bør vektlegges.

For det første er det etter vår mening viktig å unngå ordninger som innebærer etablering av en instans som er myndighetslignende, uten at det er knyttet slike krav og garantier til virksomheten som forvaltningsloven krever. Denne betenkeligheten er særlig aktuell ved eksterne ombud. Vi vil ikke avvise at det kan være behov for flere myndigheter på personvernområdet, men anbefaler at en skiller klart mellom myndighet og private "ombudsmenn". En "ombudsmann" i personopplysningslovens forstand bør etter vår mening ikke ha beslutningsmyndighet, men bør være en kompetanseperson som kan bistå registrerte, behandlingsansvarlige og andre i arbeidet med å oppfylle personopplysningslovgivningens krav.

På bakgrunn av vår vektlegging av behovet for et klart skille mellom myndigheter og private ordninger, stiller vi oss tvilende til om det er hensiktsmessig å benytte begrepet "ombud" om ordninger som er klart private. Selv om ombudsrollen i dag ikke er ensartet, hører ombudene – så vidt vi har kunnet bringe på det rene – til det offentlige apparatet.[238] Et mer hensiktsmessig begrep ville kanskje være "personvernansvarlig", men vi har ingen sterke meninger på dette punktet og har derfor benyttet ombudsmanns-betegnelsen også i fortsettelsen.

Ombudenes primære oppgave bør være å bidra til rettsriktig og lojal etterlevelse av lov, forskrift mv, i forhold til en bestemt behandlingsansvarlig. At personvernombudet ikke bør være myndighetslignende, innebærer for det første at en ikke bør forutsette et uavhengig

[237] Videre om ordningen se Öman og Lindblom 2001 s. 264 flg.

[238] Jf. for eksempel Sivilombudsmannen, Forbrukerombudet, Barneombudet, Likestillings- og diskrimineringsombudet, Ombudsmannen for forsvaret, fylkesvise pasientombud, samt flere "(helse- og) sosialombud", "byombud" og "brukerombud" i kommunene. Et unntak er "verneombud" på arbeidsplasser, se arbeidsmiljøloven kapittel 6. Disse ombudene har imidlertid myndighetslignende funksjoner, og skal bl.a. delta på Arbeidstilsynets inspeksjoner av virksomheten, samt kan stanses farlig arbeid inntil Arbeidstilsynet har tatt stilling til om arbeidet kan fortsette.

forhold mellom ombudet og behandlingsansvarlige, og at det bør være fullt ut akseptabelt at det foreligger et arbeids- eller oppdragsgiverforhold mellom personvernombudet og den behandlingsansvarlige. Samtidig må det etableres en situasjon som sikrer faglig integritet, gode samarbeidsrelasjoner, samt tilstrekkelig tid og ressurser. Behandlingsansvarlige må med andre ord kunne sikre fullt ut tilfredsstillende arbeidsforhold for ombudet. Dette innebærer trolig så omfattende krav til ombudets funksjon at det er nødvendig å gi klare fordeler til behandlingsansvarlige som kan motivere til å gå inn i en slike ordning, se neste avsnitt.

### 10.4.2 Mulige fordeler for behandlingsansvarlige med personvernombud

#### 10.4.2.1 Oversikt

Etter vår mening kan behandlingsansvarlige særlig tenkes å ha to typer motiverende grunner for å ønske opprettelsen av personvernombud:

- Lettelser i plikter etter loven; og/eller
- positiv profilering av virksomheten overfor ansatte, kunder, parter, publikum mv.

Loven bør etter vår mening støtte opp under begge typer motiverende ordninger.

Lettelser for behandlingsansvarlige som "motytelse" for personvernombud kan i utgangspunktet enten være knyttet til en

- reduksjon av registrertes rettigheter, eller
- lettelse av behandlingsansvarliges plikter etter loven, eller
- reduksjon av plikter/reduserte krav overfor Datatilsynet, eller
- etablering av nye rettigheter overfor Datatilsynet.

Etter vår mening vil det ikke være akseptabelt å redusere rettigheter overfor registrerte personer eller lempe på behandlingsansvarliges plikter overfor registrerte. En annen ting er at flere av de registrertes rettighetene bør kunne justeres og oppfylles på måter som er mindre arbeidskrevende for behandlingsansvarlige. Slike endringer faller imidlertid utenfor mandatet for denne utredningen, og vil derfor ikke bli nærmere drøftet.

#### 10.4.2.2 Lettelser i behandlingsansvarliges plikter/reduserte krav overfor Datatilsynet

Reduksjon av plikter overfor Datatilsynet, kan potensielt ha stor motiverende effekt for behandlingsansvarlige. I avsnitt 9.5.2 foreslår vi en konsesjonsordning som bl.a. tar utgangspunkt i berørte personers rett til å kreve konsesjonsbehandling på grunnlag av innsendt melding og varsel fra den behandlingsansvarlige. En mulighet er å unnta fra denne delen av konsesjonsordningen dersom det er opprettet et personvernombud som tilfredsstiller noen nærmere krav som er fastsatt i loven. Et slikt unntak vil være en lettelse ved at konsesjonssaker kan være ressurs- og tidkrevende, og dessuten gi mer uønsket oppmerksomhet enn nødvendig. Unntak kan også gi større grad av forutberegnelighet for behandlingsansvarlige, samt "regi" av saker som gjelder den behandlingsansvarliges virksomhet.

Også forpliktelsene til å dokumentere tiltak vedrørende informasjonssikkerhet og internkontroll kan tenkes å være gjenstand for lettelser. Dette gjelder særlig i forhold til internkontroll (pol § 14), fordi selve ombudsordningen nettopp kan ses som et tiltak for å sikre etterlevelse av krav i og i medhold av loven. Forutsatt at personvernombudet utfører funksjoner som er tilfredsstillende i forhold til å sikre etterlevelse av lov og forskrift mv, er det derfor mulig å godkjenne ordning med personvernombud som fullgod med ordning med internkontroll. Internkontroll og personvernombud kan med andre ord tenkes å være alternative ordninger.

En annen mulighet er å gi større frihet for behandlingsansvarlige til å behandle personopplysninger. I vårt radikale forslag til § 5a bokstav b, har vi således foreslått at barn mellom 12 og 15 år kan opptre som registrert uten medvirkning fra foreldre, dersom den behandlingsansvarlige har personvernombud. Tanken er å se dette ombudet som en garantist for at vedkommende behandlingsansvarlig følger lovens bestemmelser mv. Skjer ikke dette, har Datatilsynet kompetanse til å trekke godkjenningen av personvernombudet tilbake, se avsnitt 14.2, kapittel IV i lovutkastet.

Når det gjelder unntak fra meldeplikt, mener vi det er lite å oppnå ved å foreslå lettelser. For det første er det neppe særlig lettelse å bli fritatt fra meldeplikt dersom de samme opplysninger som inngår i en melding likevel skal være tilgjengelig hos personvernombudet. Dessuten vil verdien av meldeplikten bli vesentlig redusert dersom antallet meldepliktige reduseres. Dette gjelder særlig meldepliktens funksjon i forhold til registrerte personer og deres mulighet til å søke informasjon om behandling av personopplysninger. Vi har dessuten foreslått en vesentlig reduksjon av innholdet i meldingene (se avsnitt 9.5.2), noe som gjør at selve innmeldingen ikke kan anses å være byrdefullt. Dersom en behandlingsansvarlig har etablert personvernombud i samsvar med lovens krav, kan meldingen primært gjelde innholdet/omfaget av personvernombudets virksomhet.

#### 10.4.2.3 Etablering av nye rettigheter for behandlingsansvarlige overfor Datatilsynet

I tillegg til lemping av plikter overfor Datatilsynet, mener vi det er grunn til å se nærmere på muligheten for å gi behandlingsansvarlige med personvernombud særfordeler. Dette kan i utgangspunktet tenkes å gjelde følgende forhold:

- Saksbehandlingstider;
- Informasjonstjenester;
- Veiledningstjenester.

Fordeler for behandlingsansvarlige med personvernombud kan ses som diskriminering av andre behandlingsansvarlige, og er derfor ikke uproblematisk. Problemet er særlig knyttet til det faktum at alle behandlingsansvarlige ikke vil ha mulighet til å etablere personvernombud og derfor ikke kan velge en slik ordning med tilhørende fordeler. Mange behandlingsansvarlige som personvernombud ikke er aktuelt for er små, og kan nettopp ha behov for å oppnå de tjenester som kan tenkes knyttet til ombudsordningen. På den annen side vil slike store behandlingsansvarlige som ombudsordningen kan være attraktiv og mulig for, ha behandling av personopplysninger på et omfang og med en personvernmessig betydning, som nettopp begrunner kanalisering av ressurser til denne gruppen. Her vil vi ikke gå inn i en nærmere diskusjon vedrørende ønskeligheten av å gi særfordeler til behandlingsansvarlige med personvernombud. Spørsmålet om dette vil være lovlig og forsvarlig avhenger av den

nærmere innretningen av fordelsordningene. I det følgende begrenser vi oss til å gi små idéskisser.

Saksbehandlingstider er av stor betydning for behandlingsansvarlige, særlig i tilknytning til utvikling av informasjonssystemer som ofte er knyttet til organisasjonsmessige endringer og andre omstillingsprosesser. Forvaltningsloven § 11a inneholder regler om saksbehandlingstider, men dersom arbeidskapasiteten i forvaltningsorganet er liten i forhold til saksmengden forhindrer ikke denne bestemmelsen at det kan ta lang tid før enkeltvedtak kan treffes. Det er neppe aktuelt å introdusere særlige bestemmelser om saksbehandlingstider som innebærer positiv diskriminering av visse behandlingsansvarlige. Imidlertid kan det være grunn til å vurdere om Datatilsynet bør organisere sin virksomhet slik at saksbehandlingstider for behandlingsansvarlige med personvernombud gjennomgående kan bli kortere enn i andre tilfelle. Det kan således være aktuelt å etablere en egen enhet for saker vedrørende slike behandlingsansvarlige. Slik organisering kan også være hensiktsmessig fordi det er slike særlige kjennetegn ved saker i virksomheter med ombud at spesialisering gir mest effektiv saksbehandling. En slik arbeidsordning i Datatilsynet bør neppe etableres i lovs form fordi det ikke er akseptabelt å låse tilsynets ressursinnsats. Datatilsynet kan trolig heller ikke instrueres om å organisere sin virksomhet på den foreslåtte måten, fordi dette trolig vil støte an mot tilsynets uavhengighet, jf. pol § 42 første ledd og personverndirektivet artikkel 28 nr. 1.[239] En ordning med særlig enhet i Datatilsynet som kan gi rask saksbehandling i saker som gjelder behandlingsansvarlige med personvernombud, må/bør derfor trolig avhenge av prioriteringer og organisatoriske bestemmelser i Datatilsynet selv. Eventuelt kan særlig tjenester overfor personvernombud (jf. også nedenfor) inngå i en bestemmelse om Datatilsynets oppgaver, jf. pol § 42 nr. 1 – 8.

En neste mulighet er å etablere egne informasjonstjenester for behandlingsansvarlige med personvernombud. Også dette må trolig være basert på en intern prioritering i Datatilsynet ved at en bruker særlige ressurser på å etablere og vedlikeholde en tjeneste som spesielt er rettet mot personvernombud. Vi tenker her på tiltak ut over de rene informasjonstjenester som i dag er etablert knyttet til ombudsordningen. En slik utvidet tjeneste kan delvis være forbeholdt ombud, og kan for eksempel omfatte, rutiner for elektronisk saksbehandling med saksflytfunksjoner, sakarkiv mv. Slike saksbehandlingsrutiner kan gjøre saksbehandlingen mer åpen og brukervennlig for den behandlingsansvarlige, enn tradisjonell saksbehandling vil være. Det kan også være aktuelt å etablere "faglig forum" eller lignende, dvs. slik at Datatilsynet tilbyr tjeneste med faglig kontakt og erfaringsutveksling mellom personvernombud.

Veiledningstjenester kan ses i sammenheng med informasjonstjenester, men er her tenkt som tjenester som krever konkrete vurdering av forhold hos den behandlingsansvarlige. Idéen er at ekspertise hos Datatilsynet kan bli tilgjengelig for personvernombud etter forespørsel fra ombudet. Det kan herunder være at Datatilsynet bør kunne gi bindende forhåndsuttalelser til personvernombud vedrørende hvilke krav som er tilstrekkelige for å etterleve loven. I tillegg til forhåndsuttalelser vedrørende lovtolkingsspørsmål, kan det være aktuelt med forhåndsuttalelser vedrørende hva som skal anses å være tilfredsstillende sikring av personopplysninger, jf. pol § 13 og pof kapittel 2.

[239] "These authorities shall act with *complete independence* in exercising the functions entrusted to them" (vår kursiv).

### 10.4.3 Mulige profileringseffekter av å ha personvernombud

For behandlingsansvarlige som i stor grad er avhengig av tillit fra registrerte personer, og særlig i tilknytning til internett-baserte tjenester og internett-baserte rutiner i tilknytning til myndighetsutøvelse i offentlig forvaltning, kan personvernombud ha viktig profileringseffekt. Forutsetningen er trolig at det tydelig fremgår (i) at det eksisterer et personvernombud for virksomheten og (ii) at det kommuniseres på en tydelig og troverdig måte hva ombudsordningen går ut på. Vi antar at en offentlig merkeordning vil være viktig i forhold til begge forutsetninger. Det er nærliggende å utrede muligheten for å introdusere et ikon/symbol som merke på eksistensen av en ombudsmannsordning. På nettet kan et slikt ikon være lenket til en generell beskrivelse av ordningen med personvernombud og kontaktopplysninger mv. vedrørende hvert aktuelle ombud. Det bør tydelig fremgå at det er Datatilsynet som informerer, dvs. informasjonen bør fremstå som autorativ, ensartet og pålitelig. Bruk av ikon med tilhørende informasjon bør være obligatorisk for alle personvernombud.

Øvrige mulige profileringseffekter bør det være opp til den enkelte behandlingsansvarlige å sørge for.

### 10.4.4 Nærmere krav til rammevilkår og oppgaver for personvernombudene

Et personvernombud bør etter vår mening ha funksjoner i forhold til tre aktørgrupper:

- Ledelsen i den behandlingsansvarliges virksomhet, herunder daglig leder og daglig ansvarlige personer;
- Ansatte i den behandlingsansvarliges virksomhet;
- Personer det er registrert opplysninger om hos den behandlingsansvarlige.

Som tidligere nevnt, bør ombudets virksomhet ikke være innrettet i samsvar med Datatilsynets eller andre myndigheters konkrete behov. Hovedtilnærmingen bør være at det er ombudet som etablerer kontakt med Datatilsynet når ombudet har behov. For øvrig bør Datatilsynet forholde seg til virksomheter med personvernombud som de forholder seg til andre behandlingsansvarlige. Det bør med andre ord ikke gjelde særlige retningslinjer vedrørende kontroll med etterlevelse av lov, forskrift, konsesjoner og andre enkeltvedtak.

I forhold til ledelsen i den behandlingsansvarliges virksomhet, bør personvernombudet særlig ha ansvaret for å bistå med å:

1) bistå ved utforming av en personvernpolicy for den behandlingsansvarlige, dvs. ta stilling til hvorledes lovkrav og interne prioriteringer skal få effekt på virksomheten. Interne prioriteringer kan særlig tenkes å resultere i bedre ivaretakelse av personvern enn det loven påbyr;

2) generelt sikre etterlevelse av lov, forskrift, konsesjonsvilkår og pålegg fra Datatilsynet, herunder gjennomføre forsvarlig avveininger mellom personvern og virksomhetens interesser, jf. pol § 14;

3) sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet, jf. pol § 13.

I forhold til ansatte hos den behandlingsansvarlige, bør personvernombudet primært ha som funksjon å:

1) sikre tilstrekkelig informasjon til ansatte om lovkrav og virksomhetsinterne krav til behandling av personopplysninger;

2) være kontaktpunkt for ansatte som ønsker å ta opp problemer, forbedringspotensialer mv. med ledelsen, bringe synspunkter videre og eventuelt følge opp ledelsens videre behandling av spørsmålene;

3) sikre tilstrekkelig opplæring av ansatte på områder som har direkte betydning for ivaretakelse av personvern og informasjonssikkerhet.

I forhold til registrerte personer, bør personvernombudet primært ha som funksjon å:

1) sikre tilstrekkelig informasjon til registrerte personer om deres rettigheter, behandlingsansvarliges plikter og muligheten for å ta kontakt med behandlingsansvarlige;

2) være kontaktpunkt for registrerte personer som ønsker å ta opp spørsmål vedrørende problemer, forbedringspotensialer mv., bringe synspunkter videre og eventuelt følge opp ledelsens videre behandling av spørsmålene;

3) spesielt følge opp alle saker der registrerte personer bestrider lovligheten av den behandling av personopplysninger som skjer, særlig saker vedrørende avgivelse av samtykke og tilbaketrekking av samtykke, sletting og retting av personopplysninger (jf. pol § 27), samt opphør av å behandle personopplysninger i samsvar med pol § 28.

For at ordningene med personvernombud ikke bare skal bli papirbestemmelser, er det avgjørende å sikre ombudene tilstrekkelig kompetanse og ressurstilgang. Det bør således kreves en viss utdanning innen personopplysningsrett generelt og personopplysningsloven med forskrifter spesielt. Ombud som mangler relevant formell utdanning, bør kunne tilbys kurs i regi av Datatilsynet eller andre, i samsvar med retningslinjer fastsatt av departementet.

Når det gjelder ressurstilgangen, er det neppe aktuelt å fastsette innsatsen til et visst antall arbeidstimer per måned, år eller lignende. Det bør imidlertid vurderes å gi særlige bestemmelser om saksbehandlingstider for personvernombud, samt å legge til rette for innrapportering om uakseptabel tidsbruk og/eller opptreden fra personvernombudenes side.

Etablering av ordning med personvernombud hos den enkelte behandlingsansvarlig bør være basert på enkeltvedtak hos Datatilsynet, dvs. med klagerett til Personvernnemnda og øvrige rettssikkerhetsgarantier i henhold til forvaltningsloven knyttet til ordningen. På tilsvarende måte bør det også være anledning til å trekke tilbake tillatelse om å etablere ombudsordning, for eksempel fordi ombudet ikke etterlever de vilkår/plikter som gjelder for ordningen.

Nærmere bestemmelser om personvernombudets oppnevning, oppgaver mv. bør kunne gis i forskrift. Forutsetningen er at det til ikonet og den tilknyttede informasjonen klart fremgår for alle hvilke funksjoner og forventninger som er knyttet til ordningen.

Vi har ikke skrevet utkast til detaljerte regler for personvernombud. I stedet har vi nøyet oss med å lage utkast til slike lovbestemmelser som etter vår mening er ønskelige for å kunne innpasse ordningen i det øvrige regimet.

### 10.4.5 Om forholdet til andre rolle og aktører

Vårt forslag vedrørende personvernombud er basert på interne ordninger i den behandlingsansvarliges virksomhet. Årsaken er at det etter vår mening kreves nærhet mellom ombudet og de ombudet skal samarbeide med, samt at ombud bør ha et realistisk avgrenset arbeidsområde. Dette betyr imidlertid ikke av vi avviser kollektive private ordninger som for eksempel den som gjelder for forskning der NSD i dag har en viktig rolle som personvernombud. Etter vår mening er det imidlertid også her viktig å ta stilling til hvem slike kollektive ordninger skal være til for. Dersom NSD og andre i stor grad skal ha funksjoner som Datatilsynet ellers ville utført, er det etter vår mening mest nærliggende å ta skrittet fullt ut og etablere en egen myndighet som skal sikre personvern og informasjonssikkerhet innen forskning. Et slikt forslag foreligger for så vidt gjelder medisinsk og helsefaglig forskning.[240] Poenget er at myndighetslignende funksjoner bør kombineres med rettssikkerhetsgarantier og i utgangspunktet skal være gratis.

Alternativet er at det blir etablert private bransjekontorer som kan understøtte arbeidet med personvern og informasjonssikkerhet innen en bransje/saksområde, og som primært har oppgave å yte tjenester til medlemmene. Slike bransjekontorer bør imidlertid være basert på frivillighet, og tjenesten kan eventuelt prises. Slik sett kan NSD for eksempel tenkes å etablere "Personvernkontoret for forskning" og motta oppdrag og yte (betalte) tjenester fra forskningsinstitusjoner. Slike kontorer kan selvsagt også inngå som en del av organiseringen av en bransje, og tjenestene kan være del av medlemsfordeler. Slik kan for eksempel Finansnæringens hovedorganisasjon (FNH) tenkes å etablere medlemstjenester vedrørende personvern og informasjonssikkerhet. Det kan i så fall være aktuelt å favne videre enn de problemstillinger som personopplysningsloven aktualiserer, og FNH kan for eksempel tenkes også å tilby tjenester vedrørende informasjonssikkerhet i henhold til krav i forskrift til kredittilsynsloven mv.[241]

Bransjer og private bransjekontorer bør kunne følge en praksis basert på bransjenormer om personvern, og som kan presisere og supplere den rettslige reguleringen av feltet. Datatilsynet bør fortsatt kunne bistå ved utforming av slike normer (jf. pol § 42 annet ledd nr. 6), men vi ser ikke behov for å integrere slike bransjenormer i lov- og forskriftsreguleringen på området. Dersom det innen visse bransjer blir vanlig med personvernombud, kan dette danne grunnlag for bransjevis organisering og støttefunksjoner i forhold til ombudene, for eksempel innen helsesektoren eller telebransjen. Etter vår mening bør dette være opp til den enkelte bransje å ta stilling til, og slike bransjenormer, -kontorer mv. bør ikke være gjenstand for nærmere offentligrettslig regulering eller integreres i den offentlige myndighetsapparatet.

Dersom en mener det er behov for ny myndighet innen bestemte personvernsensitive områder, for eksempel innen helse- og samfunnsforskning, må dette selvsagt være gjenstand for egen lovregulering. Vi tar ikke her stilling til om en slik myndighet er ønskelig, eller til den nærmere – eventuelle – organiseringen av en slik myndighet.

---

[240] Se NOU 2005: 1 *God forskning – bedre helse*.

[241] Lov 7. desember 1956 nr. 1, jf. forskrift 21. mai 2003 nr. 630.

### 10.4.6 Konklusjon

Vi har lagt til grunn at det bør være sammenheng i virkemiddelapparatet, særlig slik at melde- og konsesjonsplikt og ordning med personvernombud bør ses i sammenheng. Vi har prinsipalt foreslått å vesentlig redusere konsesjonsordninger som er basert på predefinerte kriterier, og har i stedet foreslått å knytte konsesjonsspørsmålet til konkrete vurderinger i Datatilsynet og blant registrerte personer. Vi forventer at dette vil gi et forholdsvis lite antall konsesjonssaker, og at de saker som vil oppstå ofte vil gjelde spørsmål som prinsipielt eller konkret er viktige. Etter vår mening bør en derfor unngå å redusere konsesjonsordningen ytterligere i tilfelle der det er etablert personvernombud. "Gjenytelsen" for personvernombud bør etter vår mening primært gjelde bortfall av krav til internkontroll, særfordeler og profileringseffekter knyttet til behandlingsansvarlige med slike ombud. Vi tror uansett at selve eksistensen av et personvernombud vil redusere muligheten for at det oppstår konsesjonssak etter de regler som er foreslått i §§ 33 og 33a, fordi personvernombudet kan bidra til å utforme rutiner for behandling av personopplysninger som i rimelig grad ivaretar personvernhensyn. En egen enhet i Datatilsynet som spesielt skal arbeide med behandlingsansvarlige med ombud, bl.a. med veiledning, vil øke muligheten for et relativt lavt konfliktnivå vedrørende behandling av personopplysninger.

Nedenfor gjengir vi forslag til bestemmelser vedrørende personvernombud. Bestemmelsene er organisert i eget kapittel for å tydeliggjøre eksistensen av ordningen. Kapittelet er satt inn i kapittel IV som i samband med foreslått omredigering av lovens nåværende to rettighetskapitler har blitt ledig, se avsnitt 12.5.2.6. Vi mener det er gunstig å plassere et slikt kapittel i samband med et nytt, samlet rettighetskapittel (III).

**Kapittel IV Personvernombud**

**§ 27 Erklæring om å etablere personvernombud**

Behandlingsansvarlige kan inngi erklæring til Datatilsynet om at det vil bli etablert en ordning med personvernombud i samsvar med bestemmelsene i §§27a – 27b.

Etter at erklæringen er mottatt, utsteder Datatilsynet et sertifikat som bekrefter at ordningen er etablert, og beskriver det nærmere innholdet i ordningen.

Den behandlingsansvarlige har rett og plikt til å benytte sertifikatet med tilhørende informasjon i samband med behandling av personopplysninger som kommer inn under ordningen med personvernombud.

**§ 27a Fordeler knyttet til ordningen med personvernombud**

Behandlingsansvarlige som har et sertifisert personvernombud er fritatt fra kravet om internkontroll i § 14.

Datatilsynet skal tilby sertifiserte personvernombud særskilte og kostnadsfrie informasjons-, veilednings- og opplæringstjenester.

**§ 27b Personvernombudets oppgaver**

Personvernombudet skal generelt bidra til at behandlingsansvarlige etterlever bestemmelser vedrørende behandling av personopplysninger i lov, forskrift, instruks, avtaler, enkeltvedtak og domsavgjørelser.

Personvernombudet skal bistå personer det er registrert opplysninger om hos den behandlingsansvarlige og dennes databehandler ved å:

a) sikre fullgod informasjon om registrertes rettigheter og plikter i forbindelse med behandling av personopplysninger, og

b) ta opp og videreformidle registrertes synspunkter på lovligheten og hensiktsmessigheten av den behandling av personopplysninger som skjer, og

c) følge opp alle saker der registrerte personer bestrider lovligheten av den behandling av personopplysninger som skjer.

Personvernombudet skal bistå ansatte i den behandlingsansvarliges virksomhet ved å

a) informere om hvilke regler som gjelder for behandling av personopplysninger, og

b) bidra til å forbedre forhold som ansatte kritiserer, og

c) sikre at de ansatte får den nødvendige opplæring.

Personvernombudet skal bistå ledelsen hos den behandlingsansvarlige med å

a) utforme personvernpolicy for den behandlingsansvarliges virksomhet, og

b) skrive årsmelding der det redegjøres for status og pågående arbeid vedrørende personvern og informasjonssikkerhet hos den behandlingsansvarlige. Årsmeldingen skal være offentlig tilgjengelig for enhver.

**§ 28 Tilbaketrekking av sertifikat for personvernombudet**

Dersom det kan dokumenteres at et personvernombudet gjentatt og grovt har forsømt sine oppgaver etter § 27b, kan Datatilsynet treffe enkeltvedtak om å trekke sertifikatet tilbake. Den behandlingsansvarlige skal i så fall alltid varsles i samsvar med forvaltningsloven § 16.

Sertifikatet kan trekkes tilbake med den varighet som Datatilsynet bestemmer. Tilbaketrekking av sertifikatet innebærer at den behandlingsansvarlige taper retten til å benytte tjenester, betegnelser og informasjon som spesielt er knyttet til den behandlingsansvarliges deltakelse i ordningen med personvernombud.

Vedtak om tilbaketrekking av sertifikat, er gjenstand for klage til Personvernnemnda.

# Kapittel 11

# Mindreåriges personvern

## 11.1 Om mandatet

I rammen gjengir vi mandatets punkt 10 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

> *Mindreåriges personvern*
>
> Flere personvernspørsmål reiser seg med særlig tyngde når det gjelder barn og unge som ikke på samme måte som andre har forutsetninger for å se eller forstå konsekvensen av utlevering og spredning av personopplysninger eller av å gi samtykke til behandling av personopplysninger. Det bør være et særlig formål å ivareta denne gruppens personvern best mulig. **Utrederne bes vurdere om det er behov for å endre loven for å sikre mindreåriges personvern best mulig**.

Vi forstår mandatet på dette punktet som åpent, uten klare føringer og anvisning på prioriteringer. Samtidig er problemstillingene omfattende. Etter vår mening er det særlig tre hovedgrupper av problemstillinger som er aktuelle i denne sammenheng:

1. Behov for endringer i personopplysningsloven og/eller forskrifter til loven;
2. Spørsmål vedrørende særlovgivning som spesielt tar sikte på å ivareta barns personvern;
3. Spørsmål vedrørende formidling av kunnskap om hvilke regler som gjelder for behandling av personopplysninger om barn, til barna selv, deres foresatte og andre som barn ofte avgir personinformasjon til.

I dette kapittelet legger vi vekt på spørsmål under 1). Likevel begrenser vi oss ikke strengt til dette, men også se kort på spørsmål vedrørende særlovgivning. Når det gjelder mer generelle overveielser vedrørende behov for særlovgivning, viser vi til avsnitt 12.3.

Det kan være grunn til å vurdere personvernet også for andre særlige grupper enn mindreårige. Dette gjelder spesielt for demente personer som ikke er umyndiggjort, men som lever i et avhengighetsforhold til helse- og omsorgspersonell, pårørende mv., samt for personer som er umyndiggjort. Selv om enkelte vurderinger vedrørende barn også kan være relevante for disse gruppene, er forskjellene mht teknologibruk og livssituasjon for øvrig så store, at det neppe er grunn til å foreta en felles behandling.

## 11.2 Oversikt over mindreåriges handleevne

Foreldreansvaret innebærer en rett og plikt til å ta avgjørelser for barnet slik at barnets interesser og behov kan ivaretas, jf. barneloven § 30.[242] Barn under 18 år har derfor i utgangspunktet en begrenset selvstendig handleevne. Barnet skal likevel gradvis få en større selvråderett fram mot myndighetsalderen. Det er således i lov fastsatt aldersgrenser som

[242] Lov 8. april 1981 nr. 7.

sikrer barn/ungdom rett til å bestemme over seg selv innen bestemte områder/situasjoner, også før fylte 18 år. En gjennomgang av de viktigste bestemmelsene på området, viser at minst 4 alderstrinn er i bruk:

7 år:

- Barn skal få si sin mening før det tas avgjørelser om personlige forhold, jf. barneloven § 31 annet ledd.

12 år:

- Det skal legges stor vekt på barns meninger, jf. barneloven § 31 annet ledd.
- Barn mellom 12 og 16 år har rett til å be om at informasjonen om helseforhold til foreldre blir begrenset, når de anfører grunner som "bør respekteres", jf. pasientrettighetsloven § 3-4 annet ledd.[243]

15 år:

- Barn kan bestemme i spørsmål om utdanning og melde seg inn og ut av foreninger, jf. barneloven § 32.
- Barn har som hovedregel adgang til å inngå arbeidsavtaler,
- Barn kan inngå arbeidsavtaler, men disse kan heves av foreldrene, jf. vergemålsloven § 32[244] og arbeidsmiljøloven § 11-1.[245]
- Barn kan disponere over egne midler, jf. vergemålsloven § 33.
- Barn under 16 år har rett til informasjon vedrørende helseforhold sammen med foreldre, jf. pasientrettighetsloven § 3-4 første ledd.

16 år:

- Barn kan gi samtykke til helsehjelp, jf. pasientrettighetsloven § 4-3.
- Barn mottar informasjon om helseforhold alene, med mindre informasjonen er nødvendig for å oppfylle foreldreansvaret, jf. pasientrettighetsloven § 3-4.

Det er ikke fastsatt regler i personopplysningsloven eller forskriftene til loven som spesielt gjelder for barn og ungdom. Datatilsynet har imidlertid utarbeidet flere retningslinjer og veiledere som gjelder noen viktige sider ved denne gruppens personvern. Det mest generelle dokumentet er ”Barn og unges personopplysninger: Retningslinjer for innhenting og bruk”, som er utarbeidet i samarbeid med Forbrukerombudet.[246] Retningslinjene forholder seg ikke til nevnte lovgivning vedrørende barns handleevne, men angir oppfatninger om hva som bør gjelde for barn i flere praktisk viktige situasjoner som primært er knyttet til barn og ungdoms internettbruk.[247]

[243] Lov 2. juli 1999 nr. 63.

[244] Lov 22. april 1927 nr. 3.

[245] Lov 17. juni 2005 nr. 62.

[246] Se <http://www.datatilsynet.no/templates/article____892.aspx>, lansert 29. januar 2004.

[247] Dvs. administrasjon av konkurranser og ”klubber”, direkte markedsføring, adressemekling, internett-publisering. Retningslinjene omfatter ikke spørsmål vedrørende forskning eller journalistisk, kunstnerisk eller litterær virksomhet.

Hovedregelen i retningslinjene tar utgangspunkt i en aldersgrense på 15 år:

> **Hovedregler:**
>
> **Mindreårige som har fylt 15 år kan som hovedregel samtykke til innhenting og bruk av egne personopplysninger selv. For barn som er yngre enn 15 år må eventuelt foreldre samtykke til innhenting og bruk av opplysninger om barnet.**
>
> Unntak:
>
> 1) Sensitive personopplysninger skal bare innhentes med foreldrenes samtykke. Sensitive opplysninger er blant annet opplysninger om helse, om etnisk bakgrunn, livssyn, og seksuelle forhold. (Se utfyllende liste i personopplysningsloven § 2 nr. 8)
>
> 2) For småkonkurranser og liknende, der enkle kontaktopplysninger *kun* skal brukes til eventuell premiering og deretter slettes, kan også yngre barn enn 15 år samtykke til deltakelse selv. Forutsetningene er imidlertid at:
> - opplysningene slettes etter premiering
> - personverntrusselen er vurdert, og klassifisert som meget lav
> - konkurransen er egnet for den aktuelle aldersgruppen.
>
> **Det skal alltid informeres om hvilken aldersgrense som gjelder når man legger opp til at mindreårige skal oppgi personopplysninger.**

Retningslinjene gjelder primært spørsmålet om samtykkekompetanse, og belyser ikke (i alle fall ikke systematisk) spørsmål om barns autonomi i en videre forstand, for eksempel i forhold til innsynsrett og rett til å rette og slette personopplysninger om egen person mv.

Disse retningslinjene og andre oppfatninger i Datatilsynet om hvordan grensene bør trekkes i forhold til barns og unges personvern, er åpenbart et nyttig utgangspunkt for overveielser av mulig lovregulering. Vi mener imidlertid at retningslinjene i for stor grad er kasuistiske og i for stor grad knyttet opp til internett-bruk, og derfor ikke er egnet som direkte utgangspunkt for formulering av lovbestemmelser på området. Eventuelle lovbestemmelser bør ha et prinsipielt og allment innhold, mens en fortrinnsvis i informasjonsmateriale bør gjøre bruk av en kasuistisk tilnærming. En lovbestemmelse vedrørende barns samtykke, utøvelse av rettigheter mv., må dessuten ha et innhold som harmonerer med annen eksisterende lovgivning om barn og ungdoms handleevne.

Etter vår mening er det en særlig utfordring for barn og ungdoms personvern at de gradvis skal få større grad av selvstendig privatliv innenfor den private relasjonen som forholdet mellom barn og foreldre innebærer. Samtidig skal barn sikres personvern i forhold til andre som behandler opplysninger om dem utenfor hjemmet, dvs. i forhold til skole, næringsdrivende mv. Slik sett gjelder personvern for barn og ungdom "i to retninger", både i forhold til foreldre og i forhold til samfunnet rundt.

Etter vår mening er det særlig tre problemområder som er viktige for barns personvern:

- Spørsmål om innsamling av opplysninger om barn, herunder spørsmål om samtykke;
- Spørsmål om innsyn i personopplysninger om barn;
- Spørsmål om retting, sletting, supplering og blokkering av opplysninger om barn.

Forholdet mellom foreldre og barn, og til en viss grad også forholdet mellom barn og andre nærstående personer, er av så spesiell karakter, og er så preget av vårt syn på familie og privatliv, at en etter vår mening bør være tilbakeholdene med å vedta generelle og bastante regler om hvorledes opplysninger om barn bør behandles. For det første er det behov for særlige vurderinger innen særlige rettsområder, jf. avsnitt 12.3 om behov for særlovgivning. For det andre er det ofte behov for å kunne utvise konkret skjønn, bl.a. fordi individuelle og/eller situasjonsbestemte forhold kan være så spesielle at det vil være umulig å forutse faste gode løsninger som kan uttrykkes som rettsregler. Likevel mener vi personopplysningsloven bør inneholde noen utgangspunkter som tydeliggjør hvilke alminnelige regler som bør gjelde. Vi forstår samtidig at en slik regulering vil kunne fremtvinge særlovgivning for å etablere andre løsninger enn etter det som måtte følge av personopplysningsloven etter en eventuell lovendring. På den annen side mener vi at slike områdevise gjennomganger av lovgivningen er ønskelige, særlig innen lovområder der barns situasjon er spesielt regulert (barnehage, skole, barnevern mv.). Det bør derfor ikke være et vilkår for regulering av barn og unges personvern i personopplysningsloven at denne løsningen også passer inn i enhver særregulering vedrørende barn og unges forhold.

## 11.3 Behandling av personopplysninger om barn i henhold til personverndirektivet

Personverndirektivet skiller ikke mellom opplysninger som kan knyttes til barn og opplysninger som kan knyttes til voksne personer. Nasjonale lovgivere og tilsynsmyndigheter står dermed forholdsvis fritt til å tilpasse direktivets regler til mindreåriges spesielle behov.

Det foreligger ingen rekommendasjon eller annet policy-dokument fra artikkel 29 arbeidsgruppen som på inngående vis tar opp personvern for mindreårige. EU-kommisjonens enhet med direkte ansvar for personopplysningsvern og oppfølging av direktivet har heller ikke utarbeidet særskilt politikk på området.[248]

Vi kjenner ikke til eksempler på særlovgivning i andre EU-/EØS-land som direkte regulerer spørsmål om mindreåriges rettigheter vedrørende personopplysningsvern. Det samme gjelder eksempler på særbestemmelser om disse spørsmål som er inntatt i generell lovgivning på feltet. Mange nasjonale datatilsynsmyndigheter har imidlertid uttalt seg om flere av disse spørsmål og har i enkelte tilfeller truffet vedtak. Vårt inntrykk er at mye (hvis ikke mesteparten) av denne delen av tilsynsaktiviteten dreier seg om skolesektoren og ulike former for behandling av opplysninger om elever, f.eks. publisering av eksamensresultater og andre elevopplysninger på skolers nettsider mv.

Behandling av opplysninger om mindreårige har fått forholdsvis stor oppmerksomhet i praksis og politikk til Datainspektionen i Sverige. Inspektionen har utgitt flere veiledninger der barns rettigheter er viet betydelig plass. For eksempel skriver Datainspektionen følgende om barn og samtykke:

> Också den som är underårig (dvs. under 18 år) kan lämna giltigt samtycke till en tilltänkt behandling om han eller hon är kapabel att förstå innebörden av samtycket. Något entydigt svar på frågan om även den underåriges vårdnadshavare måste lämna sitt samtycke för att behandlingen ska vara tillåten, kan inte ges. Det varierar från fall till fall och beror på faktorer

[248] Kommisjonen mer generelt har imidlertid gitt betydelig støtte til flere initiativer som bl.a. har til formål å beskytte barn mot personverntrusler, særlig i internett-sammenheng. Jf. eksempelvis SAFT-prosjektet (Safety, Awareness, Facts and Tools) referert i fotnote 184.

> som ålder, uppgifternas art och ändamålet med behandlingen. Om det rör sig t.ex. om forskning där man använder uppgifter om äldre tonåringar kan det vara lämpligt att inhämta samtycke från *både* tonåringen och vårdnadshavaren. Om det är forskning som rör yngre barn ska samtycke alltid inhämtas från vårdnadshavaren. Om uppgifter om underåriga ska behandlas är det särskilt viktigt att göra en seriös bedömning av den unges förmåga att förstå de totala konsekvenserna av en behandling. En tumregel kan vara att den som fyllt 15 år normalt är kapabel att ta ställning i samtyckesfrågan. Många gånger är det dock så att andra regler än de som finns i PuL hindrar att personuppgifter om barn behandlas. Det finns t.ex. begränsningar när det gäller att skicka direktreklam till barn.[249]

Datainspektionen har i tillegg foretatt empiriske kartlegginger av hvordan elevopplysninger behandles i det svenske skolesystemet.[250] Dessuten har inspektionen fattet en rekke avgjørelser på området, bl.a. et par prinsipielt viktige vedtak om bruk av biometriske autentiseringssystemer rettet mot skoleelever.[251] Et av vedtakene er påklaget til domstolene og er nå til behandling i Regeringsrätten.[252]

## 11.4 Behov for endringer i personopplysningsloven

### 11.4.1 Innsamling av opplysninger om barn

Vi er enige i at et sentralt punkt i vurderingen av barns personvern er spørsmålet om det er barnet selv eller deres foreldre som har samtykkekompetanse. For at spørsmålet skal få betydning, må imidlertid den behandlingsansvarlige være av den oppfatning at loven faktisk krever samtykke fra barnet eller deres foreldre. Som tidligere vist i avsnittene 6.4 – 6.6, kan det ofte være tvil om det ikke i stedet for samtykke kan anføres en "nødvendig grunn", og særlig er den skjønnsmessige bestemmelsen i § 8 første ledd bokstav f aktuell som rettslig grunnlag for å behandle personopplysninger om barn og andre. I avsnitt 6.8 har vi foreslått en omlegging av §§ 8 og 9 vedrørende rettslig grunnlag, og vi har herunder foreslått å snevre inn adgangen til å anføre resultatet av en bred interesseavveining. Etter vår mening er det grunn til å vurdere en ytterligere innsnevring på dette punktet for å verne barn mot at det behandles personopplysninger om dem uten lovhjemmel, samtykke eller en av de bestemte nødvendige grunner som loven for øvrig opererer med. Vi mener på denne bakgrunn det er aktuelt å ta inn et alternativ c) i § 8c av vårt radikale lovforslag:

> **§ 8c Behandling av personopplysninger på grunnlag av skjønnsmessige avveininger**
>
> Dersom et av vilkårene i §§ 8a og 8b ikke kan oppfylles, kan den behandlingsansvarlige beslutte å igangsette behandling av personopplysninger som er nødvendig for å ivareta egne eller medkontrahenters berettigede interesser. Slik beslutning kan bare treffes dersom:
> […]
>
> *c) det ikke inngår personopplysninger om barn under 12 år, og* (her i kursiv)
>
> […]

Bestemmelsen må ses i sammenheng med forslaget til § 6a, se neste avsnitt. For barn som er mellom 12 og 15 år, forutsetter vi at foreldrene opptrer sammen med barnet, og således kan ivareta barnets personvern på tilstrekkelig måte. For barn mellom 16 og 18 år forutsetter vi at

[249] Datainspektionen 2003 s. 12. Jf. også Datainspektionen 2002a.

[250] Jf. f.eks. Datainspektionen 2002b.

[251] Jf. Datainspektionens vedtak 13. januar 2005 (sak nr. 1601-2004) og vedtak 9. mars 2005 (sak nr. 1976-2004).

[252] Jf. <http://www.datainspektionen.se/pdf/beslut/overklagan_tallriksautomater_RegR.pdf>.

disse normalt kan opptre som registrert person på egenhånd, men at foreldre kan gripe inn dersom foreldreansvaret gjør det nødvendig. På denne bakgrunn mener vi at de foreslåtte bestemmelsene samlet gir et tilstrekkelig vern også av barn mellom 12 og 18 år.

### 11.4.2 Samtykke og generelt om barns rolle som registrert person

Den bestemmelsen som er foreslått i forrige avsnitt (§ 8c bokstav c), vil skape flere situasjoner der samtykke er nødvendig, og spørsmålet blir da hvem som skal samtykke. I Datatilsynets retningslinjer vedrørende innhenting og bruk av personopplysninger om barn og unge, er det definert en hovedregel på 15 år, samtidig som det er sagt at det i tillegg må skje en skjønnsmessig vurdering der en trekker inn en rekke konkrete forhold. Retningslinjene går ut i fra at det enten er barnet eller foreldrene som har samtykkekompetanse. De synes å forutsette at foreldre kan samtykke alene på vegne av barn under 15 år, at unge som er 15 år eller eldre kan samtykke alene til å behandle personopplysninger som ikke er sensitive (jf. § 2 nr. 8), at barn under 15 år kan samtykke til behandling av personopplysninger til "småkonkurranser og liknende", og at innhenting av sensitive personopplysninger alltid må skje med foreldrenes samtykke. Retningslinjene benytter flertallsformen "foreldrene", men det er ikke nærmere kommentert om det med dette menes at begge foreldrene må samtykke.

Etter vår mening foreligger det minst tre (og ikke to) alternative løsninger på tildeling av samtykkekompetanse:

- Barnet samtykker alene;
- Barnet og foreldrene avgir felles samtykke;
- Foreldrene samtykker alene.

Også ut i fra personvernhensyn er det viktig å anerkjenne at barnet har en viss grad av autonomi, og at denne autonomien gradvis skal øke frem til myndighetsalder. Det bør derfor være et mål å la barn være meningsberettigete i så stor grad som forsvarlig.

I henhold til barneloven § 31 annet ledd skal det legges stor vekt på barns meninger når barnet har fylt 12 år. Vi mener det er i dårlig harmoni med denne bestemmelsen dersom foreldrene skal kunne samtykke alene, eventuelt mot barnets vilje. Riktignok kan det finnes spesielle situasjoner der det vil være uakseptabelt å la et barn på 12 år ha "veto" i en sak om å behandle opplysninger om barnet. Slike tilfeller vil imidlertid enten falle inn under særlovgivning (for eksempel pasientrettighetsloven), eller de bør være gjenstand for annen særlig regulering (dette kan for eksempel tenkes å gjelde barnevern og utdanning). Etter vår mening bør derfor hovedregelen etter personopplysningsloven være at barn mellom 12 og 15 år og foreldre må avgi *felles* samtykke.[253]

Når det gjelder barn mellom 7 og 12 år, er barnelovens regel at barn skal få si sin mening før det tas avgjørelser om personlige forhold, jf. barneloven § 31 annet ledd. Samtykke til å behandle personopplysninger om barnet, gjelder ofte personlige forhold, og barnet bør derfor alltid høres før samtykke gis eller nektes.

[253] Gjennomføring av felles samtykke kan selvsagt by på praktiske problemer, for eksempel i tilknytning til internett-bruk der det i dag er lagt opp til samtykke ved hjelp av "klikk" på et ikon eller lignende. Det vil imidlertid alltid være problemer av denne typen, for eksempel med å sikre seg at det virkelig er en forelder som samtykker for barnet. Felles samtykke kan kreve to-trinns prosedyre for samtykke; for eksempel ved at barnet samtykker på vanlig måte og får oppgitt et referansenummer eller lignende som deretter benyttes av foreldre som bekrefter via SMS eller e-post. Vi går ikke nærmere inn på mulige tekniske/praktiske løsninger, men legger til grunn at problemet kan løses på tilfredsstillende måte.

Når det gjelder barn eldre enn 15 år, mener vi det ikke kan fastsettes at det kun er foreldrene som kan samtykke til å innhente sensitive personopplysninger om barnet. Dette gjelder i alle fall i den grad barnet har en selvstendig, begrenset handleevne etter loven. Når barn kan gi samtykke til helsehjelp alene (jf. pasientrettighetsloven § 4-3), må de også kunne avgi helseopplysninger og andre sensitive opplysninger som er begrunnet i helsehjelpen. Etter kirkeloven[254] § 3 nr. 6 kan personer som har fylt 15 år melde seg ut og inn av Den norske kirke på egen hånd. Det er da åpenbart at de i denne sammenheng også kan gi samtykke til å behandle opplysninger om religiøs tro, filosofi mv. Det er dessuten nærliggende å mene at trosfriheten må innebære kompetanse til alene å gi samtykke til å gi slike opplysninger også til andre enn Den norske kirke.

Dersom det er to personer som har foreldreansvar, må det normalt være tilstrekkelig at én av disse samtykker. I enkelte tilfelle der samtykke til å behandle personopplysninger er knyttet til avgjørelser som er av vesentlig betydning for omsorgen for barnet, kan det imidlertid være at samtykke fra begge foreldrene må kreves. Dette spørsmålet må imidlertid løses i samsvar med reglene i barneloven vedrørende utøvelse av foreldreansvar. Dersom foreldreansvaret må utøves i fellesskap, må med andre ord samtykke fra begge foreldre kreves. Vi går ikke nærmere inn på hvorledes denne grensen bør trekkes, men understreker at den eneste praktisk mulige hovedregelen er at kun én forelder samtykker.

Selv om spørsmålet om samtykkekompetanse er viktig, er det behov for å avklare forholdet mellom barn og foreldre også i relasjon til andre deler av personopplysningsloven. Dette gjelder ikke minst spørsmål om hvem som har rett til innsyn i opplysninger om barnet (§ 18), hvem som kan kreve retting, sletting av opplysninger om barnet (§ 27) osv. Det vil etter vår mening være unødig kompliserende å regulere hvert forhold for seg. Også pedagogisk sett vil et generelt regelsett trolig være lettere å kommunisere enn flere enkeltregler. Målet må derfor være å gi en generell regulering av forholdet mellom barn og foreldre innenfor rammene av personopplysningsloven. Det overordnede spørsmålet som loven bør gi svar på er i hvilken grad barn kan opptre som "registrert person", og således opptre som aktiv part i forhold til behandlingsansvarlige, databehandler, Datatilsynet og andre.

Vi foreslår følgende generelle bestemmelse:

> Personer under 18 år kan opptre som registrert person (jf. § 6 første ledd) etter bestemmelsene i denne loven på følgende måter:
>
> a) For barn mellom 7 og 12 år kan barnets foreldre opptre alene. Foreldrene bør om mulig først spørre barnet om hva det mener om vedkommende personvernspørsmål.
>
> b) For barn mellom 12 og 15 år skal barn og foreldre opptre i fellesskap. Barn kan likevel opptre alene overfor behandlingsansvarlige som har personvernombud i samsvar med kapittel IV i denne loven.
>
> c) Barn mellom 15 og 18 år kan opptre alene, uten foreldrenes medvirkning.

[254] Lov 7. juni 1996 nr. 31.

> Uansett bestemmelsene i a – c, kan barnets foreldre gripe inn i den utstrekning ivaretagelse av foreldreansvaret gjør dette nødvendig.

Bestemmelsen er satt inn som § 6a i vårt radikale lovforslag, dvs. i tilknytning til bestemmelsen i § 6 som definerer og angir betydningen av å være "registrert person". Forslaget innebærer at barn under 12 år ikke alene kan gi fra seg opplysninger om egen person, kreve innsyn mv., men trenger foreldrenes medvirkning. Dette kan virke tungvint i forhold til barns bruk av "uskyldige" internett- og SMS-tjenester mv. Samtidig er det behov for en nedre aldersgrense, og av hensyn til regelkompleksitet bør det ikke innføres flere aldersgrenser enn de tre som her er foreslått. Det kan dessuten ses som gunstig at foreldrene på denne måten vil få nærmere kunnskaper om hva barna deres benytter internett, SMS mv. til.

### 11.4.3 Innsyn i personopplysninger om barn og informasjon til barn

Forslaget til generell løsning for spørsmålet om barn og foreldres rett til å opptre i henhold til bestemmelsene i lov, forskrift mv., gir også løsning på praktisering av innsynsretten. Så lenge barnet er under 15 år, vil de således som hovedregel opptre sammen med en forelder. Det er imidlertid grunn til å vurdere om barns innsyn bør modifiseres noe også ut over denne ordningen.

I dagens lov er det en unntaksbestemmelse som er særlig anvendelig i forhold til barn (men som ikke er spesielt knyttet til denne gruppen): Det heter således i § 23 første ledd bokstav c at retten til innsyn og informasjon ikke omfatter opplysninger som "det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær".

Bestemmelsen knytter en reservasjon til innsynsretten som gjelder opplysningenes innhold, og fremholder opplysninger om helse og personlige relasjoner spesielt. Unntaket blir kombinert med en bestemmelse i § 23 annet ledd der det åpnes for at opplysningene "på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det".

Vi er enige i at helse og personlige relasjoner representerer viktige grunner til å holde informasjon tilbake. Når det gjelder barn, kan det imidlertid være flere typer informasjon som kun bør gis via en representant for barnet: for eksempel fordi opplysninger kan virke skremmende eller forvirrende uten nærmere forklaring fra en voksen. Dersom en skal ivareta barns interesser kan det derfor være grunn til å bygge unntaket på den registrertes evne til å forholde seg til opplysningene. Det kan derfor være mer hensiktsmessig å ta utgangspunkt i den registrerte personens lave alder, evne til å forholde seg til informasjonen mv., snarere enn i bestemte opplysningstyper som helse mv. For å tydeliggjøre at unntaket gjelder overfor den registrerte direkte, og at en representant normalt vil kunne/skal få tilgang til opplysningene, bør denne bestemmelsen settes inn i forlengelsen av selve unntaket. Foreldre vil ofte være barns representanter, og dette kan med fordel sies direkte i bestemmelsen. Med denne innfallsvinkelen kan en alternativ bestemmelse til § 23 bokstav c lyde:

> Dersom det må anses utilrådelig at den registrerte får direkte kjennskap til egne personopplysninger fordi vedkommende på grunn av ung alder eller andre forhold har utilstrekkelig evne til å forholde seg til opplysningene, skal

> opplysningene gjøres kjent via en representant for den registrerte (foreldre, lege, advokat mv).

Bestemmelsen er satt inn som § 22 annet ledd i vårt radikale lovforslag. Saklig sett innebærer den foreslåtte bestemmelsen en utvidelse av unntaksbestemmelsen sammenlignet med dagens formulering, fordi unntaket ikke er spesielt knyttet opp mot noen typer personopplysninger. Samtidig er ordlyden endret slik at opplysningen *skal* legges frem via en representant for den som begjærer innsyn. Dette innebærer at opplysningene ikke er unntatt i absolutt forstand, slik som for de øvrige alternativene i § 23 første ledd bokstavene a – f. Bestemmelsen bør derfor erstatte den nåværende bestemmelsen (i § 23 annet ledd) som omhandler innsyn og informasjon ved hjelp av representant.

Bestemmelsen er formulert slik at den omfatter også andre enn barn, men barn er spesielt nevnt. Bestemmelsen innebærer at opplysninger som kan virke skremmende, nedbryte personens selvbilde mv., ikke skal gis barn direkte men først vurderes av barnets representant. Dette gjelder generelt og får størst betydning for barn fra 12 – 18 år som kan utøve direkte innsynsrett sammen med foreldre eller alene.

### 11.4.4 Om behovet for særlige reguleringer og avsluttende kommentarer

Vi antar at de bestemmelsene som her er foreslått vedrørende behandling av opplysninger om barn, vil passe som et generelt utgangspunkt. Lovens saklige virkeområde er imidlertid meget vidt, og det er ikke til å unngå at det innen bestemte felt bør gjøres andre avveininger. I tillegg er det en ulempe ved generelle bestemmelser at de er så allment formulerte, at det kan være vanskelig for registrerte, barn, foreldre, behandlingsansvarlig og andre å forstå hva lovbestemmelsen konkret innebærer for deres situasjon. Behovene for å gjøre særlige avveininger og for å gi tilstrekkelig konkrete regler, kan ofte tilsi at det bør skje en særlig regulering. I forhold til barn og unges personvern antar vi at det kan foreligge spesielle behov innenfor minst to områder:

- Markedsføring;
- Skole.

Som tidligere nevnt har Forbrukerombudet sammen med Datatilsynet gitt retningslinjer som bl.a. omfatter behandling av opplysninger om barn i tilknytning til markedsføring. Slike retningslinjer er mer detaljerte enn våre forslag til særlige bestemmelser vedrørende barn. Våre forslag er også mindre spesifikke enn de nordiske forbrukerombudenes felles retningslinjer vedrørende innhenting av personopplysninger i forbindelse med markedsføring. Her heter det bl.a.: "De næringsdrivende bør ikke tilby belønninger eller fordeler i bytte mot mindreåriges personopplysninger. De bør heller ikke benytte undersøkelser, konkurranser eller liknende metoder for å samle inn disse opplysningene". Vi ser ikke bort i fra at det kan være behov for å vedta så detaljerte regler på forskriftsnivå, for eksempel i forskrift til markedsføringsloven.[255]

Det andre området som er av stor betydning for mange barn, gjelder i forhold til bruk av IKT (internett, SMS mv) i undervisningsinstitusjoner. Dette er spesielt aktuelt i tilknytning til bruk av elektroniske læringsplattformer, dvs. der innlevering og evaluering av elevarbeider skjer elektronisk, og i tilknytning til innhenting og publisering/videregivelse av

[255] Lov 16. juni 1972 nr. 47.

personopplysninger i tilknytning til undervisning. Det er dessuten en rekke spørsmål som gjelder "fritidsbruk" av mobiltelefoner med kameraer, internett mv. der det oppstår spørsmål om hva slags bruk som er tillatt, hvilke sanksjonsmuligheter skolen har osv. Selv om flere viktige spørsmål gjelder elevenes personvern, inngår disse imidlertid i nær sammenheng med spørsmål som gjelder elevers ytrings-/informasjonsfrihet, rettssikkerhet i tilknytning til vedtak som skolen, PP-tjenesten og andre treffer mv. Dette peker etter vår mening i retning av å vurdere særregulering av IKT-bruk i skolen, inkludert regulering av flere konkrete forhold som er spesielle for skolevesenet. En slik regulering vil systematisk høre inn under opplæringslova.[256]

Avslutningsvis vil vi understreke at klarere rettsregler vedrørende barns personvern er en nødvendig men ikke tilstrekkelig forutsetning for å oppnå et tilfredsstillende vern. Særlig overfor denne gruppen er det i tillegg behov for en aktiv formidling av gjeldende regler.[257] Klare regler vil imidlertid gjøre dette formidlingsarbeidet langt lettere enn med dagens uavklarte rettssituasjon. Selv om retningslinjer fra involverte myndigheter kan innebære en god hjelp til å finne akseptable løsninger, er en praksis som baserer seg på retningslinjer for å avklare sentrale rettsspørsmål lite tilfredsstillende. Mange vil oppfatte retningslinjene som "lov" til tross for at tilsynsmyndighetene ikke er gitt kompetanse til å gi bindende regler. Etter vår mening gir en situasjon der "regelmyndighet" og håndhevelsesmyndighet er forskjellige, den beste rettssikkerheten både for de registrerte og for behandlingsansvarlige. Hovedbestemmelsene når det gjelder barns personvern bør derfor fortrinnsvis gis som lov- eller forskrift av vedkommende departement eller av Kongen, mens tilsynsmyndighetene primært bør forklare og formidle regelinnholdet, samt kontrollere etterlevelsen.

[256] Lov 17. juli 1998 nr. 61.

[257] Jf. også det vi skriver i avsnitt 5.6.

# Kapittel 12

## Spørsmål vedrørende lovstruktur, forholdet til offentlighetsloven mv.

### 12.1 Om mandatet

I rammen gjengir vi mandatets punkt 11 med vår markering av konkrete spørsmålsstillinger (i fet skrift):

> *Strukturen i personopplysningsloven og forholdet mellom personopplysningsloven, særlovgivningen og personopplysningsforskriften*
>
> Utrederne bes ta stilling til hvorledes **forholdet mellom personopplysningsloven og særlovgivningen** bør være, og hvilke spørsmål som bør reguleres i hvilke regler. I denne forbindelse bes utredet noen **overordnede retningslinjer for valg av struktur** i forholdet mellom personopplysningsloven og mer spesialisert lovgivning, og i forholdet mellom personopplysningsloven og personopplysningsforskriften. Det er en forutsetning at Datatilsynets tilsynsansvar ikke skal påvirkes av valget av lovstruktur.
>
> Utrederne bes se særskilt på **forholdet mellom offentlighetsloven og personopplysningsloven**, jf. personopplysningsloven § 5. Henvendelser til Datatilsynet og Justisdepartementet tyder på at det er behov for å klargjøre forholdet mellom lovene ytterligere. Vurderingene bør knytte seg til en ny offentlighetslov, jf. Ot.prp. nr. 102 (2004–2005).
>
> Utrederne kan også vurdere enkelte sider ved den **interne strukturen og personopplysningslovens oppbygging**, i den utstrekning det aktualiseres ved vurderingen av forholdet mellom loven og forskriften, og ellers hvor det er begrunnet i hensynet til logisk oppbygging og klarhet. Departementet antar dette kan være særlig aktuelt i forhold til bestemmelser som gir rettigheter til den registrerte, som for eksempel retten til innsyn, retting og sletting.

Dette mandatpunktet er potensielt meget omfattende og krevende. Selv om mandatet legger vekt på overordnede og prinsipielle forhold, er det nødvendig å ha forholdsvis god oversikt over hvorledes våre forslag til retningslinjer mv. faktisk vil virke, for eksempel i forhold til de mange regelverk som inngår i særlovgivningen. Vi har valgt å gi en fremstilling i forhold til særlovgivning uten å gi et stort antall referanser til konkrete regelverk. Vi har likevel sett igjennom et større antall særlige regelverk og enkeltregler enn det referansene direkte viser.

I diskusjonen av forslaget til ny offentlighetslov, har vi også trukket inn enkelte spørsmål som også gjelder forvaltningsloven, særlig når det gjelder fvl § 13 om taushetsplikt. Relasjonen mellom personopplysningsloven og forvaltningsloven kunne vært gjenstand for en bredere vurdering enn den vi her har valgt, men vi har valgt å forstå mandatet slik at det ikke innebærer ønske om en total gjennomgang av forholdet mellom de to lovene.

Når det gjelder den interne strukturen i personopplysningsloven og -forskriften, og forholdet mellom loven og forskriften, er dette fortløpende berørt gjennom flere av drøftelsene og

forslagene i de foregående kapitlene i denne rapporten. Her vil vi derfor legge vekt på spørsmål vedrørende generelle interne strukturspørsmål. Våre konkrete forslag til lov-endringer ellers, skal selvsagt være i harmoni med de generelle anbefalingene, men vi har ikke tatt oss tid til å dokumentere slikt samsvar ved å rekapitulere standpunkt i tidligere deler av denne utredningen.

I mandatet blir det understreket at Datatilsynets tilsynsansvar ikke skal påvirkes av valg av struktur. Selv om det er nevnt i samband med særlovgivning, har vi forstått dette som en generell begrensning for de spørsmål som er omhandlet i dette kapittelet. Vi har likevel funnet det nødvendig å diskutere enkelte sider ved utøvelse av forskriftskompetanse, se avsnitt 12.3.2. Avgrensingen i mandatet gjør imidlertid at vi ikke går særlig inn på forholdet mellom utøvelse av tilsyns- og forskriftskompetanse.

## 12.2 Forholdet mellom personopplysningsloven og *eksisterende* særlovgivning

### 12.2.1 Innledning og oversikt

For å kunne analysere forholdet mellom personopplysningsloven og særlovgivning, er det nødvendig å ta stilling til hvilke deler av særlovgivningen som det kan være relevant å trekke inn i vurderingen. I utgangspunktet gjelder veldig mange regelverk behandling av personopplysninger – enten eksplisitt eller implisitt – ved at personopplysninger er beslutningsgrunnlag, gjenstand for rapportering til offentlige myndigheter mv. I denne sammenheng er det imidlertid også mulig å avgrense "særlovgivning" til slike lover som gir regler av samme karakter som personopplysningsloven; som enten supplerende eller gir alternative regler. Vi tror det er viktig at det blir foretatt en kategorisering av regelverk og enkeltregler som grunnlag for en diskusjon av lovstruktur på dette området, og antar det kan være hensiktsmessig å gjøre bruk av følgende fire kategorier som utgangspunkt:

- Lovregler som gir hjemmel til å behandle personopplysninger;
- Lovregler som gir anvisning på/forutsetter bruk av personopplysninger;
- Lovregler som regulerer tilgang til personopplysninger;
- Lovregler som gir anvisning på hvordan personopplysninger skal behandles (herunder; sikres).

Vi understreker at kulepunktene snarere angir "tyngdepunkter" enn skarpt adskilte kategorier. Grupperingen danner grunnlag for inndelingen av den følgende drøftelsen, og hver enkelt gruppe blir forklart nærmere i avsnittene nedenfor. Det er grunn til å understreke at vi skiller mellom typer av *enkeltregler*, og ikke mellom typer av regelverk. Det er forholdsvis få andre (hele) regelverk som regulerer behandling av personopplysninger, og de som finnes gjelder lover og forskrifter vedrørende sentrale registre som folkeregisteret, strafferegisteret og flere av helseregistrene.[258] Disse regelverkene avviker fra personopplysningsloven, bl.a. ved at de ikke har personvern som eneste formål. Reglene er derfor i stor grad begrunnet ut i fra funksjonelle krav knyttet til det som må anses å være primærformålet. I noen tilfelle er deler av et regelverk (kapittel e.l.) viet spørsmål om behandling av personopplysninger.[259] I de

[258] De fleste forskrifter om helseregistrene er hjemlet i helseregisterloven.

[259] Se f.eks. merverdiavgiftsloven 19. juni 1969 nr. 66 kapittel VII.

fleste tilfellene fremkommer imidlertid særreguleringene som enkeltbestemmelser i regelverk som primært gjelder andre spørsmål enn personvern.[260]

I denne gjennomgangen dekker "særlovgivning" også forskrifter som regulerer behandling av personopplysninger. Forskrifter blir forholdsvis ofte anvendt på dette området, og valget mellom plassering i lov eller forskrift har vært avhengig av så mange konkrete og tidsbestemte hensyn, at det neppe kan sies å være noe fast mønster mht. hvilket nivå som er valgt.

Personverndirektivet innebærer en forpliktelse til å endre norsk lovgivning i samsvar med direktivet. Vi er ikke kjent med at det er foretatt noen gjennomgang av relevant særlovgivning med tanke på å sikre slikt samsvar. De aller fleste særreguleringer har imidlertid et slikt innhold at de neppe kommer i motstrid med direktivet og personopplysningsloven. Det er imidlertid en utfordring å sikre at det er tilstrekkelig kunnskap om at personopplysningsloven gjelder i tillegg til særlovgivningen. Enkle søk i lover og forskrifter viser at det er forholdsvis få henvisninger til personopplysningsloven fra andre lover og forskrifter. Et forsiktig anslag peker i retning av at mindre enn 1/5 av særlover og -forskrifter som regulerer behandling av personopplysninger har henvisning til personopplysningsloven.[261]

Personopplysningsbegrepet er vidt og vagt, og det er derfor stor mulighet for at de som behandler registre ikke tenker på at de har med personopplysninger å gjøre. For å sikre etterlevelse av loven kan det derfor være grunn til å vurdere om det bør gjennomføres lov- og forskriftsendringer der en setter inn hensiktsmessige henvisninger til personopplysningsloven, for på den måten å tydeliggjøre at denne loven supplerer den særlige reguleringen.

### 12.2.2 Lovregler som gir hjemmel til å behandle personopplysninger eller som gir anvisning på/forutsetter bruk av personopplysninger

Mange lovregler gir hjemmel til å samle inn og behandle personopplysninger. Disse vil ofte gjelde etablering av "registre", men hjemmelen kan også gjelde annen rett til å innhente informasjon (typisk for en forvaltningsmyndighet), uavhengig hvorledes denne informasjonen er organisert. En oversikt over særregler vedrørende behandling av personopplysninger finnes på <http://www.personvern.uio.no/pvpn/regler/index.html>, og viser ca. 100 forekomster av enkeltregler eller regelverk som hjemler opprettelse av registre mv.[262] Personopplysnings-loven inneholder ikke selv noen slike hjemler, men loven viser til mulige lovhjemler, jf. særlig §§ 8 første ledd og § 9 første ledd bokstav b og avsnitt 6.3 (foran).

Særlige forvaltningslover og mange andre lovreguleringer ellers, bygger på en forutsetning om at det skal samles inn personopplysninger som (særlig) skal inngå som faktisk beslutningsgrunnlag, for eksempel for enkeltvedtak (jf. fvl § 2 første ledd, bokstav b, jf. a). Slik særlovgivning har ofte også egne saksbehandlingsregler, som gjelder generelle krav til

---

[260] I bygdealmenningsloven 19. juni 1992 nr. 59 heter det f.eks. i § 2-5 at det for "hver bygdeallmenning [skal] føres et register over eiendommer med tilliggende bruksrett. Registeret skal inneholde opplysninger om dyrket areal, om foretatte tildelinger av ytelser fra allmenningen og hvem som til enhver tid utøver bruksretten".

[261] Anslaget er gjort på grunnlag av søk i Lovdatas baser over lover og sentrale forskrifter etter "personopplysningslov". Det er ca. 100 lov- eller forskriftsbestemmelser som hjemler personregistre, se avsnitt 12.2.5. I tillegg kommer andre reguleringer som ikke er knyttet til registerbegrepet.

[262] Oversikten er ikke oppdatert og omfatter bare hjemler for å opprette personregistre. Tallet er derfor bare et grovt anslag, men samlet antall hjemler for å behandle personopplysninger, er uansett trolig over 100.

behandling av personopplysninger og saksutredning ellers. Et av mange eksempler på slik lovgivning er ligningsloven som inneholder en rekke bestemmelser vedrørende hvorledes personopplysninger skal behandles. Det er ingen generell henvisning til personopplysningsloven i ligningsloven, men i § 3-13 nr. 6 er det tatt inn en eksplisitt henvisning vedrørende visse eksterne aktørers plikt til å følge personopplysningslovens regler. Heller ikke i tolloven[263] med tilfhørende forskrifter er det vist til personopplysningsloven, selv om disse regelverkene inneholder sentrale bestemmelser om behandling av personopplysninger, og som personopplysningsloven er et viktig supplement til.

Det er avgjørende for klarhet i denne delen av lovstrukturen at det i de to nevnte typer særlovgivning er gitt henvisninger til personopplysningsloven, eventuelt til lovens forskrifter. Særlig er dette viktig å gjøre innen særreguleringer som har alminnelige regler om behandling av personopplysninger som kan komme i motstrid med personopplysningslovens regler.

### 12.2.3 Lovregler som regulerer tilgang til personopplysninger

En lang rekke enkeltregler og enkelte regelverk regulerer tilgang til personopplysninger (eller opplysninger mer generelt). Dette gjelder særlig bestemmelser vedrørende taushetsplikt, innsynsrett, opplysningsplikt, opplysningsrett, meldeplikt mv. Personopplysningsloven har enkelte vidtfavnende regler vedrørende innsynsrett for registrerte personer (§ 18) og informasjonsplikt overfor registrerte for behandlingsansvarlige (§§ 19 og 20). Loven har bare taushetspliktregler for medarbeidere i Datatilsynet og Personvernnemnda (§ 45).

For mange mennesker er taushetsplikt en helt sentral del av personvernet. Fordi taushetsplikt stort sett er fraværende i personopplysningsloven, kan være vanskelig å forstå hvorledes ulike taushetsplikter passer inn og samspiller med personopplysningslovens bestemmelse. Forutsetningen for personopplysningsloven er at den skal kunne leses og forstås av brede lag av befolkningen. Mange av disse vil ikke ha slik oversikt over lovgivningen som kreves for å forstå sammenhengene mellom ulike regelverksstrukturer. Vi mener derfor det kan være grunn til å vurdere om det bør settes inn en bestemmelse i personopplysningsloven som ”folkeopplysning” og påminnelse om forholdet mellom personopplysningsloven og lovbestemt taushetsplikt i særlovgivning. Dette kunne for eksempel skje ved at det blir satt inn en presisering i § 8. I avsnitt 6.8 (foran) har vi tidligere foreslått en ”regibestemmelse” med ordlyden:

> **§ 8 Generelt om krav til rettslig grunnlag for å behandle personopplysninger**
>
> For å være lovlig, må behandling av personopplysninger alltid ha et rettslig grunnlag i medhold av bestemmelsene i §§ 8 – 8d i denne loven. Det rettslige grunnlaget skal vurderes og fastsettes ut i fra ett eller flere formål, se § 9.

Spørsmålet om taushetsplikt kan introduseres i personopplysningsloven som del av denne bestemmelsen. Således kan loven invitere rettsanvendere til å undersøke om det foreligger taushetsplikt, som en innledende del av undersøkelsen av rettslig grunnlag i forslagets §§ 8 – 8d:

[263] Lov 10. juni 1966 nr. 5.

> **§ 8 Generelt om krav til rettslig grunnlag mv. for å behandle personopplysninger**
>
> For å være lovlig, må behandling av personopplysninger alltid skje:
> (a) innenfor rammene av bestemmelser om taushetsplikt i lov og forskrift, og
> (b) ha et rettslig grunnlag i medhold av bestemmelsene i §§ 8 – 8d i denne loven. Det rettslige grunnlaget skal vurderes og fastsettes ut i fra ett eller flere formål, se § 9.

En slik bestemmelse vil kunne medvirke til at behandlingsansvarlige leter etter og tar hensyn til eventuelt lovbestemt taushetsplikt. Dette er en aktivitet som uansett må skje for å overholde § 13 om sikring av personopplysninger, og spesielt pof § 2-11 om sikring av konfidensialitet.

### 12.2.4 Lovregler som gir anvisning på hvordan personopplysninger skal behandles

I mars 2006 var det kun helseregisterloven som representerte en bred rettslig regulering av behandling av personopplysninger innen et spesielt saksområde. Denne loven er i hovedsak bygget opp i henhold til samme systematikk og begreper som personopplysningsloven, og har personopplysningsforskriften som forskrift (i tillegg til andre forskrifter). Det er mao. lagt opp til en meget stor grad av likhet mellom helseregisterloven og personopplysningsloven som ”mønsterlov”. Som vi kommer tilbake til i neste avsnitt, mener vi generelt at det på utvalgte områder kan være riktig og nødvendig å gjennomføre særregulering av personvernspørsmål i lov- eller forskrifts form. Vi mener imidlertid helseregisterloven ikke er et eksempel til etterfølgelse, og vil her punktvis ta opp noen spørsmål som viser strukturproblemer knyttet til denne formen for særlovgivning.

Helseregisterloven er basert på et *forslag* til personopplysningslov, og de to lovene er meget like når det gjelder internstruktur, begreper (legaldefinisjoner) og innhold i de fleste bestemmelser. I tillegg gjelder personopplysningsloven med forskrifter som utfyllende bestemmelser, se hrl § 36. Denne anvendelsen av personopplysningslov- og forskrift skaper et generelt behov for å forstå 1) forskjellene mellom de to lovene og 2) hvor utfyllende helseregisterloven er i forhold til personopplysningslov og -forskrift. Kort sagt må rettsanvendere – for å være på den sikre siden – ofte forholde seg til begge lover samtidig.

Det største problemet oppstår når personopplysningsloven med forskrifter har en bredere regulering enn helseregisterloven. I så fall oppstår spørsmålet om forskjellen skyldes at lovgiver har ment at de bestemmelser som mangler i helseregisterloven ikke bør gjelde på denne lovens område. Alternativt kan lovgiver ha ment at bestemmelsene i personopplysningsloven og -forskrifter skal gjelde fullt ut, men at disse ikke er tatt inn i helseregisterloven fordi det har vært ansett å være uhensiktsmessig å gjenta personopplysningslovens bestemmelser, f.eks. fordi en har ansett de utelatte bestemmelsene som lite praktisk viktige. I pol § 21 er det f.eks. en bestemmelse om informasjon ved bruk av personprofiler. Helseregisterloven har ingen slik bestemmelse, men samtidig skal personopplysningsloven være ”utfyllende” bestemmelser i henhold til hrl § 36. Betyr det at pol § 21 får anvendelse, eller skyldes utelatelsen at en ikke ønsket å ha en slik informasjonsplikt innen helsetjenesten? Spørsmålet kan ikke løses uten å lese forarbeidene til helseregisterloven. Imidlertid kan det være vanskelig å få noe godt svar på slike spørsmål

som gjelder utelatelser i loven. Således er spørsmålet om personprofiler for eksempel ikke kommentert i merknadene til den enkelte bestemmelse i helseregisterloven.[264]

Et lignende sammenligningsproblem oppstår i enkelte tilfelle der bestemmelsen er nesten like, for eksempel når det gjelder legaldefinisjoner. I helseregisterloven er "behandling" (av helseopplysninger) definert slik:

> behandling av helseopplysninger: enhver *formålsbestemt* bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter (vår kursiv, se § 2 nr. 5).

I personopplysningsloven lyder tilsvarende bestemmelse:

> behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter (se § 2 nr. 2).

En grunnleggende forskjell her er at bruken i følge helseregisterloven skal være "formålsbestemt", mens tilsvarende krav er ikke uttrykt i personopplysningsloven. Et slikt klart avvik må forventes å innebære at det er reelle forskjeller mellom de to bestemmelsene. Forskjellen har imidlertid ingen materiell betydning, og skyldes at helseregisterloven ble formulert på grunnlag av forslag til personopplysningslov i Ot.prp. nr. 92 (1998–1999), der ordet "formålsbestemt" var med i definisjonen. Dette ordet ble imidlertid fjernet fra personopplysningsloven under komitébehandlingen.[265]

Et annet vesentlig problem gjelder endring og styrbarhet. Særlovgivning som er bygget opp i henhold til samme struktur, begrepsbruk og innhold som personopplysningsloven kan tenkes å lede til en viss rigiditet i forhold til endring. Dersom en i utgangspunktet har tilstrebet likhet mellom reglene, er det sannsynlig at hensynet til å bevare denne likheten vil være et vesentlig argument som taler mot endring. Dette gjelder også i tilfelle der personopplysningsloven ønskes endret, med den konsekvens at det oppstår nye forskjeller mellom denne og særlovgivning som er skrevet over samme lest. For eksempel kan det forhold at helseregisterloven ligner personopplysningsloven, være argument mot vårt radikale forslag til endret personopplysningslov. Argumentet kan for eksempel være at lovene fortsatt bør være mest mulig like hverandre, og at forslag til endringer i personopplysningsloven bare må vedtas dersom tilsvarende endring kan skje i helseregisterloven, eller dersom nye forskjeller mellom lovene ikke får nevneverdig betydning. Spørsmålet blir særlig vanskelig på grunn av hrl § 36 og personopplysningslovens utfyllende funksjon i forhold til helseregisterloven.

Denne begrensede drøftelsen av problemer knyttet til særlovgivning som er utformet etter mønster fra personopplysningsloven, gir etter vår mening grunnlag for å advare mot de lovgivningstekniske valgene som er gjort ved utforming av helseregisterloven. Som vi straks kommer tilbake til, mener vi at det på flere viktige områder kan være grunn til å vurdere særlig regulering av personvernspørsmål. Dette bør imidlertid *ikke* skje ved hjelp av regelverk som har personopplysningsloven som mønster og utfyllende regelsett, slik tilfellet er for helseregisterloven.

---

[264] Se Ot.prp. nr. 5 (1999–2000) kapittel 15.

[265] Se Innst. O. nr. 51 (1999–2000) avsnitt 4.1.

### 12.2.5 Særlig om behov for gjennomgang av "registerlover" mv.

Eksisterende ”registerlover” og ”-forskrifter” er i stor grad levninger fra personregisterlovens dager. Etter vår mening er det behov for en gjennomgang av denne delen av regelverket for å undersøke behovet for endringer som kan tydeliggjøre (i) eventuelle sammenhenger mellom særreglene og personopplysningslovens og -forskriftens bestemmelser, og (ii) vurdere behov for ytterligere særregler i lys av de generelle bestemmelsene. Av mange eksempler kan vi nevne gjeldsordningsloven.[266] Lovens § 7-1 om registrering av gjeldsordninger mm., gjelder behandling av personopplysninger, men det fremgår ikke direkte av ordlyden. Bestemmelsen inneholder regler vedrørende vilkår for registrering og sletting av opplysninger. Det kan åpenbart være behov for å klargjøre forholdet til pol §§ 8 og 28, og dessuten gi en generell henvisning til personopplysningsloven.

En gjennomgang av registerlover og -forskrifter kan om mulig skje som ”dugnad” der alle departementer gjennomgår slike regler innen sitt ansvarsområde, og vurderer i forhold til et sett felles retningslinjer, jf. gjennomgangen vedrørende krav til skriftlighet og underskrift i lovgivningen.[267]

## 12.3 Forholdet mellom personopplysningsloven og *fremtidig* særlovgivning

### 12.3.1 Nærmere om behovet for særlovgivning

Personverndirektivet og (dermed) personopplysningsloven gjelder all behandling av personopplysninger innen de aller fleste samfunnsområder. Personopplysningsbegrepet er meget vidt og behandlingsbegrepet er meget vidt, noe som til sammen bidrar til å gjøre det saklige virkeområdet svært omfattende. Vi har med andre ord med en lov å gjøre som skal anvendes på skrift, lyd, bilde mv., enten den behandlingsansvarlige er den lokale idrettsforeningen eller Telenor. Et slikt spenn kunne la seg håndtere dersom lovgivningen var begrenset med et enkelt innhold. Personopplysningsloven er imidlertid omfattende med til dels komplekse regler i lov og forskrift. Lovreguleringens brede spenn gjør at reglene er formulert så generelt at de skal kunne passe på den myriaden av saksforhold som loven regulerer. Dette fører til en begrepsbruk mv. som befinner seg på et så overordnet nivå at det kan være vanskelig å forstå hva dette konkret betyr for den enkelte behandlingsansvarlige og registrerte person.

Sentrale ord som ”behandling” og ”behandlingsansvarlig” illustrerer hvor høyt over bakkeplanet loven befinner seg: Hva betyr disse begrepene på en ungdomsskole? De fleste vil trolig være i tvil om hva de rettsriktige svarene etter loven er. Det sier seg selv at dette hadde vært langt lettere dersom en gav rettsregler som spesielt gjelder skoleverkets behandling av personopplysninger. Da kunne man fastlagt at det var kommunen som hadde ansvaret for personopplysningene, at ansvaret kunne delegeres til rektorer på hver skole (jf. ”behandlingsansvarlig”), og at reguleringen gjaldt personopplysninger som inngår i elektroniske læringsplattformer og skoleadministrative systemer (jf. ”behandling”). Bestemmelsene kunne med andre ord gis helt konkret slik at innholdet i stor grad var umiddelbart gjenkjennelig for de som ble direkte berørt av reglene.

---

[266] Lov 17. juli 1992 nr. 99.

[267] Se Ot.prp. nr. 108 (2000–2001) om lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon.

Enkel gjenkjennelighet ved lesing av lovens regler er et vesentlig poeng fordi loven forutsetter at alle behandlingsansvarlige, databehandlere og registrerte personer (dvs. "folk flest") skal kunne forstå og etterleve den. Dersom denne forutsetningen svikter, kan det føre til at aktuelle aktører gir opp eller bare sporadisk eller halvhjertet gjør forsøk på å være lovlydig. Virksomhetsundersøkelsen vedrørende personvern, gir klare indikasjoner på at dette er situasjonen for mange behandlingsansvarlige.[268] For den delen av befolkningen som prøver å følge lovens bestemmelser, vil det lett oppstå sterkt behov for å få konkretisert implikasjonene av loven på bestemte, viktige områder. Datatilsynet vil i den situasjonen være nærmest til å gjøre dette, og resultatet blir en rekke avgjørelser som forklarer hvordan lov og forskrift virker på bestemte problemområder. Datatilsynet bidrar til å klargjøre rettsspørsmål ved hjelp av standardkonsesjoner, retningslinjer, tolkingsuttalelser og ulike artikler mv. på tilsynets nettsider.

Vi vil ikke her foreta en nærmere vurdering av Datatilsynets bidrag til å klare opp i de mange vanskelige rettsspørsmål som den generelle lovteksten etterlater seg. Det er imidlertid helt klart at loven slik den nå er, gjør utstrakt informasjons- og veiledningsvirksomhet fra Datatilsynet helt nødvendig. Etter vår mening er det imidlertid prinsipielt uheldig at Datatilsynet på denne måten både regulerer og kontrollerer i spørsmål som er av vesentlig betydning for folks rettsstilling. Selv om "retningslinjene" ikke kan anses som bindende forskrifter, og konsesjonsvedtakene skal være enkeltvedtak som konkret forholder seg til hver behandlingsansvarlig/behandling, vil Datatilsynets generelle utlegninger av rettsspørsmål likevel lett kunne oppfattes som gjeldende rett. Slike retningslinjer kan heller ikke sies i særlig grad å stimulere til demokratisk debatt, og må generelt antas å ha svakere legitimitet enn regler i lov eller forskrift.

Vi vil understreke betydningen av at Datatilsynet redegjør for uavklarte rettsspørsmål. Vårt poeng er at det er alt for mye å uttale seg om, fordi loven etterlater for stor usikkerhet i forhold til mange konkrete anvendelser. Når tilsynet uttaler seg, er det ikke til å unngå at dette ofte får gjennomslag fordi Datatilsynet har rollen som spesialist og myndighet på området. Vårt poeng er at uklarhetene er så store at Datatilsynets forklaringer snarere kan forstås som *nye regler* enn fortolkning av eksisterende. Det bør være en målsetting å flytte vesentlige normerende funksjoner bort fra Datatilsynet og over til *politiske myndigheter*. Begrunnelsen er primært at dette kan gi en demokratisk prosess fordi en gjennom høringsinstituttet får en bred og opplyst debatt om forslag til nye lov/forskrifter. På den måten kan en også få en bredere og dypere utredning av faktiske og rettslige spørsmål enn det Datatilsynet kan klare alene, og reguleringen kan bidra til å øke bevissthetsnivået om og legitimiteten av den rettslige reguleringen.

### 12.3.2 På hvilket myndighetsnivå bør særregler gis?

Da personopplysningsloven ble vedtatt, ble alle forskriftshjemler lagt til Kongen. I Ot.prp. nr. 92 (1998–99) fremholdt departementet i avsnitt 13.2.4 at bestemte deler av forskrifts-myndigheten kunne delegeres til Datatilsynet. Justiskomitéen understreket imidlertid at "det ved en slik delegering fortsatt vil være statsråden som er formelt ansvarlig for regelverket".[269] Komitéens merknad er en påminnelse om at delegasjon ikke innebærer en fraskrivelse av ansvar for forskriften, men tvert i mot innebærer at den delegerende myndigheten øver tilsyn med hvorledes forskriftskompetansen utøves. Dersom den delegerende myndigheten er uenig

[268] Se Ravlum 2005b og omtalen av undersøkelsen i kapittel 1 (ovenfor).

[269] Se Innst.O. nr. 51 (1999–2000) avsnitt 13.

i måten kompetansen brukes på, innebærer ansvaret at den som har fått delegert myndighet kan instrueres om å gjøre endringer.

Delegasjon forutsetter et overordningsforhold mellom den delegerende (Kongen, eventuelt et departement) og den myndighet det delegeres til (Datatilsynet). Datatilsynet er imidlertid en uavhengig forvaltningsmyndighet, og "Kongen og departementet kan ikke gi instruks om eller omgjøre Datatilsynets utøving av myndighet i enkelttilfeller etter loven" (jf. pol § 42 første ledd).

I personverndirektivet artikkel 28 heter det at "authorities shall act with complete independence in exercising the functions entrusted to them". Direktivet forutsetter ikke at tilsynsmyndigheten skal gi bindende regler, men angir spesielt "monitoring", "investigative powers", "effective powers of intervention" og "power to engage in legal proceedings". Direktivet omhandler med andre ord ikke spesielt uavhengighet i forhold til utøvelse av delegert forskriftsmyndighet, og det er derfor usikkert hvorledes direktivet skal forstås på dette punktet.

Etter vår mening gjør pol § 42 første ledd det problematisk å delegere forskriftsmyndighet til Datatilsynet fordi instruksjon fra Kongen eller departementet ikke skal kunne skje. Vi mener den beste løsningen vil være å beholde forskriftskompetansen på det politiske nivået (dvs. i vedkommende departement eller Kongen), slik at Datatilsynets rolle som uavhengig tilsyn rendyrkes. En slik kompetansefordeling er selvsagt ikke til hinder for at Datatilsynet (eventuelt sammen med andre) utfører *saksforberedende* oppgaver for departementet/Kongen. Poenget er at vedtaket og ansvaret tydelig må plasseres på et politisk nivå.

### 12.3.3 Den systematiske plasseringen av særregler og konkret tildeling av forskriftskompetanse

I dette avsnittet ser vi nærmere på to spørsmål som vi anser det er hensiktsmessig å vurdere i sammenheng. Det første spørsmålet gjelder den systematiske plasseringen av særregler innen personopplysningsretten, dvs. spørsmålet om slike regler bør gis i eller i medhold av lov eller forskrift. Dersom forskriftsformen velges, blir spørsmålet hvordan slike forskrifter bør hjemles. Det andre spørsmålet gjelder ansvar for utarbeidelse av særregler. Vi er selvsagt klar over at de nevnte valgene vil avhenge av en rekke konkrete vurderinger, men vil likevel argumentere for en så fast praksis som mulig, dvs. en praksis som kan gjøre det mulig å ha begrunnede forventninger om hvor og hvordan særregler er gitt.

Når det gjelder systematisk plassering, mener vi at særregler enten bør gis som egen lov, eller gis med hjemmel i en lov som har (tilnærmet) samme saklig virkeområde som særreglene. Vi mener det primært er forskriftsformen som bør velges. Lov kan særlig vurderes anvendt i fire typetilfelle:

(i) *Særregler gjelder et saksområde som har spesielt stor betydning for ivaretakelsen av personvern*. Et offentlig utvalg har foreslått en særlov vedrørende medisinsk og helsefaglig forskning, som inneholder bestemmelser vedrørende personvern på en måte som er integrert med regulering av andre forhold.[270] Vi tror ikke det er mange andre saksområder som kan forsvare slik egen lovgivning.

[270] Se NOU 2005: 1 *God forskning – bedre helse*.

(ii) *Særregler om behandling av personopplysninger som settes inn i eksisterende særlover*. Vi antar at behovet for slikt lovarbeid er forholdsvis stort. Således kan det for eksempel være behov for å vurdere særregler vedrørende behandling av personopplysninger i forvaltningsloven, offentlighetsloven, annen særlig forvaltningslovgivning og lovgivning vedrørende visse former for næringsvirksomhet mv. Det er neppe trolig at det i slike tilfelle vil være behov for omfattende særregler. Behovet gjelder trolig avklaring av sentrale spørsmål, samt presiseringer og suppleringer av de generelle reglene i personopplysningslov og -forskrift. Det kan for eksempel være behov for å fastsette hvem som er behandlingsansvarlig, og konkretisere/supplere regler om innsynsrett, informasjon mv.

(iii) *Særregler som hovedsakelig gjelder registrertes rettigheter bør om mulig plasseres i lov*. Det vil ofte være uhensiktsmessig å skille rettighetsbestemmelser ut fra andre bestemmelser, og dette kan være argument for at også andre (tilhørende) bestemmelser plasseres på lovnivået. Dersom rettigheter plasseres i forskrift, bør det i hjemmelsloven settes inn en bestemmelse der det tydelig fremgår at rettighetsbestemmelser er satt inn i forskrift til loven.

(iv) *Særregler innen områder som i dag er omfattet av "registerlover"*. Det kan være behov for å revidere eksisterende registerlover for å bringe dem mer i samsvar med systematikk, begrepsbruk og innhold i personopplysningsloven. "Registertenkningen" henger fortsatt igjen i mye av de lover og forskrifter som særlig ble gitt da vi hadde personregisterloven. I NOU 2003: 21 *Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetens behandling av opplysninger*, ble det fremmet forslag til modernisert strafferegistreringslovgivning (politiregisterlov). Også andre registerlover bør på lignende måte vurderes oppdatert i samsvar med/under hensyn til personopplysningsloven.

Særregler bør primært gis som forskrift. Det første spørsmålet er når slik forskrift bør gis i medhold av personopplysningsloven og når annen lovgivning bør være hjemmel. Retningslinjen bør her være å hjemle forskrifter om generelle spørsmål vedrørende behandling av personopplysninger i personopplysningsloven, og hjemle særregler i adekvat særlov. Med generelle regler sikter vi til regler som dekker det saklige virkeområdet til mange særlover. Regler vedrørende barn og ungdoms personvern (generelt) bør eventuelt gis i medhold av personopplysningsloven, mens særlige regler vedrørende personvern for elever og studenter bør gis i medhold av hhv opplæringslova og universitets- og høgskoleloven.[271] Videre bør forskrift om arbeidsgivers tilgang til epost mv. gis med hjemmel i arbeidsmiljøloven[272] (som primært regulerer forholdet mellom arbeidsgivere og arbeidstakere), heller enn i personopplysningsloven (som har et langt videre virkeområde).

Det er særlig to begrunnelser for dette systematiske valget. For det første er det som tidligere nevnt ofte et behov for å kunne gi konkrete bestemmelser som lett lar seg kommunisere til dem som skal etterleve reglene. Dette vil ofte kreve at reglene vedrørende behandling av personopplysninger bør inngå som en integrert del av øvrige bestemmelsene på området. Regler vedrørende skoleverkets behandling av personopplysninger bør med andre ord stå i et avklaret forhold til reglene om de aktivitetene som begrunner denne innsamlingen.

Den andre begrunnelsen gjelder antagelse om eierskap til og kunnskap om regelverk. Etter vår mening er det grunn til å tro at det er lettere å få gjennomslag for og kommunisert regler som er plassert i eller i tilknytning til regelverk som de personene som skal etterleve

[271] Lov 1. april 2005 nr. 15.
[272] Lov 17. juni 2005 nr. 62.

bestemmelsene er vant til å følge. Det er med andre ord grunn til å anta at bankfolk kan banklovgivningen best, skolefolk kan skolelovgivningen best, og arbeidsgivers representanter og fagforeningsrepresentanter kan arbeidsmiljølovgivningen best osv. Dersom særregler gjelder en bestemt gruppe, og disse har "sin lov", er det med andre ord nærliggende å legge særreglene om personopplysninger til denne loven.

En slik plassering av særregler kan gjøre det vanskelig å skaffe fullstendig oversikt over aktuelle reguleringer av personopplysningsrett. Med mer enn 100 registerlover og -forskrifter mv., har det imidlertid for lenge siden blitt vanskelig å ha en slik oversikt. Det er dessuten primært myndigheter og andre større organisasjoner som har behov for fullstendig oversikt over aktuell lovgivning, og disse har uansett ressursmessige forutsetninger for å makte dette. Informasjonsmateriale og løpende føringer av oversikter over aktuelle regler, vil uansett kunne være et virksomt mottiltak.

Den systematiske plasseringen av lov- eller forskrift legger føringer på hvilket departement som får ansvaret for loven. En forskrift vedrørende IKT i skolen vil for eksempel sortere under Kunnskapsdepartementet. Datatilsynet kan likevel tenkes å få et hovedansvar for utredning og saksforberedelse i tilknytning til utarbeidelse av særreglene, og vil kunne gis myndighet til å føre tilsyn med etterlevelse av loven (eventuelt sammen med annet tilsynsorgan).[273] Etter vår mening vil plassering av særregler i egen lov eller i forskrift til eksisterende særlovgivning, ikke være til hinder for hensiktsmessig arbeidsdeling mellom Datatilsynet og andre myndigheter. Vi kommer imidlertid ikke nærmere inn på forutsetninger om organisering av samarbeid på tvers av forvaltningshierarkiet mv., jf. avgrensningen i mandatet for dette arbeidet.

### 12.3.4 Prinsipper for utforming av særregler

I dette avsnittet kommenterer vi kort spredte lovgivningstekniske spørsmål som aktualiseres av diskusjonen vedrørende forholdet mellom personopplysningsloven og særregler i lov og/eller forskrift.

En viktig teknikk for å sikre gjenkjennelighet og sammenheng mellom særlovgivning og personopplysningsloven er at en i størst mulig grad følger en systematikk som er felles for flest mulig regelverk innen personopplysningsretten. Dette innebærer at personvern-prinsippene som ligger til grunn for personverndirektivet og Europarådskonvensjonen og/eller personverninteressene i størst mulig grad bør ligge til grunn for tematisering/inndeling av rettsspørsmål.

I stedet for å vedta hele regelverk som dekker de samme spørsmål som personopplysningslovens, bør en fortrinnsvis ta sikte på å regulere særlige spørsmål som:

1. avviker fra personopplysningslovens bestemmelser, eller
2. innebærer konkretiseringer av personopplysningsloven innen saksfelt og konkrete problemstillinger som er av stor betydning.

Slike regler bør i størst mulig grad plasseres som deler av eksisterende lovgivning innen vedkommende saksfelt, og som fra før har bestemmelser vedrørende behandling av

[273] Således har Datatilsynet tilsynsmyndighet i henhold til helseregisterloven kapittel 6. Også Statens helsetilsyn har tilsyns-oppgaver i forhold til loven, se hrl §§ 31 første ledd og 32 første ledd.

personopplysninger (taushetsplikt, opplysningsplikt mv.), eller der slike regler ut i fra innholdet for øvrig kan passe inn. I tilfeller der det er behov for en sammenhengende rettslig regulering av personvernrelaterte spørsmål, kan disse med fordel organiseres i eget kapittel, men det er grunn til å anta at det forholdsvis ofte kun vil være behov for noen mer enkeltstående bestemmelser.

Når det gjelder punkt 1 (ovenfor) er disse mulighetene begrenset fordi personverndirektivet er detaljert og dekker bredt. Muligheten for å vedta avvikende regler gjelder særlig utenfor direktivets virkeområde,[274] og i den utstrekning det er aktuelt å gi et bedre personvern enn det personverndirektivet og personopplysningsloven etablerer. Når det gjelder særlovgivning ut i fra grunner som angitt i punkt 2 (ovenfor) kan dette tenkes å gjelde en rekke saksområder som kan sies å være av spesiell viktighet. Tidligere har vi nevnt behov for å konkretisere personopplysningsvernet for elever/studenter og arbeidstakere. Det kan også tenkes behov for konkretisering av lovlig behandling av personopplysninger i forbindelse med andre viktige forhold, f.eks. vedrørende veiprising mv., fjernsynsovervåking av kollektiv transport, bruk av biometriske metoder mv.

Dersom særregler gis, bør en alltid vurdere å formulere disse med *utgangspunkt i* legaldefinisjonene i pol § 2. Det bør imidlertid ikke være noe krav at eksakt like begreper benyttes, men begrepene bør om mulig være utledet av begrepene i personopplysningsloven, og således utgjøre en delmengde av disse. I stedet for "personopplysning", bør en med andre ord kunne velge "helseopplysning", "elevopplysning" osv., som relateres til definisjonen av "personopplysning" og således blir en underkategori av denne. På samme måte bør det ikke være påkrevet å benytte begrepet "behandling" av personopplysninger. I stedet kan det angis noen typer behandling (f.eks. innsamling, sammenstilling), uten at disse formene for behandling (nødvendigvis) blir eksplisitt definert i lovteksten. En bestemmelse kan for eksempel regulere innsamling av elevopplysninger, en annen regulerer sammenstilling av elevopplysninger mv. Den sentrale begrepsbruken i særregler behøver med andre ord ikke være identisk med den som finnes i personopplysningsloven, men særreglene bør forholde seg til definisjonene i pol § 2. Målsettingen må være å skape fleksible og klare sammenhenger mellom personopplysningsloven og særlige reguleringer av personvernspørsmål. Dersom definisjonene i § 2 anvendes direkte, bør det ikke forekomme umotiverte avvik, jf. eksempelet fra helseregisterloven (ovenfor).

Ytterligere en teknikk gjelder tydeliggjøring av henvisningsstrukturer mellom særregulering og personopplysningsloven. Når særregler definerer et begrep med utgangspunkt i en av personopplysningslovens legaldefinisjoner, bør det m.a.o. vises til sist nevnte definisjon, for eksempel:

> Elevopplysning: personopplysning og -vurderinger som kan knyttes til den enkelte elev, jf. pol § 2 nr. 1.

For å unngå uklarheter bør særreglene dessuten eksplisitt angi hvilke av personopplysnings-loven bestemmelser som ikke skal gjelde, for eksempel:

---

[274] Se artikkel 3 nr. 2: "2. This Directive shall not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law …".

> [særregel som avviker fra § 20] Innenfor virkeområdet for denne loven, gjelder ikke krav til informasjon i § 20 i lov om behandling av personopplysninger.

Henvisningene bør med andre ord være spesifikke, og man bør unngå generelle anvisninger på at personopplysningsloven skal gjelde som utfyllende bestemmelser mv.

Etter vår mening bør bestemmelser i særregler i størst mulig grad settes i den rekkefølge de normalt bør vurderes/utføres. I den grad det er nødvendig med bestemmelser med mer fragmentarisk karakter, bør en legge vekt på å gjøre interne henvisningsstrukturer eksplisitte.

Vi mener også det kan være en god idé å gjøre bruk av enkelte regler som inneholder informasjon om regelverkets oppbygging, dvs. bestemmelser som ikke nødvendigvis har en selvstendig materiell betydning. Personopplysningsloven § 11 første ledd bokstav a er et (mindre vellykket) eksempel på dette. Paragraf 8 i vårt radikale lovforslag er et eksempel på det vi mener er en bestemmelse som inneholder hensiktsmessig informasjon til leseren:

> **§ 8 Generelt om krav til rettslig grunnlag for å behandle personopplysninger**
>
> For å være lovlig, må behandling av personopplysninger alltid skje:
>
> a) innenfor rammene av bestemmelser om taushetsplikt i lov og forskrift, og
>
> b) ha et rettslig grunnlag i medhold av bestemmelsene i §§ 8 – 8d i denne loven. Det rettslige grunnlaget skal vurderes og fastsettes ut i fra ett eller flere formål, se § 9.

Slike "regibestemmelser" kan med fordel også vurderes for å klargjøre forholdet mellom særregler og personopplysningsloven.

Det bør alltid vurderes nøye om rettsregler skal formuleres som en rettighet for registrerte eller andre, eller om bestemmelsen snarere skal handle om behandlingsansvarliges oppfyllelse av plikter i forhold til den registrerte. Bestemmelsene om retting, sletting mv. i pol § 27 er for eksempel ikke formulert som en klar rettighet for den registrerte, og det oppstår derfor tvil om hva slags rolle registrerte personer skal ha i en slik sammenheng. Dersom spørsmålet har et rettighetsaspekt, bør dette om mulig komme til uttrykk i kapittelet som favner alle rettigheter.

Når det gjelder bestemmelser om rettigheter, bør disse i størst mulig grad settes i samme kapittel i vedkommende lov, gjerne sammen med relevante rettigheter som ikke direkte gjelder behandling av personopplysninger, men som kan ha betydning for denne. Rettigheter bør med andre ord i størst mulig grad presenteres samlet slik at det er lettest mulig å finne frem.

## 12.4 Spesielt om forholdet mellom personopplysningsloven og offentlighetsloven mv.

### 12.4.1 Innledning

I dette avsnittet tar vi opp forholdet mellom ny offentlighetslov[275] (lov om rett til innsyn i dokument i offentleg verksemd, heretter; "offl") og personopplysningsloven. Någjeldende offentlighetslov er ikke trukket inn i drøftelsen. Vi behandler først spørsmål vedrørende de to lovenes virkeområde. Oppmerksomheten er deretter rettet mot viktige berøringspunkter mellom de to lovene. Vi har stilt oss spørsmålet hvordan personopplysningsloven kan sies å virke inn på realiseringen av målet om åpenhet i offentlig virksomhet (jf. offl § 1), og har identifisert tre hovedgrupper av spørsmål:

- Personopplysningsloven kan ha betydning for innholdet av offentlige arkiver og hvilket materiale som det kan kreves innsyn i, se avsnitt 12.4.3;
- Personopplysningsloven kan ha betydning for i hvilken grad det kan gis offentlig innsyn i personopplysninger, se avsnitt 12.4.4;
- Personopplysningsloven har egne bestemmelser om innsynsrett for enhver, dvs. loven kan sies å utfylle offentlighetslovens innsynsrettigheter, se 12.4.5.

Til slutt i dette hovedavsnittet gir vi en kortfattet, samlet vurdering av forholdet mellom de to lovene, med vekt på forslag som kan bidra til harmonisering og avklaring av forholdet mellom dem (avsnitt 12.4.6). Forslagene blir sammenfattet i avsnitt 12.4.7.

Gjennomgangen i dette avsnittet innebærer ingen fullstendig vurdering av forholdet mellom de to lovene. Utgangspunktet er at både personopplysningsloven og offentlighetsloven kommer til anvendelse når innsynsbegjæringer i samsvar med offl § 3 innebærer behandling av personopplysninger.[276] En slik innsynssak kan for eksempel tenkes å utløse informasjonsplikt (pol § 20), og meldeplikt (pol § 31). Det vil også kunne være innsynsrett i personopplysninger på den innsynsberettigedes hånd (pol § 18 annet og tredje ledd) osv. Vi har ikke gjennomgått alle de situasjoner som kan oppstå når de to lovene anvendes i forhold til en innsynssak etter offentlighetsloven. Det betyr imidlertid ikke at slike situasjoner er uproblematiske.

### 12.4.2 Lovenes virkeområder mv.

Personopplysningslovens virkeområde avviker fra virkeområdet for ny offentlighetslov. Loven etablerer (med noen unntak) plikter for enhver som behandler personopplysninger, *uansett sektor*. Ny offentlighetslov etablerer plikter for staten, fylkeskommunene og kommunene samt visse andre rettssubjekter som treffer vedtak eller der stat, fylkeskommune eller kommune er involvert på nærmere angitte måter, se § 2. Dette innebærer at det ikke finnes noe del av forvaltningen eller offentlig virksomhet ellers som omfattes av offentlighetsloven uten samtidig å være omfattet av personopplysningsloven. Begge lover etablerer rettigheter for "enhver", men etter personopplysningsloven er det primært registrerte personer som har rettigheter.

---

[275] Jf. Ot.prp. nr. 9 (2005–2006).

[276] Jf. dog Lovavdelingens uttalelse vedrørende personopplysningsloven § 6 (Saksnummer: 2004/04600). Uttalelsen er nærmere drøftet i neste avsnitt.

Når det gjelder *saklig virkeområde*, er gjenstanden for regulering i personopplysningsloven hel eller delvis elektronisk behandling av personopplysninger samt behandling av personopplysninger som er eller skal inn i et personregister, se pol § 3. Dette innebærer at personopplysninger i papirdokumenter og andre analoge lagringsmedier som ikke er ordnet systematisk slik at personopplysninger om den enkelte kan finnes igjen, faller utenfor personopplysningsloven, samtidig som offentlighetslovens bestemmelser gjelder. Løse papirdokumenter og saksmapper med papirdokumenter mv. som er ordnet etter sakstype, kronologi og andre kriterier som ikke er knyttet til person, faller altså ikke inn under personopplysningsloven.[277] Dokumentene i en sak det skal gis innsyn i etter offentlighetsloven kan således tenkes å falle utenfor personopplysningsloven. Likevel kan begrensede deler av saken være omfattet, for eksempel fordi det er anvendt tekstbehandling for å utarbeide ett av dokumentene i en sak, eller fordi det er anvendt elektronisk kommunikasjon i tråd med fvl § 15a. Det kan virke uhensiktsmessig og tilfeldig at ulike dokumenter i én og samme forvaltningssak skal være undergitt ulike rettslige regimer vedrørende personvern.

Selv om personopplysningsloven ikke kommer til anvendelse på personopplysningene i saken det kreves innsyn i, kan loven komme til anvendelse på selve begjæringen om innsyn. Dette er i utgangspunktet tilfellet for en elektronisk henvendelse med begjæring om innsyn etter offentlighetsloven.

Gjenstand for regulering etter offentlighetsloven er forvaltningens "saksdokument, journalar og liknande register", se offl § 3. Loven bygger på samme definisjon av "dokument" som forvaltningsloven og arkivloven, dvs. "ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande", se offl § 4 første ledd.

Både dokumentbegrepet i offentlighetsloven og "behandling av personopplysninger" i personopplysningsloven er teknologi- og medieuavhengige begreper. Dette gjør at det ikke finnes noen "personopplysning" etter personopplysningsloven som ikke kan tenkes å være del av et "dokument" etter offentlighetsloven.

Personopplysningsloven har bestemmelser om *geografisk virkeområde* som eksplisitt tar høyde for den internasjonale karakteren som preger deler av vår tids informasjonsbehandling, se pol § 4. Således gjelder norsk lov (bare) i to situasjoner: (i) når den som behandler personopplysningene er etablert i Norge; og (ii) når den behandlingsansvarlige er etablert utenfor EØS samtidig som det benyttes utstyr (for annet enn transmittering) som er plassert i Norge. Dersom den behandlingsansvarlige er etablert i et EØS-land, gjelder vedkommende lands personopplysningslovgivning, *også for behandling av personopplysninger som skjer i Norge*. Personverndirektivet forutsetter at et lands tilsynsmyndighet (i Norge; Datatilsynet) kan håndheve et annet EØS-lands lovgivning på sitt territorium, og landenes tilsynsmyndigheter skal samarbeide, se direktivets artikkel 28 nr. 6. Det kan således for eksempel skje at det behandles personopplysninger i Norge for en behandlingsansvarlig som kun er etablert i Spania[278] Reglene for behandlingen av disse opplysningene, herunder kravene til kvalitet, sletting, utlevering (til norske forvaltningsorganer mv.) vil normalt (i eksempelet) følge spansk lov, som Datatilsynet kan håndheve i samarbeid med spanske myndigheter. Vi viser ellers til drøftelsen i kapittel 4.

[277] Se Ot.prp. nr. 92 (1998–99) s. 102.

[278] Behandlingen vil da for eksempel skje i regi av en databehandler som befinner seg i Norge, dvs. en virksomhet som behandler opplysningene på den behandlingsansvarliges vegne, se pol § 2 nr. 5.

I offentlighetsloven er det så vidt vi kan se ikke gjort forbehold om hvor rettssubjekter som kommer inn under loven[279] må være etablert, og det må derfor antas at ny loven også vil gjelde rettssubjekter som er etablert i utlandet. Vi antar at dette kan være aktuelt for enkelte selvstendige rettssubjekter som kommer inn under loven. I så fall vil ny offentlighetslov gjelde, men ikke den norske personopplysningsloven. Derimot vil personopplysningslovgivningen i landet der rettssubjektet (behandlingsansvarlig) er etablert gjelde. Selv om personverndirektivet utgjør en felles ramme for EØS-land, kan det her være forskjeller mellom landene.

Forholdet mellom offentlighetsloven og personopplysningslovgivning vil med andre ord variere avhengig av hvor rettssubjektet er etablert innen EØS. Dersom norske myndigheter for eksempel etablerer et selskap i Spania som skal arbeide for å øke tilstrømningen av spanske turister til Norge e.l.,[280] vil norsk offentlighetslov og spansk personopplysningslov gjelde. En person som det er registrert opplysninger om i Spania hos et norsk rettssubjekt som kommer inn under virkeområdet etter offl § 2, kan derfor hevde at opplysningen skal slettes etter spansk personopplysningslov, slik at det ikke kan gis innsyn i opplysningene etter norsk offentlighetslov. I andre tilfelle gjelder offentlighetsloven og personopplysningsloven samtidig. I fortsettelsen drøfter vi bare sist nevnte situasjon.[281]

I personopplysningsloven § 6 første ledd heter det:

> **§ 6. Forholdet til lovbestemt innsynsrett etter andre lover**
>
> Loven her begrenser ikke innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger.

I en uttalelse fra Justisdepartementets lovavdeling[282] heter det om denne bestemmelsen at:

> Dette innebærer at reglene i personopplysningsloven ikke kommer til anvendelse i den utstrekning offentlighetsloven eller annen lovgivning gir rett til innsyn i personopplysninger. I slike tilfeller skal det med andre ord gis innsyn uavhengig av vilkårene i personopplysningsloven kapittel II. Dette gjelder bare så langt offentlighetsloven eller annen lovgivning gir innsynsrett. I forhold til offentlighetsloven innebærer dette at personopplysningsloven ikke skal gjelde ved offentliggjøring av dokumenter som er omfattet av hovedregelen om innsynsrett i offentlighetsloven § 2 første ledd, og som ikke samtidig er omfattet av unntaksreglene i offentlighetsloven eller i annen lovgivning.

Det gis her med andre ord uttrykk for at personopplysningsloven *ikke gjelder* når innsyn skal skje i henhold til hovedregelen i offentlighetsloven. Innenfor rammene av meroffentlighet, hevder Lovavdelingen at personopplysningsloven og vilkårene i §§ 8 og 9 kommer til anvendelse, fordi innsynet i dette tilfellet beror på et skjønn og ikke en "rett", jf. formuleringen i pol § 6 første ledd ("innsynsrett"). Lovavdelingen bygger primært sin konklusjon på en fortolkning av pol § 6, noe som innebærer et tilsvarende resultat i forhold til den nye offentlighetsloven (som bygger på samme hovedregel og plikten til å vurdere meroffentlighet).

---

279 Disse betegnes "organ" i loven, se offl § 4 siste ledd.

280 Jf. den type rettssubjekter som er beskrevet i offl § 2 første ledd bokstavene c og d.

281 Det er også grunn til å foreta en nærmere grenseoppgang etter de to lovene i forhold til unntakene i pol § 3 annet ledd ("behandling av personopplysninger … for rent personlige eller private formål") og § 7 for opplysninger som behandles for formål som "utelukkende [er] kunstneriske, litterære, journalistiske, herunder opinionsdannende". Her har vi imidlertid ikke funnet å kunne gå inn på slike detaljer.

282 Saksnummer: 2004/04600, datert 16.07.2004.

Vi er uenig i Lovavdelingens fortolkning. Lovavdelingen trekker ikke direkte inn forarbeidene til personopplysningsloven. Her uttaler departementet at "[b]estemmelsen [§6] … understreker i *første ledd* at personopplysningsloven ikke innskrenker andre lovbestemte innsynsrettigheter".[283] Vi forstår dette som en uttalelse om personopplysningsloven ikke kan fortolkes slik at den innskrenker lovbestemt innsynsrett. Dette er prinsipielt forskjellig fra at loven "ikke kommer til anvendelse"/"ikke skal gjelde", slik Lovavdelingen uttrykker det. Vi velger derfor å legge til grunn at personopplysningsloven gjelder i forhold til innsyn i henhold til offentlighetsloven, også når innsyn skjer i forhold til hovedregelen i § 2 første ledd. Samtidig legger vi imidlertid til grunn at personopplysningsloven må fortolkes slik at den ikke innskrenker lovfestede innsynsrettigheter. Med en slik tilnærming vil innsynsberettigede personer få tilgang til like mye som etter Lovavdelingens fortolkning. Forskjellen ligger primært i en tydeliggjøring av plikten til å vurdere om det foreligger slik lovbestemt innsynsrett eller ikke.[284] Etter vår mening er det uansett uheldig å hevde at personopplysningsloven får anvendelse i forhold til noen deler av offentlighetsloven men ikke andre, fordi dette gir et unødig komplisert forhold mellom de to lovene. I nedenstående diskusjoner har vi lagt vår forståelse av pol § 6 første ledd til grunn. Vi tror likevel det primært er resonnementer og begrunnelser, og ikke konklusjoner, som avviker fra en diskusjon basert på Lovavdelingens uttalelse.

### 12.4.3 Betydningen av personopplysningsloven for tilfanget av saksdokument som det er allmenn innsynsrett i

Personopplysningsloven kan tenkes å virke inn på adgangen til å samle inn/registrere og beholde personopplysninger. I den grad loven begrenser informasjonsinnsamling eller adgang til å lagre personopplysninger, begrenser den også det materialet som det kan kreves innsyn i.

Personopplysningsloven stiller opp visse *grunnkrav* som må tilfredsstilles for at det skal være lovlig for den behandlingsansvarlige (f.eks. forvaltningsorganer og andre rettssubjekter som kommer inn under ny offentlighetslov) å behandle personopplysninger. Dette gjelder krav til rettslig grunnlag (§§ 8 og 9), krav til angivelse av saklig begrunnede formål for behandlingen av personopplysninger (§ 11 bokstav b – c), krav til informasjonskvalitet (§ 11 bokstav d – e), krav til sikring av personopplysninger (§ 13) og krav til gjennomføring av internkontroll (§ 14). Dersom forvaltningen ikke etterlever slike krav, er behandlingen i utgangspunktet ulovlig. Et spørsmål er i så fall om innsyn etter offentlighetsloven kan omfatte personopplysninger som blir ulovlig behandlet av vedkommende. Spørsmålet kommer på spissen dersom opplysningene mangler rettslig grunnlag, jf. § 8, for eksempel dersom det gjennom nettstedet i en offentlig virksomhet samles inn personopplysninger som det ikke foreligger lovhjemmel eller "nødvendig grunn" for, og der det derfor skulle ha vært innhentet samtykke. Dersom dette ikke er gjort, er videre behandling av opplysningene ulovlig, og de skal slettes i henhold til pol § 27 første ledd som bl.a. gjelder det tilfellet at det "ikke er adgang til å behandle" personopplysningene. Unntaksbestemmelsene i § 27 som gir adgang til likevel å beholde opplysningene, gjelder tilfeller der opplysningene er uriktige eller ufullstendige, og sletteplikten fremstår derfor som absolutt. Vi går ikke nærmere inn på en diskusjon om det kan være grunnlag for likevel å beholde opplysningene, men nøyer oss med å konkludere med at dette i beste fall er tvilsomt. Foreligger det slik sletteplikt, vil det

[283] Se Ot.prp. nr. 92 (1998–99) s. 106.

[284] Jf. vårt forslag til (ny) § 8 der plikten til å undersøke om det foreligger taushetsplikt er gjort eksplisitt.

innebære at det ikke kan gis innsyn i de personopplysninger som for eksempel er resultatet av den offentlige virksomhetens brudd på pol § 8.

Også sletteplikten i pol § 28 første ledd er viktig i forhold til eksistensen av saksdokumenter i offentlig virksomhet. Utgangspunktet her er at personopplysninger ikke kan oppbevares lenger enn det som er "nødvendig for å gjennomføre formålet med behandlingen". Opplysninger i personregistre og persondatabaser mv. skal med andre ord slettes fortløpende etter hvert som den behandlingsansvarlige (f.eks. en offentlige virksomhet) har anvendt opplysningene i tråd med innsamlingsformålet, med mindre formålet begrunner fornyet/fortsatt behandling senere. For saksdokumenter der personopplysningene inngår i en sakprosatekst, bilde mv., innebærer bestemmelsen at hver personopplysning skal slettes, mens dokumentet for øvrig kan beholdes. Unntaket er hvis dokumentet gir et åpenbart misvisende bilde etter slettingen. I så fall skal hele dokumentet slettes, se § 28 siste ledd.

Sletting skal likevel ikke skje dersom opplysningene skal oppbevares etter arkivloven eller annen lovgivning som pålegger videre lagring. Dette siste gjelder for eksempel forskrift i medhold av helsepersonelloven.[285]

Arkiveringsplikten etter arkivloven[286] gjelder for "offentlege organ" (arkl § 5, jf. § 2 bokstav g), og dekker neppe alle slike virksomheter som kommer inn under offentlighetsloven, se dennes § 2 første ledd bokstavene a – d. I proposisjonen til arkivloven sies det bl.a. at arkiv i statsforetak skal regnes som private (ikke offentlige) arkiv. Det er derfor tvilsomt om alle slike rettssubjekter som kommer inn under offl § 2 bokstavene c og d kommer inn under arkivloven.

I offl § 10 er det etablert plikt til å føre journal for "organ" som er omfattet av loven, jf. § 4 siste ledd. For slike organ som også er regnet som "offentlege organ" etter arkl § 2 bokstav g, gjelder det et bevaringspåbud for journaler og andre registre, se arkivforskriften § 3-20 bokstavene e og f. Så langt arkivloven gjelder, er pol § 28 første ledd derfor ikke til hinder for at slikt materiale beholdes intakt. For offentlige virksomheter som ikke er "offentlege organ" etter arkivloven, gjelder imidlertid intet bevaringspåbud etter arkivforskriften, og personopplysninger i journaler mv. skal derfor i utgangspunktet slettes når formålet med behandlingen ikke lenger tilsier lagring.

Før vi ser nærmere på unntaksalternativene i pol § 28, vil vi gå nærmere inn på kriteriet i § 28 første ledd, og spørsmålet om hva som menes med at fortsatt lagring er "nødvendig for å gjennomføre formålet med behandlingen [av personopplysninger]".[287] Særlig er det viktig å bringe klarhet i hva som menes med "formål" i denne sammenhengen, og om praktisering av innsynsrett etter offentlighetsloven kan ses som et eget formål som begrunner fortsatt lagring.

I merknadene til pol § 28 diskuterer departementet tilfeller der det er behov for å utføre kontroll av en behandling av personopplysninger som i utgangspunktet er ferdigbehandlet. Departementet går i slike tilfeller ut i fra at opplysningene kan beholdes selv om "hovedformålet" er oppfylt.[288] Det synes imidlertid som om Personvernnemnda har lagt seg

[285] Lov 2. juli 1999 nr. 64, jf. journalforskriften (forskrift 21. desember 2000 nr. 1385) § 14 som bestemmer at legejournal ikke skal avleveres til arkiv eller deponeres før 10 år etter siste innførsel i journalen.

[286] Lov 4. desember 1992 nr. 126.

[287] Jf. også pol § 11 første ledd bokstav e.

[288] I Wiik Johansen m.fl. 2001 sies kun det samme som i departementets merknader.

på en forholdsvis streng praksis i spørsmålet om sletting etter § 28.[289] Vi går ikke her nærmere inn på hvorledes grensene er trukket eller bør trekkes i fremtiden. Likevel minner vi om at det særlig i forhold til offentlig myndighetsutøvelse er et poeng at beslutningspraksis, herunder beslutningsgrunnlag, bør kunne være tilgjengelig etter at vedtak er truffet og beslutningsformålet nådd. Særlig trekker hensynet til tilstrekkelig legalitetskontroll av fattede vedtak og forsvarlig saksutredning av fremtidige enkeltsaker i retning av at personopplysninger må kunne lagres etter at personopplysningene har vært anvendt for det primære innsamlingsformålet.

En mulighet er å se realisering av offentlighetsloven som et "fast formål" for all behandling av åpne personopplysninger[290] i offentlig virksomhet. I så fall blir dette et "evigvarende" formål, som motvirker at personopplysninger som det er innsynsrett i blir slettet. Vi antar imidlertid at dette ikke er en mulig løsning. For det første har den klart preg av å være en konstruksjon for å ivareta hensynet til offentlig innsyn. For det andre fører det til at personverndirektivet artikkel 6 ikke blir gjennomført i forhold til offentlig virksomhet.[291]

Personopplysningsloven § 28 annet ledd åpner for at personopplysninger kan lagres ut over den tid formålet med innsamlingen tilsier når fortsatt lagring skjer for historiske, statistiske eller vitenskapelige formål og hensynet til slike formål *klart* overstiger hensynet til personvern. Vilkåret er videre at opplysningene anonymiseres dersom fortsatt identifisering ikke er nødvendig. Loven må forstås slik at anonymisering skal skje dersom identiteter ikke er nødvendig for å bruke opplysningene til de historiske, statistiske eller vitenskapelige formålene som er anført som grunnlag for at opplysningene ikke skal slettes.[292]

Tredje ledd i pol § 28 åpner for å slette eller sperre personopplysninger selv om det i utgangspunktet er bestemt at opplysningene skal beholdes for historiske, statistiske eller vitenskapelige formål, jf. annet ledd. Vilkåret er at opplysningene er "sterkt belastende" for den personen opplysningene gjelder. Personvernnemnda har tolket bestemmelsen slik at sletting/sperring også kan skje selv om opplysningene er anonymiserte.[293] "Sterkt belastende" er et strengt vilkår. I tillegg må det ikke foreligge noe lovhjemlet plikt til å beholde opplysningene (jf. omtalen av særlovgivning ovenfor), og sletting/sperring må være "forsvarlig ut fra en samlet vurdering av bl.a. andres behov for dokumentasjon, hensynet til den registrerte, kulturhistoriske hensyn og de ressurser gjennomføringen av kravet forutsetter". Dette slettings-/sperringsalternativet kan derfor kun få en meget begrenset anvendelse.

Selv om den formelle adgangen til å slette/sperre personopplysninger er begrenset, er det viktig å være klar over at praksis lett kan tenkes å avvike fra lovens krav. Det er behandlingsansvarlig, dvs. den offentlige virksomheten som har de aktuelle person-opplysningene, som avgjør om det skal skje anonymisering. Beslutningen skal treffes på grunnlag av meget sammensatte og skjønnsmessige bestemmelser i personopplysningsloven, på et område der det rettskildemessige grunnlaget (foreløpig) er forholdsvis tynt. Sletting og

---

289 Se særlig sakene 2003 nr. 2, 2004 nr. 5 og 2005 nr. 6. Personvernnemnda synes å legge en strengere forståelse til grunn enn i departementets merknader. I f.eks. sak 2005 nr. 6 ble det bestemt at opplysninger i en vandelsattest som var innhentet i anledning ansettelse, måtte slettes etter at ansettelse hadde skjedd, fordi opplysningene i attesten senere ville være utdatert og ikke nødvendigvis gi et riktig bilde.

290 Dvs. ikke taushetsbelagte personopplysninger.

291 Jf. ordlyden: "1. […] personal data must be:
(c) […] not excessive in relation to the purposes for which they are collected and/or further processed".

292 Slik forstår vi også Wiik Johansen m.fl. 2001 s. 208.

293 Se sak 2003 sak nr. 2.

anonymisering skal per definisjon være irreversibelt, og slik beslutning skal derfor være endelig. Dersom anonymisering skjer, foreligger det ikke lenger personopplysninger og opplysningene vil ikke lenger komme inn under personopplysningsloven.

Femte og siste ledd i pol § 28 fastsetter at hele dokumentet skal slettes dersom de gjenværende opplysningene etter sletting av personopplysninger gir et åpenbart misvisende bilde. Dette alternativet har primært effekt i tilfelle der personopplysningene har inngått i dokumenter med saksprosa og annet lite formalisert innhold, og der de slettete opplysningene har vært bærende innholdselementer.

### 12.4.4 Betydningen av personopplysningsloven for allment innsyn i personopplysninger

#### 12.4.4.1 Innledning og spørsmålet om formålsbegrensning

Personopplysningsloven inneholder ingen andre bestemmelser om taushetsplikt enn den i § 44, vedrørende Datatilsynets og Personvernnemdas egen taushetsplikt. Loven inneholder med andre ord ingen direkte begrensninger i allmennhetens innsynsrett i personopplysninger, og det er således offl § 13 første ledd i kombinasjon med ulike bestemmelser om lovbestemt taushetsplikt, som ivaretar de viktigste begrensninger i innsynsretten ut i fra hensynet til personvern. Personopplysningsloven kan imidlertid tenkes å innebære et *indirekte konfidensialitetsvern* som vi kommer nærmere inn på i det følgende.

For det første krever personopplysningsloven at enhver behandling av personopplysninger ”bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet”, se § 11 første ledd bokstav b. I ordrett betydning vil dette innebære at innsyn i personopplysninger med hjemmel i offentlighetsloven § 3, lovlig bare vil kunne skje dersom behandlingsansvarlig har formulert innsyn som et formål for behandlingen. Paragraf 11 må imidlertid tolkes i lys av pol § 6 første ledd der det heter at ”Loven her begrenser ikke innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger”. Det er etter vår mening lite tvilsomt at formålsbestemthetsprinsippet i personopplysningsretten ikke innebærer begrensninger av lovbestemte innsynsrettigheter, og vi går derfor ikke nærmere inn på spørsmålet, jf. diskusjonen i avsnitt 12.4.2. Det er imidlertid uheldig at allmennhetens rett til innsyn ikke er tydeliggjort i personopplysningslovens bestemmelser om formålsbegrensninger. Spørsmålet har for øvrig bredere betydning enn i forhold til offentlighetsloven. Generelt må personopplysninger kunne knyttes til *ethvert* formål som er fastsatt i eller klart følger av eller i medhold av lov. Det bør derfor vurderes om dette bør presiseres i § 11, for eksempel:

> **§ 11. Grunnkrav til behandling av personopplysninger**
>
> Den behandlingsansvarlige skal sørge for at personopplysningene som behandles
>
> […]
>
> b) bare nyttes til uttrykkelig angitte *eller lovbestemte* formål som er saklig begrunnet i den behandlingsansvarliges virksomhet" (Vår tilføyelse er satt i kursiv)

Offentlighetsloven § 11 inneholder en regel om merinnsyn:

> Når det er høve til å gjere unntak frå innsyn, skal organet likevel vurdere å gi heilt eller delvis innsyn. Organet bør gi innsyn dersom omsynet til offentleg innsyn veg tyngre enn behovet for unntak.

Bestemmelsen gir anvisning på en bred avveining mellom hensynet til offentlig innsyn på den ene side, og behovet for unntak på den andre.[294] I behovet for unntak, inngår hensynet til personvern. Dette betyr at personvern kan tale mot merinnsyn. Samtidig skal en imidlertid være klar over at personvernhensyn også kan tale *for merinnsyn*. Dette er for eksempel tilfellet dersom innsyn begrenses til personopplysninger i en sak, og dette gir ufullstendig informasjon, jf. diskusjonen straks nedenfor av pol § 11 bokstavene d og e.

I tillegg til fastsettelse av og avgrensing til bestemte formål, må behandlingen av personopplysninger ha rettslige grunnlag. Dette rettslige grunnlaget må dekke alle aktuelle behandlingsformål, herunder formålet å gi innsyn til allmennheten, se pol § 8.[295] I tilfellet offentlig innsyn vil offl § 3 være tilstrekkelig lovhjemmel, se § 8 første ledd, første setning. Også i forhold til merinnsyn foreligger det lovhjemmel, se offl § 11. Kravet i personopplysningsloven om rettslig grunnlag kan med andre ord ikke begrense innsynsretten etter offentlighetsloven.[296]

#### 12.4.4.2 Krav til opplysningskvalitet

Personopplysningsloven stiller også krav til opplysningskvalitet mv, se pol § 11 første ledd bokstavene d og e. Personopplysningene skal for det første være tilstrekkelige og relevante *i forhold til formålet*. Når formålet er å oppfylle lovbestemte krav om innsyn i saksdokumenter, herunder i personopplysninger, kan disse kravene neppe virke i innskrenkende retning. Kravet om relevans må ses i sammenheng med kravet til spesifisering/avgrensing av innsynskrav etter offentlighetsloven, se offl § 28 annet ledd. Innsynet kan gjelde en bestemt sak, eller i rimelig utstrekning saker av bestemt art, eller journal eller lignende register. Uansett må de personopplysninger som følger av saken/samlingen av saker/journal mv. regnes som relevante, og det er neppe grunnlag for å gjøre noen begrensninger som spesielt gjelder tilgangen til personopplysninger (annet enn det som følger av regler om taushetsplikt og taushetsrett, jf. offl §§ 13 og 11). Kravet om tilstrekkelighet innebærer at det må gis så mye opplysninger at formålet med å kreve innsyn kan tilfredsstilles, noe som trekker i retning av at alle relevante opplysninger skal være omfattet av innsynet. Dette kan i konkrete tilfelle gi innsyn i *flere* personopplysninger enn det som direkte følger av innsynskravet. Dersom innsynskravet gjelder en bestemt sak som inneholder ufullstendige personopplysninger, tilsier kravet om tilstrekkelighet i pol § 11 første ledd bokstav d at opplysningene som ligger til saken suppleres av slike andre relevante personopplysninger som skal til for å gi et tilstrekkelig opplysningsgrunnlag.

For det andre skal personopplysningene være korrekte og oppdaterte. Når det gjelder krav til korrekthet, må opplysningene slik de foreligger, være tilstrekkelig korrekte i forhold til innsynsformålet – selv om opplysningene objektivt sett er uriktige. Hensynet til tilstrekkelig-

---

[294] Vi forstår bestemmelsen slik at det ikke er vesentlig betydningsforskjell på "omsyn" og "behov" i lovteksten, og at det er tale om å veie to grupper av hensyn/behov mot hverandre.

[295] Personopplysningsloven § 9 er ikke aktuell i forhold til innsyn fordi det alltid er taushetsplikt for sensitive personopplysninger.

[296] Men personvern er et relevant hensyn når meroffentlighet skal bedømmes.

het (jf. ovenfor), kan imidlertid i slike tilfelle tenkes å begrunne at andre, korrekte personopplysninger blir omfattet av innsynet. Kravet til oppdaterte personopplysninger, kan på samme måte begrunne at det gis supplerende og mer oppdaterte opplysninger enn det som ligger til en bestemt sak det er bedt om innsyn i. For øvrig tilsier både personopplysningslovens krav om ajourhold og realiseringen av innsynsretten, jf. offl § 1, at det gis tilgang til alle saksdokumenter og personopplysninger som det er innsynsrett i per dato for innsynskravet.[297]

#### 12.4.4.3 Sammenstilling av personopplysninger

Offentlighetsloven § 9 inneholder en rett til, "med enkle framgangsmåtar", å kreve innsyn i en *sammenstilling* av personopplysninger som er lagret i organets databaser. Sammenstillingen kan både tenkes innen én og samme database, og mellom ulike databaser. Sammenstilling innebærer det en tidligere benevnte "kopling" av personregistre. I den nå opphevde personregisterloven § 11 annet ledd nr. 3 var det fastsatt at adgangen til å kople opplysninger skulle reguleres i konsesjonen. Et meget stort antall registre var underlagt konsesjonsplikt.

Personopplysningsloven har ingen særskilte regler vedrørende kopling/sammenstilling av personopplysninger. Slik behandling må imidlertid følge lovens alminnelige krav, bl.a. i forhold til opplysningskvalitet, se pol § 11 første ledd bokstavene d og e. I tillegg er det i pol § 21 regulert særlige tilfeller der resultatet av sammenstilling av opplysninger resulterer i "personprofiler". Bestemmelsen legger ingen begrensninger på hvilke profiler som kan lagres, men stiller krav til å informere de personer som mottar henvendelser eller blir gjenstand for beslutninger på grunnlag av slike profiler. Dette får derfor først betydning dersom den innsynsberettigede bruker de personprofiler som sammenstilling av databasene gir til å henvende seg/beslutte slik pol § 21 beskriver.

#### 12.4.4.4 Utlevering av personopplysninger

Offentlighetsloven § 30 har bestemmelser om gjennomføring av innsyn. Sett fra personopplysningsloven innebærer gjennomføring av innsyn som omfatter personopplysninger, at den offentlige virksomheten *utleverer* og den innsynsberettigede *mottar* personopplysninger. Både for utlevering og mottak/innsamling av personopplysninger gjelder det bestemmelser i personopplysningsloven som det i utgangspunktet må tas hensyn til ved gjennomføringen av innsyn etter offentlighetsloven.

Når en innsynsberettiget person mottar personopplysninger, er det første spørsmålet om dette skjer på en slik måte at vedkommende selv blir behandlingsansvarlige og derfor må behandle opplysningene i samsvar med personopplysningslovens bestemmelser. For at personopplysningsloven skal komme til anvendelse på den innsynsberettigede, må forholdet komme inn under lovens saklige og geografiske virkeområde, jf. pol §§ 3 og 4. Dette innebærer for eksempel at utlevering av dokumenter som ikke er elektroniske og som ikke inneholder personregister, faller utenfor loven. For øvrig er utgangspunktet at loven kan komme til anvendelse. Forutsetningen er imidlertid at den innsynsberettigede ikke helt eller delvis er unntatt fra lovens bestemmelser: Skjer innsynet for rent personlige eller private formål, oppstår ikke behandlingsansvar etter loven. Skjer innsynet for journalistiske mv. formål, vil

[297] Personopplysningsloven § 11 første ledd bokstav e regulerer også varigheten av lagringen av personopplysninger, jf. pol §§ 27 og 28. Dette er nært knyttet til sletting, som vi anser er tilstrekkelig dekket av det som er skrevet ovenfor i dette avsnittet.

bare mindre deler av loven gjelde for den innsynsberettigede som mottar opplysningene, jf. pol § 7. I andre saker kan lovens bestemmelser komme til anvendelse på den innsynsberettigedes videre behandling av personopplysninger. Forutsetningen er imidlertid at opplysningene enten inngår i en *eksisterende* behandling av personopplysninger (for eksempel når innhentede opplysninger legges ut på den innsynsberettigedes nettside), eller at det etableres en *ny* behandling av personopplysninger i sakens anledning (en interesseorganisasjon starter for eksempel kartlegging av hvilke personer som har deltatt ved behandlingen av visse kommunale saker). Dersom personopplysningsloven kommer til anvendelse på den innsynsberettigede i rollen som behandlingsansvarlig, innebærer dette at den innsynsberettigedes må etterleve en rekke krav til den videre behandling av de innhentede opplysningene.

Offentlige virksomheter som utleverer personopplysninger som ledd i etterlevelsen av offl § 3, må etterleve personopplysningsforskriftens (pof) krav til sikring av personopplysninger (i pof kap. 2). Utgangspunktet er da at "[d]en behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her", se pof § 2-15. Kravet gjelder kun *elektronisk* overføring. Unntak er gjort i annet ledd for overføring av personopplysninger til utlandet i samsvar med pol §§ 29 og 30, samt når det er "fastsatt i lov at det er adgang til å kreve opplysninger *fra et offentlig register*" (vår kursiv). Siste unntaksalternativ innebærer at det kan utleveres opplysninger fra folkeregisteret, ektepaktregisteret, kjøretøyregisteret mv. uten at registermyndigheten forsikrer seg om at mottakeren behandler de mottatte personopplysningene i samsvar med kravene i personopplysningsloven. Lignende unntak er imidlertid ikke gjort for utlevering av opplysninger i samband med allmenninnsyn etter offl § 3 eller partsinnsyn etter offentlighetsloven § 18. Spørsmålet er ikke nærmere diskutert i kommentarene til forskriftsbestemmelsen som var del av kgl. res. 15. desember 2000 nr. 1265 der forskriften ble vedtatt.

Med forskriftens spesifikke angivelse av et unntak knyttet til offentlig register, kan det neppe konkluderes med at unntaket også gjelder etter offentlighetsloven. Konklusjonen er derfor at den offentlige virksomheten – i utgangspunktet – plikter å forvisse seg om at den personopplysningene blir utlevert til selv vil etterleve personopplysningsforskriften. Forskriften sier intet om hvorledes dette skal skje, men i kommentarene til pof § 2-15 forutsettes det at den behandlingsansvarlige som skal gi fra seg opplysninger skal få kunnskap om innholdet i sikkerhetsdokumentasjon mv. Dette er igjen knyttet til bestemte sikkerhetsgjennomganger mv. som forskrifter pålegger behandlingsansvarlige å gjennomføre. Plikten etter pof § 2-15 kan imidlertid ikke gjelde i forhold til innsynsberettigede som ikke kommer inn under loven, jf. pol § 3 annet ledd om "rent personlige eller andre private formål". Bestemmelsen er imidlertid virksom i andre tilfeller, for eksempel i forhold til pressen.[298]

Plikten etter pof § 2-15 innebærer en plikt til å nekte overføring av personopplysninger *i elektronisk form* til innsynsberettigede som ikke tilfredsstiller kravene i pof kapittel 2 om informasjonssikkerhet. Teoretisk sett kan dette innebære at innsynsretten må gjennomføres på måter som ikke innebærer utlevering av elektronisk materiale.

Kravene vedrørende overføring av personopplysninger til (f.eks.) en innsynsberettiget er med andre ord strenge og tungvinte i de tilfelle overføringen skjer elektronisk. Dersom opplysningene utleveres på papir eller lignende, oppstår ingen tilsvarende krav. Det er grunn til å tro at innsyn i stadig større omfang vil bli gjennomført i elektronisk form. I

[298] Se pol § 7 som bl.a. fastsetter at lovens bestemmelser om informasjonssikkerhet (§ 13) skal gjelde for journalistisk virksomhet.

eforvaltningsforskriften (efvf)[299] er det i § 10 dessuten lagt til rette for at dette kan skje. Bestemmelsen slår for det første fast at det kan gis tilgang til opplysninger og dokumenter i elektronisk form dersom forvaltningsorganet fører elektronisk arkiv og den innsynsberettigede samtykker eller går med på det. Paragraf 10 viser ikke til personopplysningsloven eller –forskriften, men i efvf § 13 tredje ledd bokstav g vedrørende sikkerhetsmål og sikkerhetsstrategi, er det gjort henvisning til pol § 13 og pof kapittel 2 (om informasjonssikkerhet). Dette må forstås slik at forvaltningsorganer har plikt til å fastlegge mål og strategier for å sikre gjennomføringen av bl.a. pof § 2-15, herunder i samband med praktisering av "elektronisk innsyn", jf. efvf § 10.

Som tidligere nevnt har offentlighetsloven et videre saklig virkeområde enn arkivloven fordi "organ" i offl § 4 siste ledd, jf. § 2 første ledd bokstavene c og d, favner videre enn "offentleg forvaltningsorgan". Det samme gjelder forholdet mellom "organ" etter offentlighetsloven og "forvaltningsorgan" i betydningen "et hvert organ for stat eller kommune" etter forvaltningsloven. Samspillet mellom eforvaltningsforskriften og personopplysnings-forskriften som vi nylig har redegjort for, er derfor ikke til stede for alle "organ" som kommer inn under offentlighetsloven.

### 12.4.5 Betydningen av personopplysningsloven for allment innsyn i annet enn personopplysninger

Personopplysningsloven inneholder innsynsrettigheter som supplerer offentlighetslovens regler om innsyn for enhver, se pol § 18 første ledd. Denne bestemmelsen gir enhver rett til å få opplysning om slike informasjonssystemer og -rutiner som behandler personopplysninger. Loven angir som utgangspunkt en gitt mengde opplysninger:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,
c) formålet med behandlingen,
d) beskrivelser av hvilke typer personopplysninger som behandles,
e) hvor opplysningene er hentet fra, og
f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Anvendt på offentlige virksomheter, innebærer dette i virkeligheten en rett til å få beskrevet viktige deler av beslutningssystemer og informasjonsutveksling der offentlige organer mv. deltar. Siden det ikke eksisterer noen plikt eller fast foranledning til å produsere saksdokumenter som inneholder slike opplysninger, vil dette ofte være kunnskaper det ikke er mulig å erverve ved å kreve innsyn etter offentlighetsloven. Slik sett er bestemmelsen et viktig supplement til offl § 3.

Personopplysningslovens § 18 første ledd gjelder uavhengig av sektor, noe som innebærer at bestemmelsen ofte også vil gjelde kilder for og mottakere av personopplysninger som en offentlig virksomhet behandler. Denne innsynsretten kan således også benyttes for å få innsyn hos aktører som offentlige virksomheter samhandler med. Også slik innebærer pol § 18 første ledd et viktig supplement til offl § 3.[300]

[299] Forskrift 25. juni 2004 nr. 988.

[300] I tillegg til innsynsretten for enhver etter pol § 18 første ledd, har personopplysningsloven individuelle innsynsrettigheter etter § 18 annet og tredje ledd.

I § 23 gjør personopplysningsloven felles unntak fra bestemmelser om innsyn og informasjon, med i alt 6 unntakskategorier som er sterkt inspirert av forvaltningsloven og offentlighetsloven av 1970. Offentlighetsloven (av 2006) har i alt 13 unntakskategorier, hvorav noen ligner enkeltkategorier i pol § 23, mens andre unntak gjelder spesifikke typer saksdokumenter som ikke er nevnt i personopplysningsloven. Fordi innsyn for enhver etter personopplysningsloven kun gjelder beskrivelse av informasjonssystemer og -rutiner, og fordi denne loven bare gjelder elektronisk behandling og personregistre, vil det trolig ikke være mulig å få tilgang til opplysninger som er unntatt fra innsyn etter offentlighetsloven ved å kreve innsyn etter personopplysningsloven. Vi har imidlertid ikke tatt oss tid til å gjennomføre en systematisk, sammenlignende analyse av dette spørsmålet.

Personopplysningsloven gir både innsyn for enhver (§ 18 første ledd) og innsyn for den registrerte (§ 18 annet og tredje ledd). Dette innebærer at begge innsynsrettigheter utfyller andre, brede innsynsbestemmelser; særlig de i fvl § 18 og offl § 3. Dette er noe av bakgrunnen for at det i pol § 6 annet ledd er satt inn en bestemmelse om plikt for behandlingsansvarlige til å veilede om annen lovbestemt innsynsrett: "Dersom annen lovbestemt rett til innsyn gir tilgang til flere opplysninger enn loven her, skal den behandlingsansvarlige av eget tiltak veilede om retten til å be om slikt innsyn". Personer som retter spørsmål til en offentlig virksomhet som kommer inn under offentlighetslovens bestemmelser, vil alltid også ha rett til innsyn etter pol § 18 første ledd. På denne bakgrunn ville det både være logisk og rimelig dersom det i offentlighetsloven og forvaltningsloven ble tatt inn en plikt til å veilede om annen lovbestemt innsynsrett, eventuelt avgrenset til annen innsynsrett for enhver, som den i pol § 18 første ledd.

### 12.4.6 Kort om ivaretakelse av personvern og forekomster av personvernrelaterte begreper i offentlighetsloven

På lignende måte som personopplysningsloven fremmer offentlighet, inneholder bestemmelser i offentlighetsloven bestemmelser som ivaretar personvern. Dette gjelder primært offl § 13 som fastsetter at det ikke er innsyn i dokumenter som er omfattet av lovbestemt taushetsplikt. Unntak på grunn av taushetsplikt skal også foretas av selvstendige rettssubjekter som kommer inn under offentlighetsloven[301] i samme omfang som fvl § 13 fastsetter.

For ivaretakelsen av personvern er taushetsplikt for opplysninger om "noens personlige forhold" det avgjørende. "Noens personlige forhold" er en egen kategori opplysninger som ikke uten videre passer inn i, eller har et avklaret forhold til den nært beslektete terminologien i personopplysningsloven. Begrepet ligger antagelig innenfor begrepet "personopplysning" i den forstand at det kun er tale om opplysninger om fysiske personer. Ved avgrensingen av "noens personlige forhold" er det vanlig å gå kasuistisk til verks for å undersøke hvor grensen går i forhold til "åpne" opplysninger om personer.[302] Dersom vi imidlertid legger definisjonen av "personopplysning" til grunn, genererer dette en rekke spørsmål vedrørende "noens personlige forhold" som det ikke uten videre er lett å ta stilling til på grunnlag av lovteksten:

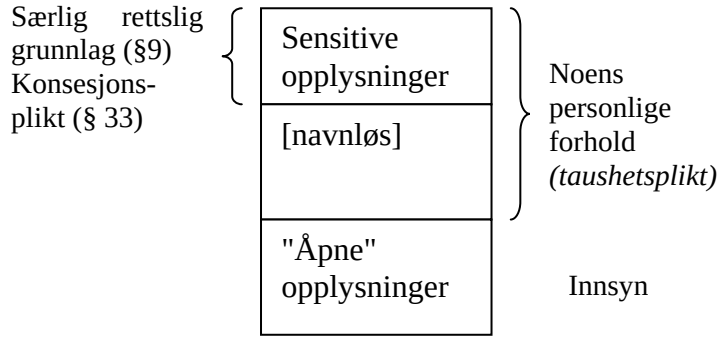
- Gjelder taushetsplikten både for levende og døde personer?

[301] Jf. § 2 første ledd bokstavene c og d. Slike rettssubjekter kommer i utgangspunktet ikke inn under forvaltningsloven, og hjemmel til å unnta på grunn av taushetsplikt er derfor satt inn i offl § 13 andre ledd.

[302] Se f.eks. Lovavdelingens uttalelse vedrørende forståelsen av fvl § 13 og § 13a (Saksnummer: 1998/10047 E AS/ØØ), datert 19. november 1998.

- Må opplysningen faktisk være koplet til en person, eller er det nok at opplysningen er potensiell?
- Hvor indirekte og sammensatt kan koplingen mellom opplysningen og personen være?
- Hvor sikker må tilknytningen mellom opplysningen og personen være?
- Hvor sikker/klar må personens identitet være?

Poenget her er for det første at det er usikkert om "noens personlige forhold" er betegnelsen på en "personopplysning", slik dette begrepet er definert i pol § 2 nr. 1. Vurdert opp i mot kulepunktene ovenfor, taler mye for at "noens personlige forhold" bygger på et smalere begrep enn "personopplysning". I tillegg kommer at noens personlige forhold er betegnelsen på en kvalifisert gruppe opplysninger om personer, dvs. det foretas implisitt en todeling der noen opplysninger ikke hører til personlige forhold (og er åpne for innsyn), mens andre gjør det (og er underlagt taushetsplikt). På en måte er "noens personlige forhold" en kvalifisering av noen opplysninger som følsomme. Likevel tilsvarer ikke "noens personlige forhold" "*sensitiv* personopplysning" i pol § 2 nr. 8. Sensitive personopplysninger hører trolig alltid til "noens personlige forhold", mens "noens personlige forhold" slett ikke alltid er sensitive i personopplysningslovens forstand. Vi har med andre ord med tre sensitivitetsgrader å gjøre, der vi kun har navn på den høyeste graden og et felles navn på de to høyeste gradene. Den midterste og den nederste graden er navnløse. Vi velger å kalle den nederste for "åpne" opplysninger, fordi det er i forhold til slike at det kan gis innsyn etter offl § 3.




Vårt poeng i denne sammenheng er at offentlighetsloven bruker fvl § 13 som mellomstasjon for å angi de personopplysninger som det er taushetsplikt for. Forvaltningsloven § 13 bygger imidlertid på en begrepsbruk som passer dårlig inn i forhold til definisjonen av "personopplysning" i pol § 2 nr. 1. Samtidig gjør offl § 10 tredje ledd en direkte henvisning til pol § 2 nr. 1 (i en forskriftshjemmel). Også i § 26 tredje ledd gjøres det en henvisning som det er nærliggende å tolke som en referanse til personopplysningsloven. Det heter her at unntak fra innsynsrett kan gjøres for "personbilete som er teke inn i eit personregister". Det er nærliggende å tolke "personbilete" som et begrep som bygger på "personopplysning" i pol § 2 nr. 1, særlig fordi det figurerer sammen med "personregister" som er definert i § 2 nr. 3.

Analysen ovenfor viser at offentlighetsloven forholder seg til personopplysningsbegrepet på tre forskjellige måter:

- Til forvaltningslovens § 13 første ledd, noe som gir et uavklart forhold til pol § 2 nr. 1;
- Til personopplysningslovens definisjoner, men uten klar henvisningsstruktur;
- Til pol § 2 nr. 1 med direkte og klar henvisning.

Etter vår mening er dette en klar indikasjon på at forholdet mellom offentlighetsloven og personopplysningsloven bør være gjenstand for systematiske vurderinger, bl.a. av lovteknisk karakter. Etter vår mening er det behov for å rydde opp i begrepsbruken for å oppnå sammenheng mellom sentrale begreper i personopplysningsloven, offentlighetsloven og forvaltningsloven. Særlig bør dette gjelde betegnelser på opplysninger som gjelder personer.

En slik samordning må også innbefatte fvl § 13 og "noens personlige forhold". Fordi vi anser det å ligge utenfor mandatet å vurdere bestemmelser i forvaltningsloven, har vi imidlertid valgt å ikke gå nærmere inn på mulige løsninger.

### 12.4.7 Allmenne vurderinger og forslag

Det er etter vår mening behov for en nærmere avklaring av forholdet mellom personopplysningsloven og offentlighetsloven. Vi antar det er behov for å gjøre endringer i begge lover:

- Det bør gjøres endringer i personopplysningsloven som tydeliggjør at allmennhetens lovbestemte innsyn i "åpne" personopplysninger ikke er i konflikt med denne lovens bestemmelser. Vi har i den sammenheng foreslått en beskjeden endring i pol § 11 første ledd bokstav b (jf. lovforslagene).
- En bør vurdere tatt inn i begge lover en "regibestemmelse", dvs. en bestemmelse som minner om eksistensen av den andre loven, og nærmere angir betydningen av denne.
- Det bør innføres eksplisitte henvisninger mellom offentlighetsloven og personopplysningsloven som tydeliggjør de viktigste sammenhengene mellom de to lovene.
- Det bør gjøres endringer i fvl § 13 første ledd for å sikre sammenheng med personopplysningsbegrepet.
- Vi mener også det er behov for å introdusere en plikt i offentlighetsloven (f.eks. i § 28) til å veilede om annen lovbestemt innsynsrett, i alle fall om annen allmenn innsynsrett, jf. pol § 18 første ledd.
- Bestemmelsen i pol § 6 vil etter vår mening få en bedre og tydeligere plassering dersom den ble flyttet til pol § 18, eller annet sted i kapittel III. Begrunnelsen er at vi ikke primært oppfatter dagens pol § 6 som lovvalgsregel, men som en regel som spesielt skal konsolidere lovbestemte innsynsrettigheter, og samtidig sikre informasjon som kan legge til rette for bruk av rettighetene.
- Det kan være grunn til å gjøre unntak fra pof § 2-15 første ledd i tilknytning til utlevering av personopplysninger som ledd i realisering av lovbestemt innsynsrett.

## 12.5 Spørsmål vedrørende interne strukturer i personopplysningsloven og -forskriften

### 12.5.1 Innledning

I dette avsnittet ser vi på to typer strukturspørsmål knyttet til personopplysningsloven. For det første tar vi opp spørsmål vedrørende lovens interne struktur. Dette gjelder særlig spørsmål vedrørende rekkefølgen og grupperingen av bestemmelsene. Vi har dessuten valgt å trekke frem innholdet i en bestemmelse som ikke inngår i mandatet, men der vi mener det eksisterer en logisk brist, sett i sammenheng til andre bestemmelser. Som konklusjon på diskusjonene vedrørende den interne strukturen vil vi fremme forslag om endringer i lovteksten. Disse forslagene atskiller seg fra øvrige forslag til lovtekst i denne utredningen, ved at endringene primært gjelder plassering og inndeling i paragrafer.

For det andre tar vi opp strukturspørsmål i forholdet mellom personopplysningsloven og forskriften til loven. Vårt radikale lovforslag, innebærer at store deler av forskriften kan oppheves. Samtidig kan andre forslag begrunne nye forskriftsbestemmelser. Vi har valgt å

ikke diskutere forholdet vedrørende de delene av forskriften som i henhold til våre forslag vør oppheves. I stedet har vi konsentrert oppmerksomheten om de kapitler i forskriften som for øvrig er uberørt av våre forslag ellers i denne utredningen. I de tilfelle vi foreslår å flytte forskriftsbestemmelser opp i loven, vil også diskusjonen av forholdet mellom lov og forskrift resultere i konkrete forslag til endret lovtekst. Vi har imidlertid unnlatt å vise hvorledes den resterende forskriftsteksten bør konsolideres.

### 12.5.2 Strukturspørsmål knyttet spesielt til loven

#### 12.5.2.1 Rekkefølgen for prøving av rettslig grunnlag og formålet for behandlingen

Personopplysningsloven § 11 første ledd bokstav a inneholder en "regibestemmelse" som opplyser noe om sammenhengen mellom sentrale bestemmelser i lovens kapittel II:

> **§ 11. Grunnkrav til behandling av personopplysninger**
>
> Den behandlingsansvarlige skal sørge for at personopplysningene som behandles bare behandles når dette er tillatt etter § 8 og § 9,
>
> […]

Bestemmelsen angir at §§ 8 og 9 skal vurderes. Siden de to neste alternativene i bestemmelsen (b og c) gjelder fastsettelse av formål for behandlingen, er det nærliggende å lese bokstav a) slik at kravene til rettslig grunnlag i §§ 8 og 9 skal vurderes før formålet blir vurdert. Rekkefølgen av bestemmelsene underbygger dette inntrykket.

Vi mener formålet, dvs. hva behandlingsansvarlige skal bruke opplysningene til, må fastsettes *før* det rettslige grunnlaget for behandlingen blir vurdert. Uansett må eventuell lovhjemmel, samtykke eller "nødvendig grunn" vurderes opp mot den planlagte bruken av opplysningene. Bestemmelsene i § 11 første ledd bokstavene b og c om formål må derfor vurderes før §§ 8 og 9. Det er naturlig at rekkefølgen av bestemmelsene gjenspeiler dette forholdet.

I § 8 i vårt radikale lovforslag er det tatt inn en regibestemmelse som gir anvisning på at det rettslige grunnlaget må prøves ut i fra fastsettelsen av formål i § 11. Denne løsningen gir ikke en riktig rekkefølge på bestemmelsene, dvs. vi har ikke foreslått å sette gjeldende § 11 foran forslaget til § 8. Ideelt sett burde også denne rekkefølgen være endret, men vi har under tvil kommet frem til at gevinsten av å flytte bestemmelsen ikke er stor nok i forhold til ulempen ved at den sentrale bestemmelsen i § 11 får en uvant plassering. Det meste er etter vår mening vunnet ved at vårt forslag til § 8 gir klar beskjed om sammenhengene mellom bestemmelsene som regulerer rettslig grunnlag og formål.

#### 12.5.2.2 Det logiske innholdet av § 11 første ledd bokstav c, jf. §§ 8 og 9

Paragraf 11 første ledd bokstav c lyder (i sin sammenheng):

> § 11. Grunnkrav til behandling av personopplysninger
>
> Den behandlingsansvarlige skal sørge for at personopplysningene som behandles
>
> […]

b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,

c) ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker,

[…]

Vi har store problemer med å få god mening ut av alternativet i bokstav c. Problemene oppstår primært når bestemmelsen leses i sammenheng med §§ 8 og 9 om rettslig grunnlag. Så vidt vi kan forstå, foreligger det tre mulige sett av situasjoner:

1. Det første rettslige grunnlaget for å behandle personopplysningene er *lovhjemmel*. Vi har da tre del-situasjoner:

   a) Det kan påberopes en ny lovhjemmel for det nye og uforenlige formålet. Så lenge det foreligger en holdbar hjemmel, kan det ikke kreves samtykke fra den registrerte. Bestemmelsen kan selvsagt ikke forstås slik at den legger begrensninger på hva lovgiver kan vedta.

   b) Det innhentes samtykke for det nye formålet, og dette supplerer den opprinnelige lovhjemmelen. Dette er det selvsagt anledning til, men bestemmelsen i § 11 første ledd bokstav c er ikke nødvendig for å uttrykke dette.

   c) Det påberopes nødvendig grunn for det nye formålet, og dette supplerer den opprinnelige lovhjemmelen. Bestemmelsen i § 11 første ledd bokstav c kan forstås som et forbud mot å påberope seg nødvendig grunn i et slikt tilfelle, ved at det pålegges alltid å innhente samtykke.

2. Det første rettslige grunnlaget for å behandle personopplysningene er *samtykke*. Igjen har vi tre del-situasjoner:

   a) Det opprinnelige samtykket suppleres av et nytt samtykke som dekker det nye og uforenlige formålet. Dette er det selvsagt full anledning til, og bestemmelsen i § 11 er overflødig for å uttrykke dette.

   b) Det opprinnelige samtykket suppleres av en lovhjemmel som dekker det nye og uforenlige formålet. Dette må det selvsagt også være full anledning til, og nytt samtykke kan ikke være påkrevet.

   c) Det opprinnelige samtykket suppleres av en ”nødvendig grunn”. Bestemmelsen i § 11 første ledd bokstav c kan forstås som et forbud mot å påberope seg nødvendig grunn i et slikt tilfelle, ved at det pålegges alltid å innhente samtykke.

3. Det første rettslige grunnlaget for å behandle personopplysningene er *”nødvendig grunn”*. Igjen har vi tre del-situasjoner:

   a) Den opprinnelige nødvendige grunnen suppleres av en lovhjemmel som dekker det nye og uforenelige formålet. Dette er det selvsagt full anledning til.

b) Den opprinnelige nødvendige grunnen suppleres av et samtykke som dekker det nye og uforenelige formålet. Dette er det selvsagt full anledning til, og bestemmelsen i § 11 er overflødig for å uttrykke dette.

c) Den opprinnelige nødvendige grunnen suppleres av en ny "nødvendig grunn" som dekker det nye og uforenlige formålet. Bestemmelsen i § 11 første ledd bokstav c kan forstås som et forbud mot å påberope seg nødvendig grunn i et slikt tilfelle, ved at det pålegges alltid å innhente samtykke.

Det er med andre ord i tilfellene i 1c, 2c og 3c at det etter vårt syn gir logisk mening å kreve samtykke dersom et nytt formål er uforenlige med det opprinnelige formålet. Dette kan uttrykkes slik:

> Dersom formålet for behandling av personopplysninger blir endret slik at det nye formålet blir uforenlig med det opprinnelige, må behandlingsansvarlige enten kunne påberope seg en lovhjemmel eller innhente et nytt samtykke fra den registrerte.

En slik formulering innebærer at "nødvendig grunn" ikke kan påberopes i tilknytning til nytt eller endret formål som er uforenlig med det første formålet. Vi tar ikke her stilling til rimeligheten av en slik bestemmelse. Uansett vil vi påpeke at bestemmelsen i § 11 første ledd bokstav c må forholde seg til det opprinnelige rettslige grunnlaget for behandlingen av personopplysninger.

#### 12.5.2.3 Innsynsbestemmelsene i § 18

Paragraf 18 inneholder bestemmelser om innsyn for enhver og innsyn for registrerte personer. Vi mener det er uheldig at disse bestemmelsene er slått sammen i én paragraf. Lovforslaget i NOU 1997: 19 gjorde et klart skille mellom de to typene av innsynsrettigheter: § 16 (innsyn for enhver) og § 18 (innsyn for registrerte). I tillegg ble det foreslått en egen bestemmelse i § 17 om Datatilsynets offentlige fortegnelser over meldinger og behandlinger.

Vi mener det er viktig å tydeliggjøre de to typene innsynsrettigheter som folk kan ha, og forslår at § 18 splittes i to bestemmelser, som er inntatt som §§ 16 og 17 i vårt radikale lovforslag:

> **§ 16 Rett til innsyn for enhver**
>
> Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:
>
> a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
>
> b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,
>
> c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra, og

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

**§ 17 Rett til innsyn for registrerte personer**

Enhver som ber om det, skal få vite om det er registrert opplysninger om vedkommende hos en behandlingsansvarlig.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) hvilke opplysninger om den registrerte som behandles, og

b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i § 16 bokstav a – f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter denne bestemmelsen gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte.

Første ledd i det foreslåtte § 17 er nytt, og er satt inn for å tydeliggjøre den individuelle innsynsretten. For øvrig er det gjort mindre justeringer for å etablere riktig sammenheng mellom bestemmelsene etter at de er inndelt i to paragrafer. Vi har ikke foreslått materielle endringer, men mener det er grunn til å vurdere om begjæring om innsyn også kan skje hos databehandler. Dette forutsetter imidlertid at gjennomføring av slikt innsyn er omfattet av avtalen mellom behandlingsansvarlig og databehandler, se pol § 15.

#### 12.5.2.4 Reservasjonsretten i pol § 26

Paragraf 26 inneholder en bestemmelse om rett til å reservere seg mot direkte markedsføring. En ytterligere begrensing i markedsføring ved hjelp av telekommunikasjoner er tatt inn i markedsføringsloven § 2b. De to bestemmelsene må åpenbart ses i sammenheng, og bør stå i én og samme lov. Fordi begge bestemmelser gjelder markedsføring, bør bestemmelsene fortrinnsvis plasseres i markedsføringsloven. En slik endring vil også innebære at kapittel 5 i personopplysningsforskriften flyttes og knyttes til denne loven. Vi antar dessuten at det er mest hensiktsmessig at Forbrukerombudet håndhever begge bestemmelser.

#### 12.5.2.5 Krav om sletting og retting mv. i pol § 27

Paragraf 27 gjelder retting, sletting, sperring og supplering av personopplysninger, og tar tak i situasjoner der det må gjøres endringer i enkeltopplysninger i situasjoner der det pågår behandling av personopplysninger som skal fortsette. Til sammenligning handler § 28 om sletting av personopplysninger når formålet ikke lenger tilsier lagring. Begge bestemmelser står i kapittel IV ("Andre rettigheter for den registrerte"). I kapittelet inngår:

- § 25 - Rett til å kreve manuell behandling;
- § 26 - Rett til å reservere seg mot direkte markedsføring;
- § 27 - Retting av mangelfulle personopplysninger;
- § 28 - Forbud mot å lagre unødvendige personopplysninger.

Vi mener dette kapittelet har preg av å være en oppsamlingsplass for bestemmelser som en ikke fant annen plassering for, og tror bestemmelsene med fordel kan plasseres annerledes. Vi mener dessuten at bestemmelser som står under kapitler med titler som angir at innholdet gjelder rettigheter, også bør formuleres som rettighetsbestemmelser.

I forrige avsnitt foreslår vi å flytte pol § 26 til markedsføringsloven, jf. vårt radikale forslag i avsnitt 13.2 (nedenfor). Den videre diskusjonen gjelder derfor de tre øvrige bestemmelsene. Paragraf 25 er klart formulert som en rettighet, og kan åpenbart stå i et rettighetskapittel. Paragraf 27 og 28 er derimot ikke formulert som rettigheter. Likevel er unntaksalternativet i § 28 tredje ledd formulert som en rett for den registrerte til å kreve sletting eller sperring av opplysninger.

Vi mener § 27 bør formuleres som en rettighet for den registrerte og plasseres i tilknytning til innsynsbestemmelsene for registrerte personer, jf. forslaget til § 17 ovenfor. I tillegg bør behandlingsansvarliges ansvar for å rette ufullstendigheter mv. komme til uttrykk i samband med bestemmelsen i § 11 om krav til opplysningskvalitet. Slik vil spørsmålet om retting, sletting mv. både komme til uttrykk som en rettighet for registrerte personer, og som en plikt for behandlingsansvarlig. Bestemmelsene vil da bli plassert i henholdsvis kapittel III og kapittel II.

Vårt (radikale) forslag er videre å sette inn en bestemmelse som tydeliggjør at registrerte har en rett til å kreve ufullstendige opplysninger endret:

> **§ 23 Rett til å kreve opplysninger slettet, rettet, supplert eller sperret**
>
> Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er rettslig grunnlag til å behandle (jf. §§ 8 – 8d), har den registrerte rett til å kreve at den behandlingsansvarlige gjør nødvendige endringer ved å slette, rette, supplere eller sperre opplysningen.
>
> Behandlingsansvarlige skal ta stilling til den registrertes krav i samsvar med § 9b siste ledd.
>
> Behandlingsansvarlige skal gjøre endringer i samsvar med de frister som er fastsatt i § 26.[303]

[303] Jf. dog nedenfor vedrørende plasseringen av pol §§ 16 og 17.

I tillegg tas inn en bestemmelse i § 9a som understreker den behandlingsansvarliges plikt til å sikre opplysningskvalitet. Vi foreslår at bestemmelsen kan være en fusjon av det som i dag utgjør § 11 første ledd bokstavene d og e og § 27:

> **§ 9a Krav til sikring av opplysningskvalitet**
>
> Den behandlingsansvarlige skal sørge for at personopplysningene som behandles
>
> a) er tilstrekkelige og relevante for formålet med behandlingen, og
>
> b) er korrekte og oppdatert, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen.

Paragraf 28 er ikke egnet som rettighetsbestemmelse. Bestemmelsen innebærer et pålegg overfor den behandlingsansvarlige, og har nøye sammenheng med spørsmålet om hva formålet tilsier mht. spørsmålet om varigheten av lagring og annen fortsatt behandling. Formålet er igjen knyttet til det rettslige grunnlaget for behandlingen. Vi mener derfor at § 28 hører hjemme i kapittel II, plassert etter bestemmelsen vedrørende formål, og at den med fordel kan settes inn (med noen suppleringer) som § 9b i vårt radikale lovforslag:

> **§ 9b Retting av mangelfulle personopplysninger**
>
> Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene, jf. § 18b. Den behandlingsansvarlige skal om mulig sørge for at feilen ikke får betydning for den registrerte, f.eks. ved å varsle mottakere av utleverte opplysninger.
>
> Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.
>
> Dersom tungtveiende personvernhensyn tilsier det, kan Datatilsynet uten hinder av annet ledd bestemme at retting skal skje ved at de mangelfulle personopplysningene slettes eller sperres. Hvis opplysningene ikke kan kasseres i medhold av arkivloven, skal Riksarkivaren høres før det treffes vedtak om sletting. Vedtaket går foran reglene i arkivloven 4. desember 1992 nr. 126 § 9 og § 18.
>
> Sletting bør suppleres med registrering av korrekte og fullstendige opplysninger. Dersom dette ikke er mulig, og dokumentet som inneholdt de slettede opplysningene av den grunn gir et åpenbart misvisende bilde, skal hele dokumentet slettes.
>
> Dersom den registrerte krever at opplysninger skal rettes, slettes, suppleres eller sperres (jf. § 23), skal den behandlingsansvarlige vurdere spørsmålet. Blir

> ikke kravet etterkommet, skal den behandlingsansvarlige gi en konkret begrunnelse for dette. Paragraf 25 – 26 gjelder tilsvarende.

Dersom en velger å gjøre disse redaksjonelle endringene, vil kapittel IV i loven være tømt. Kapittelet kan dermed benyttes til de foreslåtte bestemmelsene om Personvernombud. Endringene av plassering og formulering av § 27, samt flyttingen av § 25, gjør at kapittel III ikke lenger bare vil bestå av bestemmelser vedrørende innsynsrettigheter, men vil gjelde registrerte personers rettigheter generelt. Kapittelet kan da få tittelen "Registrerte personers rettigheter", og alle rettigheter vil her være samlet under ett.

#### 12.5.2.6 Plasseringen av §§ 16 og 17

Paragraf 16 om svartider mv. og § 17 om betaling står i dag til slutt i kapittel II. Årsaken er (formodentlig) at det er to rettighetskapitler. Siden både § 16 og § 17 gjelder gjennomføring av rettigheter, har det ikke vært mulig å plassere disse bestemmelsene i ett av disse kapitlene. Ovenfor har vi imidlertid foreslått å etablere et kapittel III der alle rettigheter inngår. Paragraf 16 og 17 bør derfor plasseres til slutt i dette kapittelet, etter nåværende § 24 som regulerer hvordan innsyn skal gis.

### 12.5.3 Spørsmål knyttet til forholdet mellom lov og forskrift

#### 12.5.3.1 Oversikt

Lovdata har ført opp følgende forskrifter med hjemmel i personopplysningsloven:

1. Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265 (FAD), med hjemmel i pol §§ 3, 4, 12, 13, 14, 23, 26, 30, 31, 32, 33, 41, 43, 44, 48, 51.

2. Forskrift om kontroll med post- og telegramforsendelser av 19. august 1960 nr. 0002 (JD), med hjemmel i pol § 23.

3. Forskrift om kommunikasjonskontroll (kommunikasjonskontrollforskriften) av 31. mars 1995 nr. 281 (JD), med hjemmel i pol § 23.

4. Delegering av myndighet til Datatilsynet etter personopplysningsforskriften av 4. november 2003 nr. 1932 (FAD), med hjemmel i pol § 33.

5. Overføring av ansvarsområder fra Justis- og politidepartementet til Kommunal- og regionaldepartementet, Kulturdepartementet, Arbeids- og administrasjons-departementet, Nærings- og handelsdepartementet, Finansdepartementet, Statsministerens kontor og Landbruksdepartementet. Delegering av myndighet, av 15. desember 2000 nr. 1263 (SMK).

Forskriften under 1 er hovedforskriften, og er nærmere drøftet i dette avsnittet. Forskriftene under 2 og 3 er gitt med primær hjemmel i andre lover, og de to siste vedtakene gjelder overføring og delegasjon av myndighet etter personopplysningsloven. Her nøyer vi oss med kort å bemerke at det ville ha gitt bedre orden og klarhet dersom all kompetansetildeling

vedrørende loven hadde vært samlet i én organisatorisk avgjørelse, jf. nr. 4 og 5 på listen ovenfor.

Personopplysningsforskriften (pof) har følgende kapittelinndeling:

Kapittel 1. Personopplysningslovens virkeområde
Kapittel 2. Informasjonssikkerhet
Kapittel 3. Internkontroll
Kapittel 4. Kredittopplysningsvirksomhet
Kapittel 5. Reservasjonsregisteret
Kapittel 6. Overføring av personopplysninger til utlandet
Kapittel 7. Melde- og konsesjonsplikt
I. Konsesjonsplikt m.m.
II. Behandlinger som er unntatt fra meldeplikt
III. Behandlinger som er unntatt fra konsesjonsplikt og meldeplikt
IV. Behandlinger som er unntatt fra konsesjonsplikt, men underlagt meldeplikt
Kapittel 8. Fjernsynsovervåking
Kapittel 9. Forskjellige bestemmelser
Kapittel 10. Sluttbestemmelser

Vi har tidligere fremmet forslag som vil innebære at kapittel 5 tas ut og gis som forskrift med hjemmel i markedsføringsloven. Kapittel 7 vil bli vesentlig redusert dersom våre forslag til endringer i bestemmelser vedrørende melde- og konsesjonsplikt blir fulgt.

#### 12.5.3.2 Bestemmelser i forskriften som bør vurderes tatt inn i loven

Som grunnlag for denne drøftelsen velger vi å anta at forskrifter generelt er langt mindre tilgjengelig for de fleste behandlingsansvarlige og registrerte personer enn loven. Retningslinjen må derfor være at bestemmelser som de fleste brukere av loven bør kjenne for å unngå at det oppstår vesentlige misforståelser vedrørende innholdet av den totale rettslige reguleringen i lov og forskrift, bør plasseres som del av *lov*teksten. Omvendt bør bestemmelser som primært er av betydning for en begrenset gruppe brukere av loven og forskrift, plasseres i forskriften. Det samme gjelder regler som inneholder detaljregler på et område.

Vi har ikke kommet over bestemmelser i loven som er av slik karakter at de bør overflyttes forskriften. Derimot mener vi enkelte forskriftsbestemmelser bør vurderes tatt inn i loven.

I forskriftens kapittel 1 er det gitt bestemmelser vedrørende lovens saklige og geografiske virkeområde. Blant unntakene for det saklige virkeområde er ”saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvistemålsloven og tvangsfullbyrdelsesloven mv.)”, se § 1-3. Dette utgjør etter vår mening en så vesentlig begrensing i lovens virkeområde, at den bør tas inn i § 3d i det radikale lovforslaget og i § 4 i vårt moderate forlag. Øvrige bestemmelser i pof kapittel 1 har et slikt innhold at de kan stå i forskriften.

I pof kapittel 9 er det tatt inn flere bestemmelser som gjelder Personvernnemda. De fleste av disse er av så detaljert/teknisk karakter at de kan stå i forskriften. Første ledd i § 9-1 fastsetter nemndas kompetanse:

> Personvernnemnda behandler klager over Datatilsynets avgjørelser som nevnt i personopplysningsloven § 42 fjerde ledd og klager over Datatilsynets enkeltvedtak etter forskriften her.

Første delen av forskriftsbestemmelsen gjengir pol § 43 første ledd første setning: "Personvernnemnda avgjør klager over Datatilsynets avgjørelser, jf. § 42 fjerde ledd". Den materielle betydningen av pof § 9-1 er med andre ord at den gir nemnda kompetanse også i forhold til vedtak etter forskriften. Denne delen av Personvernnemndas kompetanse er etter vår mening så avgjørende at den bør fremgå direkte av loven. Personopplysningsloven § 43 annet ledd kan for eksempel lyde:

> Personvernnemnda behandler klager over Datatilsynets avgjørelser som nevnt i personopplysningsloven § 42 fjerde ledd og klager over Datatilsynets enkeltvedtak etter forskrift om behandling av personopplysninger (personopplysningsforskriften) 15. desember 2000 nr. 1265.

Personopplysningsforskriften § 9-3 inneholder en bestemmelse om bruk av fødselsnummer:

> **§ 9-2. Forsendelser som inneholder fødselsnummer**
>
> Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon.

Dette er en detaljbestemmelse som normalt derfor bør inngå i forskrift snarere enn i lov. Undersøkelser viser imidlertid at 90% av befolkningen anser fødselsnummer som en opplysningstype som det er veldig eller ganske viktig å beskyttte.[304] Det kan derfor antas at det er stor allmenn interesse for hvilke regler som gjelder for bruk av slike numre.

Personopplysningsloven § 12 inneholder en bestemmelse om "Bruk av fødselsnummer m.v." Denne bestemmelsen innbefatter også "andre entydige identifikasjonsmidler", og blant disse er identifikasjonsmidler som gjør bruk av biometri. Biometriske metoder for identifisering reiser så mange særlige spørsmål, at det etter vår mening er grunn til å behandle disse i en egen bestemmelse. I så fall kan § 12 endres slik at den utelukkende gjelder fødselsnumre. Den siterte bestemmelsen i pof § 9-3 kan i så fall inngå som tredje ledd i en omredigert pol § 12.

#### 12.5.3.3 Drøftelse av samsvaret mellom loven og enkelte forskriftsbestemmelser

Under dette avsnittet vil vi ta opp spørsmålet om forholdet mellom bestemmelsene i pof kapittel 2 og 3 og hjemmelsbestemmelsene i personopplysningsloven. Dette er delvis innholdsmessige spørsmål, men dels også strukturspørsmål fordi det gjelder forholdet mellom regelverksnivåene.

Kapittel 2 om sikring av personopplysninger har i § 2-1 en slags formålsbestemmelse. Første ledd lyder:

> **§ 2-1. Forholdsmessige krav om sikring av personopplysninger**

[304] Se Ravlum 2005a tabell 4.1.

> Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det *for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet* er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene. (vår kursiv)

Vi mener det er et problem at det i forskriften uttrykkes et formål med sikkerhetsbestemmelsene som går ut over formålet for loven som er hjemmel for bestemmelsene om informasjonssikkerhet. I pol § 1, heter det således:

> **§ 1. Lovens formål**
>
> Formålet med denne loven er å beskytte den enkelte mot at *personvernet* blir krenket gjennom behandling av personopplysninger.
>
> Loven skal bidra til at personopplysninger blir behandlet i samsvar med *grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger*. (vår kursiv)

Etter vår mening kan ikke formålet med forskriften være videre enn formålet med personopplysningsloven som hjemler forskriftsbestemmelsene. Formålsbestemmelsen i pol § 1 må derfor også legges til grunn ved tolkningen av forskriften, herunder dennes kapittel 2.

Kapittel 2 om informasjonssikkerhet er hjemlet i pol § 13 tredje ledd som lyder:

> Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Bestemmelsen inneholder ikke holdepunkter for at forskrift om informasjonssikkerhet kan gis for andre hensyn enn lovens formålsbestemmelse angir.

Personopplysningsforskriften er også hjemlet i helseregisterloven,[305] og formålet med denne loven er:

> **§ 1. Lovens formål**
>
> Formålet med denne lov er å bidra til å gi helsetjenesten og helseforvaltningen informasjon og kunnskap uten å krenke personvernet, *slik at helsehjelp kan gis på en forsvarlig og effektiv måte*. Gjennom forskning og statistikk skal loven bidra til informasjon og kunnskap om befolkningens helseforhold, årsaker til nedsatt helse og utvikling av sykdom for administrasjon, kvalitetssikring, planlegging og styring. Loven skal sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger. (vår kursiv)

Når personopplysningsforskriften anvendes med utgangspunkt i helseregisterloven, vil derfor "hindre fare for tap av liv og helse" i pof § 2-1 være relevant. Vi kan imidlertid ikke finne grunnlag for at "økonomiske tap og tap av anseelse" er i samsvar med lovbestemmelser som hjemler forskriften.

Etter vårt syn må personopplysningsloven forstås slik at det kun er personvern i den betydning som er angitt i pol § 1 som kan angis som formål for arbeid med informasjonssikkerhet. Det innebærer at det ikke alene er nok at for eksempel økonomiske interesser står på spill for at det skal oppstå en plikt til å sikre personopplysningene. En helt annet forhold er at manglende sikring av personopplysninger *også* kan ha økonomiske implikasjoner, helsemessige konsekvenser mv. Det kan ikke avvises at slike mulige konsekvenser vil kunne få innvirkning på vurderingen av de personvernmessige konsekvensene. Personopplysningsforskriften § 2-1 første ledd har imidlertid én oppregning der personvernhensyn og andre hensyn presenteres som likestilte. Etter vårt syn er dette ikke i god harmoni med hjemlene i personopplysningsloven.

[305] Se hrl § 16 siste ledd.

Etter vår mening er det uheldig at pof § 2-1 første ledd har et innhold som er i dårlig samsvar med loven. I en situasjon der personopplysningsforskriften er hjemlet i flere lover med ulike formål, mener vi det er særlig uheldig med separat formålsangivelse i forskriften. Paragraf 2-1 første ledd bør derfor endres.

Neste forhold vi tar opp gjelder samsvaret mellom pol § 13 og pof kapittel 2, henholdsvis pol § 14 og pof kapittel 3. Første ledd i § 13 lyder:

> Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for *tilfredsstillende* informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. (vår kursiv)

I bestemmelsens siste ledd er Kongen gitt myndighet til å gi forskrifter om informasjons-sikkerhet, "herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak". Rammen for slike forskrifter er pol § 13, og særlig første ledd som fastsetter at informasjonssikkerheten skal være "tilfredsstillende". Bestemmelsen innebærer at det skal gjøres en konkret risikovurdering, og det skal settes i verk slike tiltak at sikkerheten anses å være tilfredsstillende. Det forutsettes med andre ord at den behandlingsansvarlige[306] skal gjennomføre konkrete vurderinger og iverksette adekvate tiltak. Datatilsynet kan imidlertid overprøve disse vurderingene, se pol § 2-2, jf. pol § 46.

I pof § 2-1 annet ledd heter det at

> Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.

Bestemmelsen reflekterer kravet om "tilfredsstillende" informasjonssikkerhet og nødvendigheten av å gjøre konkrete vurderinger. Det er således ingen nødvendig motstrid mellom denne bestemmelsen og pol § 13 første ledd. De øvrige bestemmelsene i forskriftens kapittel 2 om informasjonssikkerhet, inneholder imidlertid *påbud* om å gjennomføre, organisatoriske, tekniske og fysiske sikringstiltak mv. Således er det gjennomgående benyttet "skal" i alle de i alt 16 paragrafene i sikkerhetskapittelet som er rettet mot behandlings-ansvarlige. Det er vanskelig å se hvorledes slike plikter til å gjennomføre tiltak, harmonerer med kravet om "tilfredsstillende" informasjonssikkerhet som er fastsatt ut i fra en konkret vurdering av hver behandling av personopplysninger. Vi tar ikke her stilling til hvorledes problemet bør løses, men mener at pol § 13 og/eller forskriftens kapittel 2 bør endres slik at det er langt bedre samsvar mellom de to nivåene.

Etter vår mening eksisterer det et lignende problem i forholdet mellom pol § 14 om internkontroll og kapittel 3 i forskriften om internkontroll. I bestemmelsens første ledd heter det at

> Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske *tiltak som er nødvendige* for å oppfylle kravene i eller i medhold av denne loven […] (vår kursiv)

Også her forutsettes det en konkret vurdering av hver behandling av personopplysninger, og det er den behandlingsansvarlige som – i første omgang – selv skal ta stilling til om det er nødvendig med tiltak og hvilke tiltak som eventuelt er påkrevet å iverksette. Til tross for dette er det i pof § 3-1 tredje ledd bokstavene a – f gitt en rekke "skal"-krav. Kravenes

[306] Tilsvarende krav gjelder i forhold til eventuelle databehandlere.

obligatoriske karakter understrekes av at Datatilsynet i § 3-2 er gitt kompetanse til å dispensere fra kravene i forskriftens kapittel 3 "når særlige forhold foreligger".

De obligatoriske kravene i forskriften innebærer påbud om at behandlingsansvarlig skal ha *rutiner* for en rekke forhold/hendelser vedrørende innhenting av samtykke, formålsbestemthet, opplysningskvalitet, gjennomføring av innsyn, reservasjonsrettigheter og melde- og konsesjonsplikt. Vårt poeng er at det i en rekke tilfelle over hode ikke er aktuelt med slike rutiner, og at det i andre tilfelle lett kan hevdes at slike rutiner ikke er nødvendige, jf. pol § 14 første ledd. Etter gjeldende forskrifter er det for eksempel en rekke behandlinger av personopplysninger som verken kommer inn under melde- eller konsesjonsplikt, og det er derfor åpenbart at disse ikke skal ha rutiner for "oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt", jf. pof § 3-1 tredje ledd bokstav f. I andre tilfeller er problemområdet aktuelt, der det skal for eksempel innhentes samtykke. Likevel vil dette lett kunne ha et så lite omfang og innebære så begrenset skade for personvernkrenkelser, at etablering av en "rutine" ikke kan sies å være nødvendig for å sikre etterlevelse av loven mv.

Vi vil heller ikke på dette punktet fremme forslag om hvorledes samsvaret mellom pol § 14 og forskriftens kapittel 3 skal bli tilfredsstillende. Det er imidlertid avgjørende at en finner frem til løsninger som vil kunne oppleves som anvendbare og fornuftige, uansett om det er en stor statsetat eller en liten privat bedrift som skal finne frem til hva som er "tilfredsstillende" (kapittel 2) eller "nødvendig" (kapittel 3).

### 12.5.4 Avsluttende kommentarer

Avslutningsvis anbefaler vi at det arbeides for å motvirke at forskriften til personopplysningsloven får et stort omfang. For det første bør en i så stor grad som mulig velge rettslige utgangspunkter i loven som innebærer at behovet for unntak blir lite. Vårt forslag til nye konsesjonsbestemmelser er et eksempel på det. For det andre bør alle bestemmelser som har generell eller annen vesentlig betydning for forståelsen av loven, plasseres i loven selv. For det tredje bør alle detaljregler som gjelder særskilte livsområder, der det finnes adekvat lovgivning på området, om mulig plasseres i slik lov, eller som forskrift med hjemmel i slik lov. Den viktigste begrunnelsen for dette er at behandling av personopplysninger som regel er en så integrert del av annen virksomhet at den rettslige reguleringen av slik informasjonsbehandling må inngå i øvrig rettslig regulering på vedkommende området. Sammenhengen med de generelle reglene i og i medhold av personopplysningsloven, kan understrekes ved hjelp av lovhenvisninger mv. Det er videre grunn til å understreke at slik plassering av detaljregler ikke nødvendigvis berører spørsmålet om tilsynsmyndighetenes kompetanse. Således inneholder for eksempel lov om Schengen informasjonssystem særlige regler om behandling av personopplysninger, samtidig som Datatilsynet er tilsynsmyndighet etter loven.[307]

[307] Jf. lov 16. juli 1999 nr. 66, herunder §§ 21 til 24 om Datatilsynet som tilsynsmyndighet.

# Kapittel 13

## Samlet presentasjon av lovforslag

### 13.1 Innledning

I det følgende presenterer vi to alternative lovforslag. Det første forslaget er vårt primære forslag og det som etter vår mening vil gi den klareste og beste revisjonen av loven. Fordi endringene her er store, har vi benevnt dette "radikalt lovforslag". Det andre forslaget inneholder også flere viktige endringer, men fremstår likevel som langt mer moderat, fordi det ikke innebærer strukturelle endringer av betydning, se "moderat lovforslag" i avsnitt 13.3.

Når lovforslagene leses, må en særlig være oppmerksom på to forhold. For det første er forslagene begrenset av mandatet, noe som innebærer at flere deler av loven ikke har vært gjenstand for vår vurdering, og således ikke er omfattet av våre forslag. Slik sett er begge lovforslag ufullstendige. For det andre, kan det være grunn til å minne om at forslagene er utarbeidet uten bred deltakelse og prøving av formuleringer, sammenhenger mv. Selv om vi selvsagt har lagt vekt på å utforme klare og konsistente bestemmelser, kan det derfor være en noe større mulighet enn ellers for at enkelte bestemmelser trenger videre bearbeiding. På ett punkt i det radikale forslaget (§ 33a), er valgte tallstørrelser snarere en antydning av hva som kan være aktuelt, enn en klar anbefaling fra vår side.

For at det skal være mulig å skjelne mellom våre forslag og opprinnelig lovtekst, er de opprinnelige lovtekstene satt i denne skrifttypen. Der en bestemmelse både inneholder opprinnelig og ny tekst, slik at det samlet sett fremstår som en ny bestemmelse, er hele teksten markert som vårt forslag.

### 13.2 Radikalt lovforslag

Det følgende lovforslaget er "radikalt" i den betydning at forslaget innebærer forholdsvis store redaksjonelle og systematiske endringer, særlig i de to første kapitlene. I tillegg er det forslag som innebærer at gjeldende rett kommer langt tydeligere frem, direkte av ordlyden i bestemmelsene. Vi har også foreslått flere materielle endringer, som for eksempel begrenser lovens saklige virkeområde, reduserer melde- og konsesjonsplikt, og innføring av en tydeligere og mer omfattende ordning med personvernombud.

Det radikale lovforslaget innebærer noe mer tekst enn i någjeldende lov. Dette er gjort for at lovteksten i langt større grad enn tidligere skal være forståelig uten dypdykk i forarbeider og forvaltningspraksis. Noe tekst har dessuten kommet til fordi forskriftsbestemmelser er flyttet opp i loven. Den totale tekstmengden etter vårt radikale lovforslag, er likevel klart redusert, fordi forskriftsbestemmelsene vil få en langt mindre omfang.

Når tekstmengde og regelkompleksistet skal vurderes, er det etter vår mening viktig å vurdere lov og forskrift i sammenheng. Forutsetningen må være at behandlingsansvarlige og registrerte personer må lese og forstå de bestemmelser som angår dem, uansett om bestemmelsene er plassert i loven eller i forskriften. Forskriften kan derfor ikke brukes for å "gjemme bort" et regelvolum og en kompleksitet for å kunne gi et skinn av enkelthet med en forholdvis kortfattet lovtekst.

# Kapittel I Lovens formål, virkeområde, grunnleggende begreper og krav til organisering

## § 1. Lovens formål

Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.

Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

## § 2. Personopplysning og personregister

Med personopplysning forstår en i denne loven: opplysninger og vurderinger som direkte eller indirekte kan knyttes til en levende, identifiserbar, fysisk enkeltperson.

Med sensitive personopplysninger forstår en i denne loven; opplysningstyper som er egnet til å åpenbare

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk 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.

Personopplysninger kan komme til uttrykk som skrift, bilde, lyd eller andre signaler.

Opplysninger om døde personer som samtidig er opplysninger om levende personer, regnes bare som personopplysninger dersom de gjelder den levende personens familiemessige relasjoner eller arvelige, helsemessige forhold.

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

Opplysninger som både gjelder fysiske personer og organisasjoner, regnes bare som personopplysninger dersom de direkte gjelder personers personlige relasjoner, klientforhold, formelle posisjoner, handlinger, preferanser, evner eller behov.

Humant biologisk materiale (inklusiv bestanddeler av slikt materiale) regnes ikke i seg selv som personopplysning etter denne loven.

Med personregister forstår en i denne loven: systematiske fortegnelser over personopplysninger eller lagringsmedier som understøtter gjenfinning av opplysninger om bestemte personer.

## § 3. Saklig virkeområde

Loven gjelder for:

a) behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, og

b) annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister.

Med behandling av personopplysninger forstår en i denne loven: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Kongen kan gi forskrift om at loven eller deler av den ikke skal gjelde for bestemte institusjoner eller saksområder.

Kongen kan gi forskrift om behandling av personopplysninger i særskilte virksomheter eller bransjer.

**§ 3a. Unntak fra loven for private aktiviteter**

Loven gjelder ikke behandling av personopplysninger som den enkelte foretar som ledd i rent personlige, familiemessige eller andre private aktiviteter.

**§ 3b. Unntak fra deler av loven for å ivareta ytringsfrihet**

For behandling av personopplysninger utelukkende for kunstneriske, litterære eller journalistiske, herunder opinionsdannende, formål gjelder bare bestemmelsene i kap. I, §§ 13-15, kap. VII og kap. VIII.

**§ 3c. Behandling av personopplysninger i rettspleien mv.**

Personopplysningsloven gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvistemålsloven og tvangsfull-byrdelsesloven mv.).

**§ 3d. Unntak fra deler av loven for personopplysninger som er strengt pseudonymisert**

For personopplysninger som bare er knyttet til et strengt pseudonym, gjelder ikke bestemmelsene i kap. III.

Med strengt pseudonym menes et kjennetegn som erstatter alle ekte identifiserende kjennetegn ved personen, og som effektivt skjuler personens virkelige identitet. Kongen fastsetter ved forskrift hvilke organisatoriske, tekniske og andre krav som må tilfredsstilles for at opplysninger kan regnes som strengt pseudonymiserte.

Før streng pseudonymisering er gjennomført, og dersom strengt pseudonymiserte opplysninger tilbakeføres til personens ekte identitet, kommer hele loven til anvendelse.

## § 4. Geografisk virkeområde

Loven gjelder for behandlingsansvarlige som er etablert i Norge, jf. § 7. Kongen kan i forskrift bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen, og fastsette særlige regler om behandling av personopplysninger for disse områdene.

Loven gjelder også for behandlingsansvarlige som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge. Dette gjelder likevel ikke dersom hjelpemidlene bare brukes til å overføre personopplysninger via Norge.

## § 5. Forholdet til andre lover

Bestemmelsene i loven gjelder for behandling av personopplysninger om ikke annet følger av en særskilt lov som regulerer behandlingsmåten.

Loven her begrenser ikke innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger.

## § 6. Om registrert person og krav til gyldig samtykke

Med registrert person forstås i denne loven en person som en personopplysning kan knyttes til. Registrert person har rett til å anvende rettigheter etter loven, og kan for øvrig påtale forhold som har betydning for etterlevelse av bestemmelsene i lov, forskrift og konsesjon.

Behandling av personopplysninger kan være avhengig av samtykke fra den registrerte, se § 8a bokstav d. For at en registrert person gyldig kan anses å ha gitt sitt samtykke, må det foreligge en viljeserklæring som er frivillig, uttrykkelig og informert. I erklæringen må det klart fremgå at den registrerte personen godtar behandling av opplysninger om seg selv. Det må minst gis opplysninger til den registrerte personen tilsvarende det som er fastsatt i § 17.

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.

## § 6a. Barns adgang til å opptre som registrert person

Personer under 18 år kan opptre som registrert person (jf. § 6 første ledd) etter bestemmelsene i denne loven på følgende måter:

a) For barn mellom 7 og 12 år kan barnets foreldre opptre alene. Foreldrene bør om mulig først spørre barnet om hva det mener om vedkommende personvernspørsmål.

b) For barn mellom 12 og 15 år skal barn og foreldre opptre i fellesskap. Barn kan likevel opptre alene overfor behandlingsansvarlige som har personvernombud i samsvar med kapittel IV i denne loven.

c) Barn mellom 15 og 18 år kan opptre alene, uten foreldrenes medvirkning.

Uansett bestemmelsene i a – c, kan barnets foreldre gripe inn i den utstrekning ivaretagelse av foreldreansvaret gjør dette nødvendig.

## § 7. Behandlingsansvarlig virksomhet eller person

Med behandlingsansvarlig forstår en i denne loven en virksomhet eller person som har rett til å bestemme over behandling av personopplysninger i siste instans, herunder over formålet med behandlingen og hvilke hjelpemidler som skal brukes.

Det skal være en behandlingsansvarlig virksomhet eller person for hver behandling av personopplysninger, jf. § 3.

Behandlingsansvarlige virksomheter kan delegere utøvelsen av behandlingsansvaret til underordnede virksomheter dersom disse er underlagt full instruksjonsmyndighet vedrørende utøvelsen av behandlingsansvaret.

Dersom behandlingsansvaret er delt mellom flere virksomheter og/eller personer, skal disse inngå en skriftlig avtale der det fremgår hvorledes ansvaret skal fordeles og ivaretas.

En behandlingsansvarlig virksomhet eller person som ikke er etablert i Norge, men som utfører behandlinger av personopplysninger som kommer inn under norsk lov i samsvar med § 4 annet ledd, skal peke ut en stedlig representant. Stedlige representant skal ivareta rollene som daglig leder og driftsansvarlig for de deler av behandlingen som skjer i Norge, jf. § 7a.

## § 7a. Daglig ansvar for behandling av personopplysninger

Daglig leder for behandlingsansvarlig virksomhet eller behandlingsansvarlige person, har det øverste daglige ansvaret for etterlevelsen av bestemmelsen i denne loven med forskrifter.

Til hver behandling av personopplysninger skal det alltid være en driftsansvarlig person. I virksomheter skal driftsansvarlig person alltid knyttes til en bestemt stilling. Driftsansvarlig person skal ivareta behandlingsansvaret i tråd med daglig leders bestemmelser, og være kontaktperson for registrerte personer og andre som henvender seg til virksomheten om vedkommende behandling av personopplysninger.

## § 7b. Databehandler

Med databehandler forstår en i denne loven en virksomhet eller person som behandler personopplysninger på vegne av den behandlingsansvarlige i henhold til en oppdragsavtale.

## Kapittel II Grunnkrav til behandling av personopplysninger

### § 8. Generelt om krav til rettslig grunnlag for å behandle personopplysninger

For å være lovlig, må behandling av personopplysninger alltid skje:

a) innenfor rammene av bestemmelser om taushetsplikt i lov og forskrift, og

b) ha et rettslig grunnlag i medhold av bestemmelsene i §§ 8 – 8d i denne loven. Det rettslige grunnlaget skal vurderes og fastsettes ut i fra ett eller flere formål, se § 9.

### § 8a. Primære rettslige grunnlag for behandling av personopplysninger

Personopplysninger (jf. § 2 nr. 1) kan behandles dersom:

a) det klart er fastsatt i lov eller med hjemmel i lov at det er adgang til slik behandling, eller

b) etterlevelse av lovgivning gjør det nødvendig at opplysningene blir behandlet, eller

c) behandlingen bare gjelder opplysninger som de registrerte personene selv frivillig har gjort alminnelig kjent, eller

d) den registrerte har gitt sitt samtykke til behandlingen i samsvar med kravene i § 6 annet ledd, og samtykket ikke er trukket tilbake.

### § 8b. Sekundære rettslige grunnlag for behandling av personopplysninger

Dersom vilkårene i § 8a ikke kan oppfylles, eller vilkåret i § 8a bokstav d er umulig eller uforholdsmessig vanskelig eller ressurskrevende å legge til grunn for behandlingen, kan den behandlingsansvarlige likevel behandle de opplysninger som er nødvendig for:

a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, eller

b) å vareta den registrertes vitale interesser og den registrerte ikke er i stand til å samtykke, eller

c) å utføre forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling, eller for forvaltning av helsetjenester, når opplysningene behandles av helsepersonell med lovbestemt taushetsplikt, eller

d) at den behandlingsansvarlige skal kunne fastsette, gjøre gjeldende eller forsvare et gyldig rettskrav eller oppfylle en rettslig forpliktelse, eller

e) at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter, eller

f) for å fremme kulturelle, historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for de registrerte.

**§ 8c. Behandling av personopplysninger på grunnlag av skjønnsmessige avveininger**

Dersom et av vilkårene i §§ 8a og 8b ikke kan oppfylles, kan den behandlingsansvarlige beslutte å igangsette behandling av personopplysninger som er nødvendig for å ivareta egne eller medkontrahenters berettigede interesser. Slik beslutning kan bare treffes dersom:

a) hensynet til personvern ikke overstiger de hensyn som taler for at behandling av personopplysninger skal skje, og

b) det ikke inngår noen sensitiv opplysningstype i den planlagte behandlingen, og

c) det ikke i overveiende grad inngår personopplysninger om barn under 12 år, og

d) behandlingsansvarlig har gjort en systematisk kartlegging av mulige ulemper for den enkeltes personvern.

Forbudet mot å behandle sensitive personopplysninger (bokstav b) gjelder ikke for ideelle organisasjoners behandling av opplysninger om medlemmer og andre personer som frivillig er i regelmessig kontakt med organisasjonen på grunn av organisasjonens ideelle formål. Adgangen til å behandle sensitive personopplysninger gjelder bare opplysninger som blir samlet inn direkte fra de registrerte. Disse opplysningene kan ikke utleveres til andre uten samtykke fra den registrerte, jf. § 6 annet ledd.

**§ 8d. Datatilsynets adgang til å tillate behandling av personopplysninger som mangler rettslig grunnlag etter §§ 8a – 8c**

Dersom viktige samfunnsinteresser tilsier det, kan Datatilsynet treffe enkeltvedtak om at personopplysninger kan behandles også i andre tilfeller enn som nevnt i §§ 8a – 8c. I vedtaket skal det fastsettes hva som skal anses å være tilfredsstillende krav til opplysningskvalitet (jf. § 9a) og sikkerhetstiltak (jf. § 13).

**§ 8e. Register over straffedommer**

Et fullstendig register over straffedommer kan bare føres under kontroll av en offentlig myndighet.

**§ 9. Angivelse av formål for behandlingen**

Den behandlingsansvarlige skal sørge for at personopplysninger

a) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, og

b) ikke blir behandlet for formål som er uforenlige med det opprinnelige formålet, med mindre behandlingsansvarlige enten kan påberope seg en lovhjemmel eller har innhentet et nytt samtykke fra den registrerte for det nye formålet.

Dersom behandlingsansvarlig planlegger å sammenstille personopplysninger for å utføre kontroll med den registrerte eller noen i hans husstand, skal dette eksplisitt angis som formål.

### § 9a. Krav til opplysningskvalitet

Den behandlingsansvarlige skal sørge for at personopplysninger som behandles

a) er tilstrekkelige og relevante for formålet med behandlingen, og

b) er korrekte og oppdatert, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen.

### § 9b. Retting av mangelfulle personopplysninger

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene. Den behandlingsansvarlige skal om mulig sørge for at feilen ikke får betydning for den registrerte, f.eks. ved å varsle mottakere av utleverte opplysninger.

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

Dersom tungtveiende personvernhensyn tilsier det, kan Datatilsynet uten hinder av annet ledd bestemme at retting skal skje ved at de mangelfulle personopplysningene slettes eller sperres. Hvis opplysningene ikke kan kasseres i medhold av arkivloven, skal Riksarkivaren høres før det treffes vedtak om sletting. Vedtaket går foran reglene i arkivloven 4. desember 1992 nr. 126 § 9 og § 18.

Sletting bør suppleres med registrering av korrekte og fullstendige opplysninger. Dersom dette ikke er mulig, og dokumentet som inneholdt de slettede opplysningene av den grunn gir et åpenbart misvisende bilde, skal hele dokumentet slettes.

Dersom den registrerte krever at opplysninger skal rettes, slettes, suppleres eller sperres (jf. § 23), skal den behandlingsansvarlige vurdere spørsmålet. Blir ikke kravet etterkommet, skal den behandlingsansvarlige gi en konkret begrunnelse for dette. Paragraf 25 – 26 gjelder tilsvarende.

### §10. Forbud mot å behandle personopplysninger når formålet ikke lenger tilsier lagring

Den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.

Den behandlingsansvarlige kan uten hinder av første ledd lagre personopplysninger for historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulempene den kan medføre for den enkelte. Den

behandlingsansvarlige skal i så fall sørge for at opplysningene ikke oppbevares på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig.

Den registrerte kan kreve at opplysninger som er sterkt belastende for ham eller henne skal sperres eller slettes dersom dette

a) ikke strider mot annen lov, og

b) er forsvarlig ut fra en samlet vurdering av bl.a. andres behov for dokumentasjon, hensynet til den registrerte, kulturhistoriske hensyn og de ressurser gjennomføringen av kravet forutsetter.

Datatilsynet kan – etter at Riksarkivaren er hørt – treffe vedtak om at retten til sletting etter tredje ledd går foran reglene i arkivloven 4. desember 1992 nr. 126 § 9 og § 18.

Hvis dokumentet som inneholdt de slettede opplysningene gir et åpenbart misvisende bilde etter slettingen, skal hele dokumentet slettes.

### § 11. Bruk av biometriske identifikasjonsteknikker

[...]

### § 12. Bruk av fødselsnummer

Fødselsnummer kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og bruk av fødselsnummer er nødvendig for å oppnå slik identifisering.

Datatilsynet kan pålegge en behandlingsansvarlig å bruke fødselsnummer for å sikre at det ikke skal skje forveksling av identitet.

Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon.

Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer.

### § 13. Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

### § 14. Internkontroll

Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

Kongen kan gi forskrift med nærmere regler om internkontroll.

### § 15. Databehandlerens rådighet over personopplysninger

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.

## Kapittel III Registrerte personers rettigheter mv.

### § 16. Rett til innsyn for enhver

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) hvem som er den driftsansvarlige person (jf. § 7a annet ledd) som registrerte personer kan henvende seg til,

c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra, og

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

## § 17. Rett til innsyn for registrerte personer

Enhver som ber om det, skal få vite om det er registrert opplysninger om vedkommende hos en behandlingsansvarlig.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) hvilke opplysninger om den registrerte som behandles, og

b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i § 16 bokstav a – f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter denne bestemmelsen gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte.

## § 18. Informasjonsplikt når det samles inn opplysninger fra den registrerte

Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) formålet med behandlingen, herunder om opplysningene skal benyttes for å kontrollere den registrerte eller noen i hans husstand,

c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,

d) det er frivillig å gi fra seg opplysningene, og

e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. §§ 16 og 17, og retten til å kreve retting, jf. § 23.

Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd.

## § 19. Informasjonsplikt når det samles inn opplysninger fra andre enn den registrerte

En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 18 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.

Den registrerte har ikke krav på varsel etter første ledd dersom

a) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov,

b) varsling er umulig eller uforholdsmessig vanskelig, eller

c) det er på det rene at den registrerte allerede kjenner til informasjonen varslet skal inneholde.

Når varsling unnlates med hjemmel i bokstav b, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene.

### § 20. Informasjonsplikt ved bruk av personprofiler

Når noen henvender seg til eller treffer avgjørelser som retter seg mot den registrerte på grunnlag av personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, f.eks. som ledd i markedsføringsvirksomhet, skal den behandlingsansvarlige informere den registrerte om

a) hvem som er behandlingsansvarlig,

b) hvilke opplysningstyper som er anvendt, og

c) hvor opplysningene er hentet fra.

### § 21. Rett til informasjon om automatiserte avgjørelser

Hvis en avgjørelse har rettslig eller annen vesentlig betydning for den registrerte og fullt ut er basert på automatisk behandling av personopplysninger, kan den registrerte som avgjørelsen retter seg mot, kreve at den behandlingsansvarlige gjør rede for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen.

### § 22. Unntak fra retten til informasjon

Retten til innsyn etter §§ 16, 17 og 21 og plikten til å gi informasjon etter § 18, § 19 og § 20 omfatter ikke opplysninger som

a) om de ble kjent, ville kunne skade rikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner,

b) det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger,

c) det i medhold av lov gjelder taushetsplikt for,

d) utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre,

e) det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om, herunder hensynet til den registrerte selv.

Dersom det må anses utilrådelig at den registrerte får direkte kjennskap til egne personopplysninger fordi vedkommende på grunn av ung alder eller andre forhold har

utilstrekkelig evne til å forholde seg til opplysningene, skal opplysningene gjøres kjent via en representant for den registrerte (foreldre, lege, advokat mv).

Den som nekter å gi innsyn i medhold av første ledd må begrunne dette skriftlig med presis henvisning til unntakshjemmelen.

Kongen kan gi forskrift om andre unntak fra innsynsretten og informasjonsplikten og om vilkår for bruk av innsynsretten.

### § 23. Rett til å kreve opplysninger slettet, rettet, supplert eller sperret

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er rettslig grunnlag til å behandle (jf. §§ 8 – 8d), har den registrerte rett til å kreve at den behandlingsansvarlige gjør nødvendige endringer ved å slette, rette, supplere eller sperre opplysningen.

Behandlingsansvarlige skal ta stilling til den registrertes krav i samsvar med § 9b siste ledd.

Behandlingsansvarlige skal gjøre endringer i samsvar med de frister som er fastsatt i § 26.

### § 24. Rett til å kreve manuell behandling

Den som en fullt automatisert avgjørelse som nevnt i § 21 retter seg mot eller som saken ellers direkte gjelder, kan kreve at avgjørelsen overprøves av en fysisk person.

Retten etter første ledd gjelder ikke dersom den registrertes personverninteresser varetas på tilstrekkelig måte og avgjørelsen er hjemlet i lov eller knytter seg til oppfyllelse av kontrakt.

### § 25. Om veiledning og hvordan informasjonen skal gis

Dersom annen lovbestemt rett til innsyn gir tilgang til flere opplysninger enn loven her, skal den behandlingsansvarlige av eget tiltak veilede om retten til å be om slikt innsyn.

Informasjonen kan kreves skriftlig hos den behandlingsansvarlige eller hos dennes databehandler som nevnt i § 15. Før det gis innsyn i opplysninger om en registrert, kan den behandlingsansvarlige kreve at den registrerte leverer en skriftlig og undertegnet begjæring.

### § 26. Frist for å svare på henvendelser om informasjon m.v.

Den behandlingsansvarlige skal svare på henvendelser om innsyn eller andre rettigheter etter §§ 16, 17, 21, 22, 23 og 24 uten ugrunnet opphold og senest innen 30 dager fra den dagen henvendelsen kom inn.

Dersom særlige forhold gjør det umulig å svare på henvendelsen innen 30 dager, kan gjennomføringen utsettes inntil det er mulig å gi svar. Den behandlingsansvarlige skal i så fall gi et foreløpig svar med opplysninger om grunnen til forsinkelsen og sannsynlig tidspunkt for når svar kan gis.

### § 26a. Betaling

Den behandlingsansvarlige kan ikke kreve vederlag for å gi innsyn og informasjon eller vurdere krav om sletting mv.

## Kapittel IV Personvernombud

### § 27. Erklæring om å etablere personvernombud

Behandlingsansvarlige kan inngi erklæring til Datatilsynet om at det er etablert en ordning med personvernombud i samsvar med bestemmelsene i §§ 27a – 27b.

Etter at erklæringen er mottatt, utsteder Datatilsynet et sertifikat som bekrefter at ordningen er etablert, og beskriver det nærmere innholdet i ordningen.

Den behandlingsansvarlige har rett og plikt til å benytte sertifikatet med tilhørende informasjon i samband med behandling av personopplysninger som kommer inn under ordningen med personvernombud.

### § 27a. Fordeler knyttet til ordningen med personvernombud

Behandlingsansvarlige som har et sertifisert personvernombud er fritatt fra kravet om internkontroll i § 14.

Datatilsynet skal tilby sertifiserte personvernombud særskilte og kostnadsfrie informasjons-, veilednings- og opplæringstjenester.

### § 27b. Personvernombudets oppgaver

Personvernombudet skal generelt bidra til at behandlingsansvarlige etterlever bestemmelser vedrørende behandling av personopplysninger i lov, forskrift, instruks, avtaler, enkeltvedtak og domsavgjørelser.

Personvernombudet skal bistå personer det er registrert opplysninger om hos den behandlingsansvarlige og dennes databehandler ved å:

a) sikre fullgod informasjon om registrertes rettigheter og plikter i forbindelse med behandling av personopplysninger, og

b) ta opp og videreformidle registrertes synspunkter på lovligheten og hensiktsmessigheten av den behandling av personopplysninger som skjer, og

c) følge opp alle saker der registrerte personer bestrider lovligheten av den behandling av personopplysninger som skjer.

Personvernombudet skal bistå ansatte i den behandlingsansvarliges virksomhet ved å

a) informere om hvilke regler som gjelder for behandling av personopplysninger, og

b) bidra til å forbedre forhold som ansatte kritiserer, og

c) sikre at de ansatte får den nødvendige opplæring.

Personvernombudet skal bistå ledelsen hos den behandlingsansvarlige med å

a) utforme personvernpolicy for den behandlingsansvarliges virksomhet, og

b) skrive årsmelding der det redegjøres for status og pågående arbeid vedrørende personvern og informasjonssikkerhet hos den behandlingsansvarlige. Årsmeldingen skal være offentlig og gratis tilgjengelig for enhver.

### § 28. Tilbaketrekking av sertifikat for personvernombudet

Dersom det kan dokumenteres at et personvernombud gjentatt og grovt har forsømt sine oppgaver etter § 27b, kan Datatilsynet treffe enkeltvedtak om å trekke sertifikatet tilbake. Den behandlingsansvarlige skal i så fall alltid varsles i samsvar med forvaltningsloven § 16.

Sertifikatet kan trekkes tilbake med den varighet som Datatilsynet bestemmer. Tilbaketrekking av sertifikatet innebærer at den behandlingsansvarlige taper retten til å benytte tjenester, betegnelser og informasjon som spesielt er knyttet til den behandlingsansvarliges deltakelse i ordningen med personvernombud. Vedtak om tilbaketrekking av sertifikat, er gjenstand for klage til Personvernnemnda.

## Kapittel V Overføring av personopplysninger til utlandet

### § 29. Grunnleggende vilkår

**[Ingen endringer]**

### § 30. Unntak

Personopplysninger kan også overføres til stater som ikke sikrer en forsvarlig behandling av opplysningene dersom

a) den registrerte har samtykket i overføringen (jf. § 6 annet ledd), og den registrerte forut for avgivelsen av samtykket er gjort oppmerksom på den særlige risiko som overføringen kan innebære,

b) det foreligger plikt til å overføre opplysningene etter folkerettslig avtale eller som følge av medlemskap i internasjonal organisasjon,

c) overføringen er nødvendig for å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,

d) overføringen er nødvendig for å inngå eller oppfylle en avtale med en tredjeperson i den registrertes interesse,

e) overføringen er nødvendig for å vareta den registrertes vitale interesser,

f) overføringen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav,

g) overføringen er nødvendig eller følger av lov for å beskytte en viktig samfunnsinteresse, eller

h) det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.

Datatilsynet kan tillate overføring selv om vilkårene i første ledd ikke er oppfylt dersom den behandlingsansvarlige gir tilstrekkelige garantier for vern av den registrertes rettigheter. Datatilsynet kan sette vilkår for overføringen.

Kongen kan gi forskrift om overføring av personopplysninger til utlandet, herunder om å stanse eller begrense overføring til bestemte stater som ikke tilfredsstiller kravene i § 29.

## Kapittel VI Melde-, varslings- og konsesjonsplikt

### § 31. Plikt til å melde og varsle om ny behandling av personopplysninger

Den behandlingsansvarlige skal gi melding til Datatilsynet om behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler.

Varsel om at meldingen er sendt skal gis til personer som vil bli berørt av den behandlingen av personopplysninger som meldes. Gjelder behandlingen et stort eller ubestemt antall personer, skal varselet gis til relevante interesseorganisasjoner eller meddeles allmennheten på hensiktsmessig måte.

Melding og varsel skal gis senest 30 dager før behandlingen tar til. Datatilsynet skal gi den behandlingsansvarlige kvittering for at melding er mottatt.

Kongen kan gi forskrift om unntak fra melde- og varslingsplikt etter §§ 31 og 31a, og om innholdet i meldinger og varsler etter § 32. Datatilsynet kan gi nærmere regler vedrørende den praktiske gjennomføringen av melde- og varslingsplikten, jf. §§ 31 – 32.

### § 31a. Plikt til fornyet melding og varsel

Ny melding og nytt varsel må gis dersom det skjer endringer i:

a) hvem som har behandlingsansvaret og på hvilken måte ansvaret eventuelt er delt (§ 7), eller

b) det rettslige grunnlaget for behandlingen (§§ 8 – 8d), eller

c) formålet med behandlingen (§ 9), eller

d) dersom opplysninger blir utlevert til andre enn det tidligere opplyst om.

Selv om det ikke har skjedd endringer, skal det gis ny fullstendig melding tre år etter at forrige melding ble gitt, jf. § 31.

### § 32. Meldingens og varselets innhold

Meldingen skal inneholde bekreftelse av at det foreligger dokumentasjon vedrørende behovet for å iverksette tiltak for å

a) sikre personopplysninger i samsvar med § 13, og

b) sikre etterlevelse av lov, forskrift mv. i samsvar med § 14 om internkontroll, jf. likevel § 27a om unntak fra krav om internkontroll for virksomheter med personvernombud.

Det skal videre opplyses om det er fremkommet protester mot den planlagte behandlingen fra organisasjoner som representerer de registrerte personene. Det skal eventuelt kort gjøres rede for slik uenighet, og hvem som har fremmet synspunktene.

Varselet skal gi opplysning om at:

a) melding er sendt til Datatilsynet, og

b) at det eksisterer rett til å kreve konsesjonsbehandling i samsvar med § 33a.

**§ 33. Datatilsynets rett til å kreve konsesjonsbehandling**

Datatilsynet kan etter en konkret vurdering bestemme at behandling av personopplysninger krever konsesjon. Konsesjonsplikt kan bare pålegges dersom det er fare for at behandlingen kan krenke tungtveiende personverninteresser, jf. § 1.

Avgjørelse om plikt til å søke konsesjon skal behandles etter reglene for enkeltvedtak, se forvaltningsloven (fvl) kapittel IV – VI.

Avgjørelse i samsvar med første ledd skal begrunnes, jf. fvl § 25. Ved vurdering av om konsesjonsplikt skal pålegges, kan Datatilsynet bl.a. ta hensyn til om det skal behandles sensitive personopplysninger (jf. § 2 annet ledd), om behandlingen gjelder en gruppe personer med spesielt behov for beskyttelse, om personopplysninger skal sammenstilles fra flere kilder, formålet med behandlingen og mengden personopplysninger.

Den behandlingsansvarlige kan kreve at Datatilsynet avgjør om en behandling vil kreve konsesjon.

Datatilsynet kan gi nærmere regler vedrørende den praktiske gjennomføringen av konsesjonsplikten jf. §§ 33 – 33b.

**§ 33a. Registrerte personers rett til å kreve konsesjonsbehandling**

Registrerte personer eller deres valgte representanter kan kreve at Datatilsynet ilegger konsesjonsplikt for behandling av personopplysninger. Datatilsynet skal konsesjonsbehandle saken dersom

a) det kan dokumenteres at minst 40% av de personene som det vil bli registrert personopplysninger om krever det, eller

b) en organisasjon der mer enn 60% av de registrerte er medlemmer treffer vedtak om det, eller

c) det kan dokumenteres at minst 5000 personer stiller seg bak kravet om konsesjonsbehandling.

Krav om konsesjon etter denne bestemmelsen må fremmes senest 30 dager etter at varsel fra den behandlingsansvarlige ble mottatt, jf. § 31 annet og tredje ledd. Dersom behandlingen omfatter sensitive opplysningstyper (jf. § 2 nr. 7) er fristen 60 dager. Datatilsynet skal gi den behandlingsansvarlige kvittering for at krav om konsesjonsplikt er mottatt.

Datatilsynet kan treffe vedtak om andre grenseverdier enn de som fremgår av første ledd bokstavene a – c. Vedtaket kan bare gjøres for ett år ad gangen, og skal straks kunngjøres. Er det ikke kunngjort noe vedtak, gjelder lovens grenseverdier.

**§ 33b. Konsesjonsplikt i henhold til forskrift**

Kongen kan ved forskrift fastsette at det skal kreves konsesjon for å behandle personopplysninger innen bestemte næringer, for bestemte formål, eller på bestemte måter.

Kongen kan gi utfyllende forskrifter om konsesjonsbehandling etter § 33a og unntak fra konsesjonsplikt etter § 33c.

**§ 33c. Unntak fra konsesjonsplikt når behandlingen har hjemmel i lov**

Datatilsynet kan ikke nekte behandling av personopplysninger eller stille vilkår for at slik behandling kan skje dersom dette vil stride mot bestemmelse i lov eller forskrift gitt i medhold av slik lov. Det samme gjelder behandling av personopplysninger som er utvetydig forutsatt i nevnte lover eller forskrifter.

Innenfor gjeldende lov- og forskriftsbestemmelser som nevnt i forrige ledd, kan Datatilsynet likevel treffe vedtak om supplerende tiltak som åpenbart er nødvendig for å ivareta personvernet, og som ikke hindrer realisering av lovens eller forskriftens formål.

**§ 34. Avgjørelsen av om konsesjon skal gis**

Ved avgjørelsen av om konsesjon skal gis, skal det klarlegges om behandlingen av personopplysninger kan volde ulemper for den enkelte som ikke kan avhjelpes gjennom bestemmelsene i kapitlene II – V og vilkår etter § 35. I så fall må det vurderes om ulempene blir oppveid av hensyn som taler for behandlingen.

**§ 35. Vilkår i konsesjon**

I konsesjonen skal det vurderes å sette vilkår for behandlingen når slike vilkår er nødvendige for å begrense ulempene behandlingen ellers ville medføre for den registrerte.

**[Ingen flere endringer]**

**§ 42a. Datatilsynets kompetanse og rolle i internasjonale forhold**

Datatilsynet kan av eget tiltak eller etter henvendelse fra myndighet i et annet land innenfor EØS-området, kontrollere at behandling av personopplysninger som finner sted i Norge er

lovlig, selv om behandlingen er underlagt lovgivning i et annet EØS-land. Datatilsynet kan kreve de opplysningene som trengs for å gjennomføre denne kontroll, jf. § 44. Bestemmelsene i §§ 45, 46 og 47 får tilsvarende anvendelse.

Uten hinder av taushetsplikt kan Datatilsynet utveksle opplysninger med datatilsynsmyndigheter i andre EØS-land når dette er nødvendig for å utføre Datatilsynets oppgaver.

**§ 43. Personvernnemndas organisering og oppgaver**

Personvernnemnda er et uavhengig forvaltningsorgan administrativt underordnet Kongen og departementet. Paragraf 42 første ledd annet punktum gjelder tilsvarende.

Personvernnemda behandler klager over Datatilsynets avgjørelser som nevnt i personopplysningsloven § 42 fjerde ledd og klager over Datatilsynets enkeltvedtak etter forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265.

## 13.3 Moderat lovforslag

Følgende "moderate" lovforslag bygger i all hovedsak på gjeldende lovtekst. Endringene gjelder særlig to typer spørsmål. For det første har vi innarbeidet de viktigste presiseringene av sentrale begreper mv, men dette er gjort i mindre omfang enn i det radikale lovforslaget. Årsaken er primært at lovens nåværende struktur (særlig i § 2), ikke tillater så omfattende presiseringer som vi i utgangspunktet mener er ønskelig.

For det andre gjelder endringene i det moderate lovforslaget, slike endringer som vi antar er lite kontroversielle, og som lar seg innpasse uten at det får nevneverdige strukturelle konsekvenser eller på annen måte forplanter seg til andre deler av loven og skaper endringsdynamikk. Viktigst blant disse endringene er trolig endringene i mindreåriges kompetanse til å opptre som registrert person (§ 2a), § 8 første ledd bokstav f vedrørende rettslig grunnlag, endringsforslag vedrørende melde- og konsesjonsplikt (§§ 31 og 33) og bestemmelsen om Datatilsynets kompetanse i internasjonale forhold (§ 42a).

## Kapittel I Lovens formål og virkeområde

**§ 1. Lovens formål**

[Ingen endring]

**§ 2. Definisjoner**

I denne loven forstås med:

1) personopplysning: opplysninger og vurderinger som direkte eller indirekte kan knyttes til en levende, identiserbar, fysisk enkeltperson,

2) behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,

3) personregister: systematiske fortegnelser over personopplysninger eller lagringsmedier som understøtter gjenfinning av opplysninger om bestemte personer,

4) behandlingsansvarlig: den fysiske eller juridiske person som har rett til å bestemme over behandlingen av personopplysninger, herunder om formålet for behandlingen og hvilke hjelpemidler som skal brukes,

5) databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige,

6) registrert: den som en personopplysning kan knyttes til,

7) samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,

8) sensitive personopplysninger: opplysningstyper som er egnet til å åpenbare

   a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk 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.

**§ 2a. Barns adgang til å opptre som registrert person**

Personer under 18 år kan opptre som registrert person (jf. § 6 første ledd) etter bestemmelsene i denne loven på følgende måter:

For barn mellom 7 og 12 år kan barnets foreldre opptre alene. Foreldrene bør om mulig først spørre barnet om hva det mener om vedkommende personvernspørsmål.

For barn mellom 12 og 15 år skal barn og foreldre opptre i fellesskap. Barn kan likevel opptre alene overfor behandlingsansvarlige som har personvernombud i samsvar med kapittel IV i denne loven.

Barn mellom 15 og 18 år kan opptre alene, uten foreldrenes medvirkning.

Uansett bestemmelsene i a – c, kan barnets foreldre gripe inn i den utstrekning ivaretagelse av foreldreansvaret gjør dette nødvendig.

**§ 3. Saklig virkeområde**

Loven gjelder for

a) behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, og

b) annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister.

Loven gjelder ikke behandling av personopplysninger som den enkelte foretar som ledd i rent personlige, familiemessige eller andre private aktiviteter.

Kongen kan gi forskrift om at loven eller deler av den ikke skal gjelde for bestemte institusjoner og sakområder.

Kongen kan gi forskrift om behandling av personopplysninger i særskilte virksomheter eller bransjer. For behandling av personopplysninger som ledd i kredittopplysningsvirksomhet kan det i forskrift gis bestemmelser bl.a. om hvilke typer opplysninger som kan behandles, hvilke kilder personopplysninger kan hentes fra, hvem kredittopplysninger kan utleveres til og hvordan utleveringen kan skje, sletting av kredittanmerkninger og taushetsplikt for de ansatte i kredittopplysningsbyrået. Det kan også gis regler om at loven eller enkelte bestemmelser gitt i eller i medhold av den skal gjelde for behandling av kredittopplysninger om andre enn enkeltpersoner.

### § 4. Geografisk virkeområde

[Ingen endring]

### § 5. Forholdet til andre lover

[Ingen endring]

### § 6. Forholdet til lovbestemt innsynsrett etter andre lover

[Ingen endring]

### § 7. Forholdet til ytringsfriheten

[Ingen endring]

## Kapittel II Alminnelige regler for behandling av personopplysninger

### § 8. Vilkår for å behandle personopplysninger

Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for

a) å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,

b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse,

c) å vareta den registrertes vitale interesser,

d) å utføre en oppgave av allmenn interesse,

e) å utøve offentlig myndighet, eller

f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Dersom det sistnevnte grunnlaget anvendes, skal det som del av dokumentasjonen vedrørende internkontroll (jf. § 14) alltid inngå en redegjørelse for og vurdering av hvilke personverninteresser som er aktuelle, og hvilke forhold som begrunner at det ville ha vært uforholdsmessig vanskelig eller ressurskrevende å innhente samtykke.

**§ 9. Behandling av sensitive personopplysninger**

[Ingen endring]

**§ 10. Register over straffedommer**

[Ingen endring]

**§ 11. Grunnkrav til behandling av personopplysninger**

Den behandlingsansvarlige skal sørge for at personopplysningene som behandles

a) bare behandles når dette er tillatt etter § 8 og § 9,

b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,

c) ikke blir behandlet for formål som er uforenlige med det opprinnelige, med mindre behandlingsansvarlige enten kan påberope seg en lovhjemmel eller har innhentet et nytt samtykke fra den registrerte for det nye formålet,

d) er tilstrekkelige og relevante for formålet med behandlingen, og

e) er korrekte og oppdatert, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen, jf. § 27 og § 28.

Senere behandling av personopplysningene for historiske, statistiske eller vitenskapelige formål anses ikke uforenlig med de opprinnelige formålene med innsamlingen av opplysningene, jf. første ledd bokstav c, dersom samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene den kan medføre for den enkelte.

**§ 12. Bruk av fødselsnummer m.v.**

Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Datatilsynet kan pålegge en behandlingsansvarlig å bruke identifikasjonsmidler som nevnt i første ledd for å sikre at personopplysningene har tilstrekkelig kvalitet.

Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon.

Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer og andre entydige identifikasjonsmidler.

### § 13. Informasjonssikkerhet

[Ingen endring]

### § 14. Internkontroll

[Ingen endring]

### § 15. Databehandlerens rådighet over personopplysninger

[Ingen endring]

### § 15a. Ivaretakelse av personvern for personer under 18 år

Personer under 18 år kan opptre som registrert person etter bestemmelsene i denne loven på følgende måter:

a) For barn mellom 7 og 12 år kan foreldre opptre alene. Barn skal om mulig først spørres om hva de mener.

b) For barn mellom 12 og 15 år kan barn og foreldre opptre felles. Barn kan likevel opptre alene dersom det ikke er nevneverdig risiko for at barnets personvern blir skadelidende.

c) Barn mellom 15 og 18 år kan opptre alene, uten foreldrenes medvirkning.

Uansett bestemmelsene i a – c, kan barnets foreldre gripe inn i den utstrekning ivaretagelse av foreldreansvaret gjør dette nødvendig.

### § 16. Frist for å svare på henvendelser om informasjon m.v.

[Ingen endring]

### § 17. Betaling

[Ingen endring]

## Kapittel III Informasjon om behandling av personopplysninger

### § 18. Rett til innsyn for enhver

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,

c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra, og

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

**§ 18a. Rett til innsyn for registrerte personer**

Enhver som ber om det, skal få vite om det er registrert opplysninger om vedkommende hos en behandlingsansvarlig.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) hvilke opplysninger om den registrerte som behandles, og

b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i § 18 første ledd bokstav a – f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte.

**§ 19. Informasjonsplikt når det samles inn opplysninger fra den registrerte**

[Ingen endring]

**§ 20. Informasjonsplikt når det samles inn opplysninger fra andre enn den registrerte**

[Ingen endring]

**§ 21. Informasjonsplikt ved bruk av personprofiler**

[Ingen endring]

**§ 22. Rett til informasjon om automatiserte avgjørelser**

[Ingen endring]

### § 23. Unntak fra retten til informasjon

[Ingen endring]

### § 24. Hvordan informasjonen skal gis

[Ingen endring]

## Kapittel IV Andre rettigheter for den registrerte

### § 25. Rett til å kreve manuell behandling

[Ingen endring]

### § 26. Rett til å reservere seg mot direkte markedsføring

[Ingen endring]

### § 27. Retting av mangelfulle personopplysninger

[Ingen endring]

### § 28. Forbud mot å lagre unødvendige personopplysninger

[Ingen endring]

## Kapittel V Overføring av personopplysninger til utlandet

### § 29 Grunnleggende vilkår

[Ingen endring]

### § 30. Unntak

Personopplysninger kan også overføres til stater som ikke sikrer en forsvarlig behandling av opplysningene dersom

a) den registrerte har samtykket i overføringen (jf. § 2 nr. 7), og den registrerte forut for avgivelsen av samtykket er gjort oppmerksom på den særlige risiko som overføringen kan innebære,

b) det foreligger plikt til å overføre opplysningene etter folkerettslig avtale eller som følge av medlemskap i internasjonal organisasjon,

c) overføringen er nødvendig for å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,

d) overføringen er nødvendig for å inngå eller oppfylle en avtale med en tredjeperson i den registrertes interesse,

e) overføringen er nødvendig for å vareta den registrertes vitale interesser,

f) overføringen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav,

g) overføringen er nødvendig eller følger av lov for å beskytte en viktig samfunnsinteresse, eller

h) det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.

Datatilsynet kan tillate overføring selv om vilkårene i første ledd ikke er oppfylt dersom den behandlingsansvarlige gir tilstrekkelige garantier for vern av den registrertes rettigheter. Datatilsynet kan sette vilkår for overføringen.

Kongen kan gi forskrift om overføring av personopplysninger til utlandet, herunder om å stanse eller begrense overføring til bestemte stater som ikke tilfredsstiller kravene i § 29.

## Kapittel VI Melde- og konsesjonsplikt

### § 31. Meldeplikt

[Ingen endring]

### § 32. Meldingens innhold

Meldingen skal inneholde bekreftelse av at det foreligger dokumentasjon vedrørende behovet for å iverksette tiltak for å

a) sikre personopplysninger i samsvar med § 13, og

b) sikre etterlevelse av lov, forskrift mv i samsvar med § 14 om internkontroll.

Kongen kan gi forskrift om hvilke opplysninger meldingene skal inneholde og om gjennomføringen av meldeplikten.

### § 33. Konsesjonsplikt

Det kreves konsesjon fra Datatilsynet for å behandle slike personopplysninger som er omfattet av personopplysningsforskriften kapittel [xx] (forskrift 15. desember 2000 nr. 1265). Slike forskrifter fastsettes av Kongen.

Dersom behandlingen vil krenke tungtveiende personverninteresser, eller behandlingen gjelder spørsmål av stor prinsipiell betydning (jf. § 1), kan Datatilsynet bestemme at også behandling av andre personopplysninger må ha konsesjon. Slike avgjørelser kan bare treffes som enkeltvedtak, jf. forvaltningsloven § 2 første ledd, bokstav b, jf. bokstav a.

Den behandlingsansvarlige kan kreve at Datatilsynet avgjør om en behandling vil kreve konsesjon.

Konsesjonsplikt etter første og annet ledd gjelder ikke for behandling av personopplysninger i organ for stat eller kommune når behandlingen har hjemmel i egen lov.

Kongen kan gi forskrift om at visse behandlingsmåter ikke trenger konsesjon etter første ledd. For behandlingsmåter som unntas fra konsesjon kan det gis forskrift for å begrense ulemper som behandlingen ellers kan medføre for den registrerte.

### § 34. Avgjørelsen av om konsesjon skal gis

[Ingen endring]

### § 35. Vilkår i konsesjon

[Ingen endring]

## Kapittel VII Fjernsynsovervåking

[Ingen endringer]

## Kapittel VIII Tilsyn og sanksjoner

### § 42. Datatilsynets organisering og oppgaver

[Ingen endring]

### § 42a. Datatilsynets kompetanse og rolle i internasjonale forhold

Datatilsynet kan av eget tiltak eller etter henvendelse fra myndighet i et annet land innenfor EØS-området, kontrollere at behandling av personopplysninger som finner sted i Norge er lovlig, selv om behandlingen er underlagt lovgivning i et annet EØS-land. Datatilsynet kan kreve de opplysningene som trengs for å gjennomføre denne kontroll, jf. § 44. Bestemmelsene i §§ 45, 46 og 47 får tilsvarende anvendelse.

Uten hinder av taushetsplikt kan Datatilsynet utveksle opplysninger med datatilsynsmyndigheter i andre EØS-land når dette er nødvendig for å utføre Datatilsynets oppgaver.

### § 43. Personvernnemndas organisering og oppgaver

Personvernnemnda er et uavhengig forvaltningsorgan administrativt underordnet Kongen og departementet. Paragraf 42 første ledd annet punktum gjelder tilsvarende.

Personvernnemda behandler klager over Datatilsynets avgjørelser som nevnt i personopplysningsloven § 42 fjerde ledd og klager over Datatilsynets enkeltvedtak etter forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265.

[…]

[Ingen flere endringer]

## Kapittel IX Ikraftsetting. Overgangsregler. Endringer i andre lover

[Ingen endringer]

# Kapittel 14

## Administrative og økonomiske konsekvenser og forutsetninger

### 14.1 Innledning

I dette kapittelet gjennomgår vi kort viktige administrative og økonomiske konsekvenser av våre forslag. I tillegg tydeliggjør vi i avsnitt 14.7 det vi mener er administrative *forutsetninger* for forslagene våre. Poenget med å skjelne mellom konsekvenser og forutsetninger, er å understreke at enkelte av forslagene ikke kan tilrås med mindre en er villige til å sette inn ressurser i et bestemt omfang. Det er bl.a. ikke alltid mulig å plukke ut enkelte forslag som en mener har akseptable økonomiske og administrative konsekvenser, og la å realisere andre elementer.

Konsekvensene av ethvert lovforslag ser klart forskjellig ut avhengig av om det er virkninger for vedkommende myndighet eller for private parter det er tale om. Her har vi valgt å kort kommentere konsekvenser for Datatilsynet og behandlingsansvarlige. Vår forutsetning er at registrerte personer ikke skal ha økt kostnad eller nevneverdig økt strev enn det de har etter dagens lovgivning. Tvert i mot er intensjonen gjennomgående å gjøre situasjonen enklere for registerte personer. Dette kan vi i hvert fall oppnå dersom behandlingsansvarlige kan bli flinkere til å etterleve lovens bestemmelser og generelt være mer imøtekommende i forhold til personer som for eksempel krever innsyn.[308]

Den følgende redegjørelsen gjelder våre antagelser. Vi har således ikke hatt tid eller budsjett til å gjøre faktiske undersøkelser hos Datatilsynet eller et utvalg av behandlingsansvarlige virksomheter. Likevel tror vi at vurderingene har verdi. Vurderingene er knyttet til hovedelementene i forslaget, og gjelder forslag som enten både finnes i radikalt og moderat lovforslag, kun i radikalt lovforslag, eller som er knyttet til større deler av forslagene sett under ett.

### 14.2 Tydeliggjøring og omgruppering av bestemmelsene i kapitlene I og II

Forslaget innebærer tydeliggjøring og anvisning av løsninger på en rekke fortolkingsspørsmål som i dag er knyttet til disse kapitlene. En åpenbar konsekvens av endringene er at personer som kjenner loven fra før av, vil måtte sette seg inn i en ny redaksjon av bestemmelsene. Innholdet vil imidlertid være lett gjenkjennelig og forståelig for denne gruppen brukere.

Personer som ikke har befattet seg med detaljer i den nåværende lovteksten, men kun kjenner loven rent overflatisk, vil bli konfrontert med en kompleksitet som de tidligere ikke var klar over. Kompleksiteten er imidlertid ikke ny, og har tidligere krevet studier av litteratur og forarbeider mv. for å bringe klarhet i hva som er en riktig forståelse. Under forutsetning av at slike behandlingsansvarlige gjør forsøk på å finne frem til rettsriktige fortolkninger, innebærer endringen trolig en lettelse fordi loven alene ofte vil gi tilstrekkelig informasjon. På den annen side kan den endrede lovteksten gjøre det vanskeligere å "slurve" med lovanvendelsen, noe som kan innebære en reelt økt belastning for de behandlingsansvarlige. Dette er

[308] Jf. f.eks. Haug 2004 som i et kontrollert forsøk med innsynsbegjæringer som ble sendt av elever ved Brunla ungdomsskole, kun fikk 42% svar (39 av 93 innsynsbegjæringer).

imidlertid en belastning som er en underliggende forutsetning for denne loven, og som internkontrollbestemmelsen i § 14 aktualiserer.

For Datatilsynet vil enhver endring av lovens redaksjon og lovendringer ellers, kunne gi en økt pågang av spørsmål mv., og med et generelt økende behov for informasjons- og veiledningstjenester. Jo flere som faktisk forholder seg til lovteksten, desto større kan denne pågangen bli. Denne effekten vil derfor i stor grad være avhengig av departementenes og Datatilsynets profilering og lansering av lovendringene. For øvrig vil medarbeiderne i Datatilsynet ha en skolering og bakgrunn som gjør det forholdsvis raskt å sette seg inn i endringer som primært er av redaksjonell og systematisk karakter.

## 14.3 Unntak for strengt pseudonymiserte opplysninger

Unntaket forutsetter at det gjøres et videre utviklings- og utredningsarbeid, jf. § 3d i avsnitt 13.2. Arbeidet bør trolig ledes/koordineres fra Datatilsynet, og innebærer en ekstra kostnad for tilsynet i en begrenset periode.

Streng pseudonymisering vil trolig forutsette utvikling av nye tjenester og/eller produkter, noe som innebærer en ny kostnad for behandlingsansvarlige. Ordningen er imidlertid frivillig, og det er derfor opp til hver behandlingsansvarlig å gjennomføre kost/nytte vurderinger av å bruke unntaksalternativet i § 3d. Behandlingsansvarlige vil derfor ha tilfredsstillende kontroll på slike utgifter.

## 14.4 Rett til å kreve opplysninger slettet, rettet mv.

Dette forslaget (se § 23 i avsnitt 13.2) innebærer ikke en prinsipielt ny rettighet, men betyr først og fremst en fremheving av sletting, retting mv. som en individuell rettighet. Tydeliggjøringen kan innebære noe flere begjæringer fra registrete personer mv., men det er ikke grunn til å tro at effekten vil bli stor, og den mulige ekstra pågangen vil langt på vei være avhengig av Datatilsynets informasjonsvirksomhet knyttet til denne rettigheten.

## 14.5 Personvernombud

Forslaget forutsetter store administrative endringer hos Datatilsynet, bl.a. på grunn av behov for å etablere en egen gruppe av ansatte som har ombudene som spesielt arbeidsområde, behov for undervisning og veiledning mv. Tjenester som er spesielt rettet mot personvernombudene er imidlertid ikke spesifikt lovregulert, og Datatilsynet og Fornyings- og administrasjonsdepartementet (FAD) vil derfor ha forholdsvis god kontroll over konsekvensene. Det er imidlertid helt uvisst hvorledes det foreliggende forslaget vil slå an blant de behandlingsansvarlige, og det kan derfor ikke utelukkes at det i perioder blir stor pågang av henvendelser vedrørende ombudsordningen.

Saksbehandlingen i tilknytning til ombudene er foreslått å være meget begrenset. Opprettelsen av personvernombud er forutsatt å være basert på en ensidig ”erklæring” fra den behandlingsansvarlige (§ 27). Eventuelt tilbaketrekking av ombudsmannsordninger, vil være langt mer krevende. Det er imidlertid ikke grunn til å tro at det vil være mange som svikter i en rolle som er frivillig.

For at personvernombudene skal fungere, må det trolig utvikles et enkelt internett-basert hjelpemiddel for å håndtere erklæringer, utarbeide tilstrekkelig informasjonsmateriale, "sertifikat" mv. Det er imidlertid tale om beskjedne utviklingsprosjekter.

## 14.6 Melde-, varslings- og konsesjonsplikten

Forslagene vedrørende endringer i melde-, varslings- og konsesjonsplikten utgjør den gruppen av forslag som har de største administrative og økonomiske virkninger. Vi har valgt å kommentere radikalt og moderat lovforslag samlet. Drøftelsene vedrørende det radikale forslaget er det mest omfattende, og vil derfor være utgangspunkt for de fleste av drøftelsene. Begge forslag er ment å innebære lettelser både for Datatilsynet og for behandlingsansvarlige.

### 14.6.1 Meldeplikten

Forslaget i § 32 innebærer en lettelse for den behandlingsansvarlige på to måter. For det første er meldingenes innhold vesentlig redusert, og innebærer at selve innmeldingen er mindre ressurskrevende. På den annen side, skifter meldingen karakter fra å være inngivelse av et sett av opplysninger som beskriver vedkommende behandling, til å bli et varsel om at den behandlingsansvarlige har utført sine plikter i henhold til § 13 (informasjonssikkerhet) og § 14 (internkontroll). Slik sett innebærer endringen et større press på behandlingsansvarlige i retning av å etterleve lovens krav, og dette vil kunne gi større arbeidsmengde.

Når det gjelder Datatilsynet, innebærer endringen i innholdet av meldingene at informasjonsmengden blir langt mindre å håndtere. Dette innebære neppe noen lettelse for tilsynet, fordi tilsynet så vidt vi kjenner til, i dag ikke gjør aktiv bruk av innkomne meldinger. Innholdet av meldingene etter vårt forslag, vil gjøre disse svært nyttige for Datatilsynet og bør legge til rette for at meldeordningen kommer i aktiv bruk. Således legger meldingene til rette for dokumentkontroll, fordi både § 13 og § 14 krever at tiltak skal dokumenteres. Datatilsynet har i økende grad gjennomført kontroller ved å innhente og vurdere slik eksisterende dokumentasjon, noe som klart øker kontrollkapasiteten i tilsynet. Kontrollen kan både ta utgangspukt i "positiv" og "negativ" kunnskap, dvs. en kan gjennomføre kontroller av behandlingsansvarlige som har meldt, og en kan – ikke minst – gjennomføre kontroller med behandlingsansvarlige som ikke har meldt inn at de har fulgt loven på disse to helt sentrale punktene.

Et økt press på behandlingsansvarlige kan komme til å generere flere spørsmål vedrørende informasjonssikkerhet og internkontroll, noe som kan innebære en økt arbeidsbelastning på tilsynet, særlig i en innkjøringsfase. En mulig respons kan imidlertid være å utarbeide bedre informasjon og hjelpemidler som gjøres tilgjengelig via nettet, og dette kan trolig dempe en enventuelt økt pågang noe.

For det andre innebærer endringen i melderutinen at fornyet melding kun skal inngis ved bestemte typer endringer, og ikke som i dag ved enhver endring.[309] Denne lettelsen vil imidlertid i praksis trolig ha marginal betydning fordi, så vidt vi kjenner til, sendes det i dag forholdsvis få endringsmeldinger.

[309] De endringer som det her er tale om, innebærer at det må skje ny vurdering av informasjonssikkerhet og internkontroll.

### 14.6.2 Varslingsplikten

Plikten til å varsle berørte personer mv. i forslaget til § 31 annet ledd, vil kun berøre behandlingsansvarlige, og vil kun være aktuelt i tilfeller av nye behandlinger og ved nærmere bestemte endringer av eksisterende behandling. Forslaget vil således bare innebære marginale konsekvenser for den behandlingsansvarlige, og vil heller ikke berøre Datatilsynet.

### 14.6.3 Konsesjonsplikten

Konsesjonsplikten etter forslagene i §§ 33 – 33b består av tre elementer som må vurderes hver for seg. Når det gjelder Datatilsynets kompetanse til selv å pålegge konsesjonsplikt (§ 33), er terskelen senket i forhold til dagens regulering i § 33 annet ledd, ved at "åpenbart" ikke inngår i vilkåret for ileggelse av konsesjonsplikt. Slik bestemmelsen nå står, har Datatilsynet derfor en meget stor grad av frihet mht. den arbeidsbelastning de skal påta seg, jf. "kan … bestemme". Dette forslaget må derfor anses å være uproblematisk ift. administrative og økonomiske konsekvenser.

Konsesjonsbehandling etter krav fra berørte personer (§ 33a) innebærer at initiativet til konsesjonssaker i utgangspunktet er flyttet utenfor Datatilsynets og lovgivers kontroll, og lagt i hendene på registrerte personer. Kombinasjonen med varslingsplikten i § 31 annet ledd er ment å stimulere til lokal meningsutveksling og enighet mellom behandlingsansvarlige og berørte registrerte personer. Tidsfrister og krav til fremgangsmåter i § 33a innebærer dessuten krav som trolig vil gi klare begrensninger i hvilke konsesjonskrav som vil fremkomme. I tillegg har vi foreslått kompetanse for Datatilsynet til å justere krav til antall personer bak konsesjonskrav mv., se § 33a siste ledd. Dette er gjort for å kunne styre tilstrømingen av saker i forhold til tilsynets kapasitet og prioriteringer. Innenfor Datatilsynets årlige antallsbegrensninger vil en imidlertid være bundet, og det kan tenkes å oppstå uforutsette situasjoner som medfører større antall krav om konsesjoner enn hva kapasiteten tillater. Risikoen for at dette skal skje, er imidlertid neppe stor. Dessuten kan Datatilsynet tilpasse seg en slik situasjon ved i en periode å igangsette færre konsesjonssaker med hjemmel i § 33.

Vi har også foreslått konsesjon i henhold til bestemmelse om forskrift, for behandling innen bestemte næringer, for bestemte formål eller for behandling som skjer på bestemte måter, se § 33b. Her må de administrative og økonomiske konsekvensene primært vurderes i sammenheng med fastsettelsen av forskriftene. Det er imidlertid et poeng at det i slike tilfeller må forutsettes at konsesjonsbehandling er enkeltvedtak som krever individuell behandling og konkret vurdering av hver sak. Derfor er det etter vår mening viktig å tydeliggjøre administrative konsekvenser mv., slik at uakseptable belastninger ikke blir håndtert ved å standardisere konsesjonsbehandlingen i stedet for å redusere på konsesjonsplikten.

## 14.7 Administrative og økonomiske forutsetninger for lovforslagene

Flere av de foreslåtte endringene forutsetter at det gjennomføres et administrativt utviklingsarbeid for å sikre at lovendringene kan bli vellykkede. Dette gjelder særlig unntaket for strengt pseudonymiserte opplysninger, ordningen med personvernombud og (helt spesielt) forslagene til nye regler vedrørende melding, varsling og konsesjon. Utviklingsarbeidet innebærer krav til gjennomgang av organisering, rutiner og – ikke minst – utvikling av IKT-systemer for å støtte/del-automatisere ulike funksjoner. Slike arbeider vil trolig overstige det Datatilsynet i dag alene kan bære i tillegg til de løpende oppgavene, og forutsetter trolig at det

settes av ekstraordinære midler som gjør det mulig å engasjere eksterne oppdragstakere mv. Det er heller ikke trolig at Datatilsynet har en organisasjon som er egnet for drift av de aktuelle IKT-systemene, og det bør derfor undersøkes i hvilken grad slike funksjoner bør settes bort til eksterne tjenesteleverandører.

Vi nevner disse administrative forutsetningene spesielt, fordi Datatilsynet etter vår mening tidligere ikke har levet opp til lovgivers intensjoner på viktige punkter. Etter personregisterloven § 4 gjaldt dette en alment tilgjengelig fortegnelse over konsesjoner som aldri ble etablert, og i dag er meldepliktsystemet og bruken av meldingene sterkt avvikende fra det som ble forutsatt da loven ble vedtatt.

Uten velfungerende informasjonssystemer som er integrert i den øvrige saksbehandlingen, vil foreslåtte ordninger kunne bli lite nyttige, og kan i verste fall fremstå som rene byråkratiske øvelser. Med tilstrekkelig satsing på system- og organisasjonsutvikling mv., kan imidlertid de samme "unyttige" ordningene bli hjørnestener i tilsynsvirksomheten. Uten vilje til administrativ satsing, vil flere virkemidler i loven ha meget begrenset virkning. På den annen side er det ikke gitt at full administrativ satsing gir de ønskede resultater. Gitt at slik satsing skjer, bør en derfor vurdere om det skal gjennomføres forskning/evaluering for å skaffe grunnlag for endret organisering og systemløsninger mv. Det kan herunder være aktuelt å vurdere forsøksvirksomhet, kombinert med begrenset virkeområde for enkelte bestemmelser. Således kan det for eksempel tenkes at bestemmelsen i § 33a om registrertes rett til å kreve konsesjonsbehandling, begrenses til arbeidstakere i en forsøksperiode. Etter forsøksperioden kan ordningen evalueres og eventuelt utvides. En slik tilnærming reduserer selvsagt risikoen for uakseptable administrative og økonomiske konsekvenser. Innen en begrenset prøveområde, er det imidlertid viktig at ordningen gjennomføres med de ressurser som er nødvendige for lovendringen skal få ønskede effekter.

## 14.8 Behov for overgangsregler

I denne utredningen har vi ikke gått inn på spørsmålet om behov for overgangsregler mv. Spørsmålet må konkret vurderes etter at en har bestemt seg for hvilke endringer som bør foreslås mv. Etter vår mening er det i denne sammenheng en viktig vurdering som gjelder administrative og økonomiske konsekvenser. Enkelte behandlingsansvarlige har nedlagt et stort arbeid for å etterleve dagens lov. Ved endring av loven, må en ta spesiell hensyn til at slike innsatser ikke får klart redusert verdi. Særlig må en sikre at ingen endring vil innebære at utført arbeid med internkontroll og informasjonssikkerhet helt eller delvis må gjøres på nytt. Vi har ikke foreslått endringer i disse bestemmelsene, men det er foreslått endringer av andre bestemmelser som får betydning for de vurderinger som må gjøres av internkontroll og informasjonssikkerhet. Det kan derfor være grunn til å vurdere overgangsregler som sikrer at behandlingsansvarlige som allerede har gjennomført vurderingene ikke må fornye disse før etter et visst antall år har gått.

# Litteratur og kilder

## Bøker, artikler mv.


Andersen 1989: E.S. Andersen, *Systemutvikling* (Bærum: NKI Forlaget, 1989).

Artikkel 29 arbeidsgruppen 1997: Artikkel 29 arbeidsgruppen, "Recommendation 1/97: Data protection law and the media", XV/5012/97-EN, WP1 (25.2.1997), <http://europa.eu.int-/comm/justice_home/fsj/privacy/docs/wpdocs/1997/wp1_en.pdf>.

Artikkel 29 arbeidsgruppen 1998: Artikkel 29 arbeidsgruppen, "Working document on transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection Directive", DG XV D/5025/98/EN/final, WP12 (24.7.1998), <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf>.

Artikkel 29 arbeidsgruppen 2002: Artikkel 29 arbeidsgruppen, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites", 5035/01/EN/final, WP56 (30.5.2002), <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf>.

Berg m.fl. 2005: H. Berg, F.O. Refsdal og L. Holmen, *Datatilsynets bruk av IKT – en analyse i forhold til mål og rammeverk for e-forvaltning*, Bachelor-oppgave, DRI 3001 prosjektarbeid (Avdeling for forvaltningsinformatikk, Universitetet i Oslo, 2005).

Beyleveld m.fl. 2004: D. Beyleveld, D. Townsend, S. Rouillé-Mirza og J. Wright (red.), *The Data Protection Directive and Medical Research Across Europe* (Aldershot: Ashgate, 2004).

Bing 1988: J. Bing, "En bakgrunn for analyse av informasjonsrettslige bestemmelser", *Jussens Venner*, 1988, hefte 4/5, s. 109–121.

Bing 1999: J. Bing, "Data protection, jurisdiction and the choice of law", *Privacy Law & Policy Reporter*, 1999, bind 6, s. 92–98.

Bing 2001: J. Bing, "The identification of applicable law and liability with regard to the use of protected material in the digital context", i I. Walden og J. Hörnle (red.), *E-commerce Law and Practice in Europe* (Cambridge: Woodhead Publishing, 2001) del 9 kapittel 2.

Blume 2000: P. Blume, *Personoplysningsloven* (København: Akademisk Forlag, 2000).

Blume 2006: P. Blume, *Retlig regulering af internationale persondataoverførsler* (København: Jurist- og Økonomforbundets forlag, 2006).

British Institute of International and Comparative Law 2003: British Institute of International and Comparative Law, *The implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, rapport for EU-kommisjonen (16.5.2003), tilgjengelig ved <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/biiclstudy-soundimage_en.pdf>.

Bygrave 2000: L.A. Bygrave, ”Determining Applicable Law Pursuant to European Data Protection Legislation”, *Computer Law & Security Report*, 2000, bind 16, s. 252–257.

Bygrave 2002: L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague / London / Boston: Kluwer Law International, 2002).

CNIL 2006: Commission Nationale de l’Informatique et des Libertés, ”Transferts de données à caractère personnel vers des pays non membres de l’Union européenne” (januar 2006), <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf>.

Copenhagen Economics 2005: Copenhagen Economics, *The Economic Importance of the Country of Origin Principle in the Proposed Services Directive*, rapport for UK Department of Trade and Industry (17.11.2005), tilgjengelig ved <http://www.copenhageneconomics.-com/publications/Country_of_origin_principle.pdf>.

Dahlbom og Mathiassen 1993: B. Dahlbom og L. Mathiassen, *Computers in Context: The Philosophy and Practice of Systems Design* (Cambridge, Mass.,: NCC Blackwell, 1993).

Dammann og Simitis 1997: U. Dammann og S. Simitis, *EG-Datenschutzrichtlinie* (Baden-Baden: Nomos Verlagsgesellschaft, 1997).

Danielson m.fl. 2005: J. Danielson, A-K. Groven, T. Kristoffersen, H.J. Rivertz og A Skomedal, *Elektroniske spor*, Rapport nr. 1008 (Oslo: Norsk regnesentral, 2005).

Datainspektionen 2002a: Datainspektionen, ”Registrering av personuppgifter från barn”, Samrådsyttrandan desember 2002, tilgjengelig ved <http://www.datainspektionen.se/puo/samrad/personuppgifter_barn.shtml>.

Datainspektionen 2002b: Datainspektionen, ”Behandling av elevers personuppgifter i grundskolan”, Rapport 2002:2, tilgjengelig ved <http://www.datainspektionen.se/pdf/rapporter/skolrapport.pdf>.

Datainspektionen 2003: Datainspektionen, ”Samtycke enligt personuppgiftslagen” (januar 2003), tilgjengelig ved <http://www.datainspektionen.se/pdf/skrifter/nr11.pdf>.

Djønne m.fl. 1987: E. Djønne; T. Grønn og T. Hafli, *Personregisterloven med kommentarer* (Oslo: TANO, 1987).

Eggen 1999: K. Eggen, ”Norges internasjonale forpliktelser på ytringsfrihetens område”, særskilt vedlegg nr. 1 (del II) til NOU 1999: 27.

Eggen 2002: K. Eggen, *Ytringsfrihet* (Oslo: Cappelen Akademisk Forlag, 2002).

Engelschiøn m.fl. 2002: S. Engelschiøn, C. Lie Ulrichsen og B. Nilsen, *Helseregisterloven. Kommentarutgave* (Oslo: Universitetsforlaget, 2002).

Eurobarometer 2003: Flash Eurobarometer No. 147, ”Data Protection in the European Union” (desember 2003), tilgjengelig ved <http://europa.eu.int/comm/public_opinion-/flash/fl147_data_protect.pdf>.

EU-kommisjonen 2003: EU-kommisjonen, *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, Brussel (15.5.2003), tilgjengelig ved <http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf>.

Haug 2004: A.V. Haug, *Innsyn for ungdom med IKT: Erfaringer med et pedagogisk opplegg omkring personvern og IKT for ungdomsskolen*, Forvaltningsinformatisk notatserie 2004 nr. 4 (Avdeling for forvaltningsinformatikk, Universitetet i Oslo, 2004).

Haug Aronsen 2002: K.E. Haug Aronsen, *Personopplysningsloven § 7. En analyse av forholdet mellom personvern og ytringsfrihet slik det er uttrykt i personopplysningsloven § 7*, CompLex 11/02 (Oslo: Institutt for rettsinformatikk i samarbeid med Unipub, 2002).

Hörnle 2005: J. Hörnle, "Country of Origin Regulation in Cross-Border Media: One Step Beyond the Freedom to Provide Services?", *International & Comparative Law Quarterly*, 2005, bind 54, s. 89–126.

Jarbekk 1996: E.I.E. Jarbekk, *Personvern og overføring av personopplysninger til utlandet*, CompLex 4/96 (Oslo: Tano, 1996).

Jordahl 1996: T. Jordahl, *Fotorett i mediene* (Oslo: Juristforbundets forlag, 1996).

Korff 2002: D. Korff, *EC Study on Implementation of Data Protection Directive – Comparative summary of national laws*, rapport for EU-kommisjonen (september 2002), tilgjengelig ved <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport-/consultation/univessex-comparativestudy_en.pdf>.

Kuner 2003: C. Kuner, *European Data Privacy Law and Online Business* (Oxford: Oxford University Press, 2003).

Mæland 1998: H.J. Mæland i A. Bratholm og M. Matningsdal (red.), *Straffeloven med kommentarer – Tredje del: Forseelser* (Oslo: Universitetsforlaget, 1998).

Nielsen og Waaben 2001: K.K. Nielsen og H. Waaben, *Lov om behandling af personoplysninger – med kommentarer* (København: Jurist- og Økonomforbundets Forlag, 2001).

Olsen og Mahler 2005: Thomas Olsen og Tobias Mahler, *Privacy – Identity Management. Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems* (D11 Report on Privacy – Identity Management, Legal IST Project, 2005).

Ravlum 2005a: Inger-Anne Ravlum, *Setter vår lit til Storebror … og alle småbrødrene med? Befolkningens holdning til og kunnskap om personvern*, Rapport 789/2005 (Oslo: Transportøkonomisk institutt, 2005).

Ravlum 2005b: Inger-Anne Ravlum, *Behandling av personopplysninger i norske virksomheter. En spørreundersøkelse om personvern og personopplysningsloven*, Rapport 800/2005 (Oslo: Transportøkonomisk institutt, 2005).

Selmer 1995: K.S. Selmer, "Hva er «data»?", *Lov og Rett*, 1995, s. 149–150.

Statistisk sentralbyrå v/ Gulløy 1997: Statistisk sentralbyrå ved E. Gulløy, *Undersøkelse om personvern: Holdninger og erfaringer 1997*, Notat 97/48 (Oslo: Statistisk sentralbyrå, 1997).

Teknologirådet 2005: Teknologirådet, *Elektroniske spor og personvern*, Rapport 1/2005 (Oslo: Teknologirådet, 2005).

Thaulow 2003: J.C. Thaulow, *Etableringslandsprinsippet: En analyse av E-handelsdirektivet art 3 og prinsippet om fri bevegelighet av tjenester ved elektronisk handel*, CompLex 3/03 (Oslo: Institutt for rettsinformatikk / Unipub, 2003).

Tokvam 1995: O. Tokvam, *Personvern og straffeansvar – straffelovens § 390*, CompLex 4/95 (Oslo: Tano, 1995).

Wiik Johansen m.fl. 2001: M. Wiik Johansen, K-B. Kaspersen og Å.M. Bergseng Skullerud, *Personopplysningsloven. Kommentarutgave* (Oslo: Universitetsforlaget, 2001).

Öman og Lindblom 2001: S. Öman og H.-O. Lindblom, *Personuppgiftslagen: En kommentar* (Stockholm: Norstedts Juridik, 2001).

## Forarbeider, innstillinger mv.

NOU 1997: 19, *Et bedre personvern – forslag til lov om behandling av personopplysninger*.

NOU 1999: 27, *"Ytringsfrihed bør finde Sted". Forslag til ny Grunnlov § 100*.

NOU 2001: 19, *Om biobanker*.

NOU 2003: 21, *Kriminalitetsbekjempelse og personvern – politiets og påtalemyndighetens behandling av opplysninger*.

NOU 2005: 1, *God forskning – bedre helse*.

Innst. O. nr. 51 (1999–2000), *Om lov om behandling av personopplysninger (personopplysningsloven)*.

Ot.prp. nr. 92 (1998–99), *Om lov om behandling av personopplysninger (personopplysningsloven)*.

Utgitt av :
Justis- og politidepartementet
www.jd.dep.no

Oppgi publikasjonskode: G-390

Trykk:
Departementenes servicesenter 05/09 - 200