



DET KONGELIGE ARBEIDS-  
OG ADMINISTRASJONSDEPARTEMENT

# St.meld. nr. 43

(2003–2004)

---

Datatilsynets og Personvernemndas  
årsmeldinger for 2003



# Innhold

<b>1 Innledning</b> .....	5	<b>4 Administrasjon og ressurser</b> .....	11
<b>2 Arbeids- og administrasjons- departementets merknader til Datatilsynets årsmelding for 2003</b> .....	8	<b>Vedlegg</b>	
		1 Datatilsynets årsmelding for 2003 .....	12
		2 Personvernemndas årsmelding for 2003 .	45
<b>3 Arbeids- og administrasjons- departementets merknader til Personvernemndas årsmelding for 2003</b> .....	10		





DET KONGELIGE ARBEIDS-  
OG ADMINISTRASJONSDEPARTEMENT

# St.meld. nr. 43

## (2003–2004)

### Datatilsynets og Personvernemndas årsmeldinger for 2003

*Tilråding fra Arbeids- og administrasjonsdepartementet av 11. juni 2004,  
godkjent i statsråd samme dag.  
(Regjeringen Bondevik II)*

## 1 Innledning

*Hva betyr personvern for deg?* Den enkeltes vurdering vil blant annet avhenge av egne erfaringer og opplevelser, påvirkninger utenfra, hvor komplisert det er å ivareta personvernet i det enkelte tilfellet og ikke minst av den enkeltes kunnskaper og bevissthet om personvern – eller mangelen på slike. Teknologirådet publiserte i februar 2004 rapporten *Holdninger til personvern – Rapport fra fokusgrupper om elektroniske spor og personvern*. En interessant observasjon var at de fleste unge deltakerne oppfattet personvern som noe viktig, *uten å være helt sikre på hvorfor*.

#### *Personvernet i endring*

Både verdisyn og teknologi er i stadig endring. Samfunnsutviklingen har ført til at vi er blitt avhengige av elektroniske tjenester. Hensyn til kostnads-effektivisering og ønsket om nye og mer individuelt tilpassede tjenester fører til stadig større press mot mer omfattende bruk av slike tjenester. Vektleggingen av personvern i forhold til ulike andre samfunns-hensyn må vurderes fra sak til sak, og hva som er viktig for den eldre garde, er ikke nødvendigvis like viktig for yngre mennesker. Personvern-hensyn kan, avhengig av situasjonen, trekke i sam-

*me* eller *motsatt* retning ved vurdering av for eksempel kriminalitetsbekjempelse, effektivisering, en åpnere forvaltning eller den enkeltes ytringsfrihet. Ulike personer vil ha ulik oppfatning av hva som i hvert enkelt tilfelle anses som det viktigste hensynet. Det er derfor svært viktig at vi har en levende personverndebatt i Norge – med Datatilsynet som en sentral premissleverandør og deltaker.

Et aktuelt eksempel på endring i verdisyn er flytting av grensen for frivillig meddelelse av egne personlige opplysninger. Deltakelse i realityprogram og registrering av handlevaner for å oppnå bonuspoeng er velkjent. Nylig lanserte et selskap en gratis e-posttjeneste der annonser blir plassert inn i e-post basert på innholdet i denne. Dette forutsetter gjennom søking av all e-post. Flere kritikere har uttrykt bekymring over hva gjennom søking av konfidensiell e-post kan bety for personvernet. Men som Teknologirådets undersøkelse viser, innser mange markedsverdien av egne personopplysninger. Egne personopplysninger er i større og større grad blitt en salgsvare.

Personopplysningsloven pålegger *behandlingsansvarlige* plikter i forbindelse med bruk av personopplysninger. Tradisjonelt har det vært slik at *behandlingsansvarlige* i hovedsak har vært offentlige

og private virksomheter, mens enkeltpersoners bruk av opplysninger i hovedsak har vært unntatt på bakgrunn av unntaksbestemmelsen for private formål. Enkeltpersoners forhold til loven har derfor først og fremst vært knyttet til retten til å være i fred, og kravet om at opplysningene som behandles er korrekte. Grensene er imidlertid i ferd med å flyttes. Interessant i denne sammenheng er en relativt ny forhåndsuttalelse fra EF-domstolen om at en hjemmeside ikke kan sies å være privat dersom den ligger tilgjengelig for alle på Internett. Når den ikke kan anses som privat, vil den være underlagt den ordinære personvernlovgivningen. Den eksplosive bruken av kameramobiler, med påfølgende utlegging av bilder på nettet, aktualiserer personopplysningslovens krav særlig overfor de unge. Det er en utfordring både for offentlige og private virksomheter å informere bedre om den enkeltes plikter ved bruk av personopplysninger, konsekvensene av ulik bruk av personopplysninger og den enkeltes muligheter for å beskytte seg mot uønsket bruk av slike opplysninger.

Datatilsynet hadde i 2003 blant annet fokus på kommunesektoren. Som Datatilsynet viser til har den teknologiske utviklingen og satsing på service og tilgjengelighet, kombinert med krav til effektivisering, gjort at det i mange kommuner foregår et betydelig utviklingsarbeid som stiller store krav til avklaring av ansvarsforhold og dokumentasjon av informasjonssikkerhet. Det vises for eksempel til tiltak som selvbetjeningsløsninger via Internett, herunder utlegging av journaler og dokumenter, samlokalisering av etater samt etablering av offentlige servicekontorer og regionale samarbeidsløsninger. En frivillig overgang til flere og bedre elektroniske tjenester, krever imidlertid at innbyggerne kan stole på at det er trygt å bruke disse tjenestene. Dette krever igjen at personvernet ivaretas ved at personopplysningene ikke misbrukes. Arbeids- og administrasjonsdepartementet ser derfor positivt på at flere kommuner har gått sammen og etablert *Foreningen kommunal informasjonssikkerhet* ([www.kins.no](http://www.kins.no)).

#### *Bedre offentlige tjenester og hensynet til personvern*

I fjorårets stortingsmelding skrev Arbeids- og administrasjonsdepartementet at det – som både effektiviserings- og personverndepartement – ville sørge for at personvern stod sentralt i gjennomføringen av *Strategi for IKT i offentlig sektor 2003–2005*. Et viktig krav er at personopplysninger skal være korrekte. Departementet har derfor igangsatt et arbeid som blant annet omfatter kvalitet på og tilgjengelig-

het til nøkkelinformasjon som brukes mye både i offentlig sektor og i næringslivet.

Videre omtalte departementet arbeidet med samordningen av Aetat, trygdeetaten og sosialtjenesten (SATS). Det ble i 2003 satt ned en egen arbeidsgruppe som hadde som mandat å utrede spørsmål knyttet til sikring av taushetsplikt og personvern ved samarbeid og samlokalisering i første linjen. Arbeidsgruppen har levert rapporten «Samarbeid og informasjonsutveksling mellom Aetat, trygdeetaten og sosialtjenesten – rettslige muligheter og begrensninger.» Rapporten kan leses på [www.samordning.dep.no](http://www.samordning.dep.no). Rapporten synliggjør at det innenfor dagens regelverk er muligheter for utvidet samhandling. I det videre arbeidet legges det opp til forsøk med enhetsforvaltning basert på anbefalingene i rapporten. Arbeidsgruppen skriver imidlertid at en framtidig reorganisering av velferdsforvaltningen krever en revisjon av lovgivningen, slik at oppgaver og virkemidler som faglig sett hører sammen samles i felles formål.

#### *Bevisstgjøring av ansvaret etter personopplysningsloven – oppnevning av personvernombud*

Ved ikrafttreddelsen av personopplysningsloven i 2001 rettet Datatilsynet oppmerksomheten fra forhåndskontroll (konsesjoner) til etterkontroll (tilsyn) og informasjon. Tanken var blant annet at omleggingen skulle ansvarliggjøre brukerne av personopplysninger i større grad. Loven pålegger derfor de behandlingsansvarlige relativt omfattende plikter.

Personopplysningsloven åpner imidlertid for å lette noe på pliktene etter loven for virksomheter som setter særlig fokus på personvern. Virksomheter som oppnevner personvernombud, får unntak fra meldeplikt etter personopplysningsloven. Tilsvarende muligheter til å opprette personvernombud er gitt på helseområdet, og foreslås også innført i den nye politiregisterloven, jf. NOU 2003: 21. Bruken av personvernombud er med på å flytte noe av ansvaret for oppfølgingen av personvernarbeidet fra Datatilsynet og ut til de involverte virksomhetene. Oppnevningen bidrar til større bevisstgjøring av brukerne av personopplysninger, og er med på å gi virksomheten en positiv personvernprofil. I Sverige var det pr. 31. mars 2004 oppnevnt 3 200 personvernombud for til sammen 5 406 virksomheter. På samme tidspunkt var det oppnevnt bare fem personvernombud i Norge. Dette til tross for Datatilsynets fokus på dette. Erfaringen med de oppnevnte ombudene er stort sett positive, og Arbeids- og administrasjonsdepartementet mener derfor det er

grunn til å vurdere ytterligere insentiver for å få oppnevnt flere slike ombud.

*Desentralisering av myndighet etter personopplysningsloven*

Arbeids- og administrasjonsdepartementet ønsker tiltak som bidrar til å styrke private og offentlige virksomheters fokus, og dermed etterlevelse av personvernregelverket. For å styrke både personvernet og lokaldemokratiet har det kommet initiativ til å overføre tilsyn og kontroll med kameraovervåking fra Datatilsynet til kommunene. Ved å gi kommunene en viss frihet til å avgjøre om, hvordan og i hvilken utstrekning overvåkingskameraer bør tillates på gater og torv, vil kommunene bevisstgjøres til en helhetstenking rundt personvernspørsmål. Arbeids- og administrasjonsdepartementet mener dette kan gi mange positive effekter, både i forhold til personvern og lokalt engasjement. Spørsmålet

om en eventuell overføring av myndighet og ansvar vil bli vurdert nærmere av de involverte partene.

*Datatilsynets 25-årsjubileum i 2005 (Personvernåret 2005)*

Datatilsynet ble opprettet med virkning fra 1. januar 1980 og feirer sitt 25-årsjubileum i 2005. Stortinget ba ved behandling av personopplysningsloven som trådte i kraft i 2001, om en etterkontroll av loven etter fire års virketid. Begge disse begivenhetene i 2005 gir grunnlag for å sette ekstra fokus på personvern dette året. Arbeids- og administrasjonsdepartementet håper at jubileumsåret kan benyttes som anledning til skape ekstra bevissthet rundt personvernspørsmål gjennom blant annet økt mediaoppmærksomhet og økt debatt. Arbeids- og administrasjonsdepartementet oppfordrer *alle* til å ha personvern sentralt på dagsordenen.

## 2 Arbeids- og administrasjonsdepartementets merknader til Datatilsynets årsmelding for 2003

### *Datatilsynets arbeidsområde*

Datatilsynets hovedoppgave er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Datatilsynet er tilsynsmyndighet etter personopplysningsloven og helseregisterloven. I NOU 2003: 21 *Kriminalitetsbekjempelse og personvern* foreslås det at Datatilsynet i en viss utstrekning også skal være tilsynsmyndighet etter denne loven. I NOU 2004: 5 Arbeidslivslovutvalget: «Et arbeidsliv for trygghet, inkludering og vekst», foreslås det imidlertid at Arbeidstilsynet skal være tilsynsmyndighet etter loven, også for de foreslåtte bestemmelsene om personvern i arbeidslivet. Arbeids- og administrasjonsdepartementet mener generelt at det er mest hensiktsmessig at hovedansvaret for tilsyn med personvernarbeid er samlet hos Datatilsynet.

### *Datatilsynets overordnede prioriteringer*

Datatilsynet fokuserte i 2003 spesielt på helsesektoren, kommunesektoren og arbeidslivssektoren. Ved valg at innsatsområder har Datatilsynet bl.a. vurdert mengde og type personopplysninger som behandles, antall klager på området og henvendelser fra publikum og media. Den samlede bruken av ressurser og virkemidler som Datatilsynet benytter, tilsyn sammen med bl.a. bransjekontakt, råd og veiledning, samt å skape medieoppmerksomhet, gir etter Arbeids- og administrasjonsdepartementets syn en hensiktsmessig arbeidsform.

### *Oppfølging av regelverket*

Datatilsynet gjennomførte 79 operative tilsyn i 2003. Dessverre ble det også dette året avdekket at mange virksomheter har liten kunnskap om personvernregelverket og de prinsippene dette bygger på. Datatilsynet avdekket særlig uryddighet i forhold til ansvar og myndighet, samt brudd på bestemmelsene om internkontroll og informasjonssikkerhet. Personopplysningsloven og -forskriften gir detaljerte bestemmelser om hvem som er ansvarlige for behandlingen av personopplysninger – og hva dette nærmere innebærer. Arbeids- og administrasjonsdepartementet anser de avdekkede avvikene som svært uheldige i og med at de nevnte

kravene til ryddighet i ansvarsforhold, samt en tilfredsstillende internkontroll og informasjonssikkerhet, skal være med på å sikre en forsvarlig behandling av personopplysninger. Arbeids- og administrasjonsdepartementet har merket seg at enkelte av tilsynsobjektene anser at regelverket kan være vanskelig å etterleve. Departementet mener det er viktig at både regelverk og annen oppfølging vurderes kontinuerlig for å lette etterlevelsen.

Arbeids- og administrasjonsdepartementet kan med tilfredshet registrere at etterlevelsen av meldepikten har bedret seg. Også her har imidlertid virksomhetene et betydelig forbedringspotensial. Det er viktig at alle virksomheter, både i offentlig og privat sektor, setter seg inn i egne plikter etter personopplysningsloven og helseregisterloven.

### *Nytt regelverk mv.*

I fjorårets stortingsmelding påpekte Arbeids- og administrasjonsdepartementet viktigheten av at personvern hensyn blir vektlagt tidlig i prosesser vedrørende nytt regelverk og nye samfunnstiltak, jf. utredningsinstruksens krav. Datatilsynet deltok også i 2003 i en rekke arbeidsgrupper og utvalg, og hadde derfor direkte mulighet for å bidra til at personvernkonskvenser ble grundig utredet. Arbeids- og administrasjonsdepartementet anser det som viktig at Datatilsynet på denne måten får mulighet til å påvirke utredningsarbeid på et tidlig tidspunkt.

Der Datatilsynet ikke deltar direkte i et utredningsarbeid, er det særlig viktig at utrederne på egne tiltak vurderer personvernkonskvenser. Arbeids- og administrasjonsdepartementet har igangsatt et prosjekt for generelt å bedre kvaliteten på utredningsarbeid, herunder hvordan en kan forbedre planleggingen av utredningsarbeid for å unngå for korte høringsfrister.

### *Delegering av forskriftkompetanse*

Arbeids- og administrasjonsdepartementet delegerer myndighet etter personopplysningsforskriften til Datatilsynet med virkning fra 1. januar 2004. Den delegerede myndigheten omfatter de fleste av bestemmelsene i personopplysningsforskriften med unntak av bestemmelser om personopplysningslo-



vens virkeområde, Personvernemnda, straff og lovens sluttbestemmelser. Hensikten med delegeringen er bl.a. å gjøre det lettere for Datatilsynet å vurdere bruk av forskrift kontra bruk av konsesjoner for ulike bransjeområder. Selv om antall konsesjoner har gått betydelig ned ved innføring av personopplysningsloven, mener både Arbeids- og administrasjonsdepartementet og Datatilsynet at antall konsesjoner fortsatt er for høyt.

#### *Personopplysninger i barnevernet*

Personopplysninger skal ikke oppbevares lengre enn det som er nødvendig. Barnevernstjenesten har som oppgave å avdekke om barn lever under forhold som kan gi grunnlag for tiltak i henhold til barnevernloven. For å kunne utføre sine lovpålagte oppgaver på en forsvarlig måte, er barnevernstjenesten avhengig av opplysninger om barn som kommer i kontakt med barnevernet. Formålet med opplysningene som ligger i en bekymringsmelding, tilsier at det er nødvendig å oppbevare meldingen i noe tid etter at denne er henlagt. I brev til Datatilsynet datert 6. juli 1993 var Barne- og familiedepartementet derfor av den oppfatning at bekymringsmeldinger som ikke blir fulgt opp med en undersøkelse, bør oppbevares i ett år før makulering. Barne- og familiedepartementet er i ferd med å utarbeide et rundskriv om taushetsplikt. Rutiner for oppbevaring og sletting av personopplysninger vil også bli behandlet i rundskrivet. Rundskrivet skal etter planen være ferdig i løpet av 2004.

#### *Internasjonalt arbeid*

Personvernarbeidet blir stadig mer internasjonalt. Dette skyldes ikke bare at problemstillingene stort

sett vil være like fra land til land – men også stadig voksende muligheter for flyt av personopplysninger over landegrensene. Arbeids- og administrasjonsdepartementet anser det som banebrytende at det i 2003 ble opprettet et eget ombud for personvern i EU-kommisjonen.

Europakommisjonen gjennomførte i 2003 en omfattende undersøkelse i alle EU-landene om folks syn på personvern og informasjonssikkerhet. Resultatene viser store forskjeller mellom landene. De nordiske landene scorer jevnt over høyt når det gjelder tillit til at offentlige og private virksomheter ikke misbruker de registrerte personopplysningene. Videre ligger de nordiske landene over gjennomsnittet når det gjelder tillit til at arbeidsgivere behandler personopplysninger akseptabelt. Mindre oppløftende er imidlertid tallene vedrørende kjennskap til personvernlovverket og håndhevingen av dette. Her er tallene generelt lave i alle EU-landene. For mer informasjon om undersøkelsen og resultatene, se Datatilsynets hjemmesider på [www.datatilsynet.no](http://www.datatilsynet.no).

#### *Klager behandlet av Arbeids- og administrasjonsdepartementet*

Ordinære klager etter personopplysningsloven og helseregisterloven skal behandles av Personvernemnda. Arbeids- og administrasjonsdepartementet behandler imidlertid klager av administrativ karakter som faller utenfor Personvernemndas området. I 2003 behandlet Arbeids- og administrasjonsdepartementet én klagesak. Datatilsynets vurdering om avvisning ble opprettholdt fordi det påklagede forholdet lå utenfor Datatilsynets kompetanseområde.

### **3 Arbeids- og administrasjonsdepartementets merknader til Personvernemndas årsmelding for 2003**

Personvernemnda skal avgjøre klager over Datatilsynets avgjørelser. Nemnda kan også ta opp saker av eget tiltak.

Nemnda viser i sin årsmelding til at enkelte av sakene fra 2003 er av prinsipiell karakter. På denne måten får nemnda en rettsskapende funksjonen ved utvikling av personvernregelverket.

Personvernemndas medlemmer er oppnevnt for fire år av gangen, med adgang til forlengelse i ytterligere fire år. Første oppnevning skjedde med virkning fra 2001. Det betyr at det i 2004 må oppnevnes medlemmer med virkning fra 2005. Leder og nestleder med vararepresentanter oppnevnes av Stortinget, mens de frem øvrige medlemmene med varamedlemmer oppnevnes av regjeringen.

## 4 Administrasjon og ressurser

Arbeidsmengden til både Datatilsynet og Personvernemnda stabiliserte seg i 2003 i forhold til 2002 da overgangsordningene til personopplysningsloven og helseregisterloven gikk ut. Personvernemnda behandlet åtte klagesaker i 2003, samme antall som i 2002.

Som følge av blant annet den teknologiske utviklingen blir imidlertid personvernspørsmålene i seg selv stadig mer komplekse. For Datatilsynet har særlig konsesjonssøknader knyttet til helse og forskning vist seg arbeidskrevende. Dette betyr at Datatilsynet må allokere stadig mer ressurser til disse områdene.

Videre blir personvernlovverket stadig mer fragmentert. Arbeids- og administrasjonsdepartementet viser her bl.a. til NOU 2003: 21 *Kriminalitetsbekjempelse og personvern* hvor det foreslås egne personvernbestemmelser innenfor politiets arbeidsfelt. Fragmentering av personvernlovgivnin-

gen får betydning for Datatilsynet fordi de i større grad må spesialisere kompetansen. På lengre sikt kan dette også få konsekvenser for Personvernemnda, som i større grad kan få behov for å innhente eksterne vurderinger. Arbeids- og administrasjonsdepartementet vil følge nøye med i utviklingen og vurdere om både Datatilsynet og Personvernemnda har tilstrekkelige ressurser.

Arbeids- og administrasjonsdepartementet

t i l r å r :

Tilråding fra Arbeids- og administrasjonsdepartementet av 11. juni 2004 om Datatilsynets og Personvernemndas årsmeldinger for 2003 blir sendt Stortinget.

---

## Vedlegg 1

# Datatilsynets årsmelding for 2003

## 1 Om Datatilsynet

---

Datatilsynet har siden opprettelsen i 1980 hatt til oppgave å beskytte den enkelte mot at personvernninteressene krenkes gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvernhen-syn som behovet for vern av personlig integritet og privatlivets fred. Det juridiske grunnlaget for Data-tilsynets virksomhet er regulert i Lov om behan-dling av personopplysninger av 14. april 2000 (perso-nopplysningsloven) og Lov om helseregistre og be-handling av helseopplysninger (helseregisterlo-ven) av 18. mai 2001.

Datatilsynet er et uavhengig forvaltningsorgan, administrativt underordnet Kongen v/Arbeids- og administrasjonsdepartementet. Datatilsynets uavhengighet innebærer at departementet ikke kan gi instruks om, eller omgjøre, Datatilsynets utøving av myndighet etter personopplysnings- eller helsere-gisterloven. Som klageinstans i forhold til Datatilsy-nets vedtak er det opprettet en Personvernemnd. Personvernemnda utgir sin egen årsmelding.

Personopplysningsloven legger opp til at det i første rekke er opp til hver enkelt å ivareta sitt eget personvern. I tillegg har de som behandler perso-nopplysninger fått et større ansvar enn de hadde et-ter den gamle personregisterloven. Som en følge av dette er Datatilsynets oppgaver i stor grad gått fra forhåndsgodkjenning til etterkontroll.

### *Datatilsynets oppgaver*

Datatilsynet skal holde seg orientert og informere om den nasjonale og internasjonale utviklingen i behandlingen av personopplysninger, og om de problemene som knytter seg til slik behandling. Datatilsynet skal identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begren-ses. Deltakelse i råd og utvalg er derfor en viktig del av Datatilsynets arbeid. Også som høringsin-stans i saker som kan ha en personvernmessig kon-sekvens har Datatilsynet innflytelse på samfunnsut-viklingen.

Datatilsynet fører en offentlig fortegnelse over alle behandlinger av personopplysninger som er

meldt inn. Videre behandler Datatilsynet søknader om konsesjon, der dette kreves etter loven.

Gjennom aktivt tilsyn og saksbehandling kon-trollerer Datatilsynet at lover og forskrifter for be-handling av personopplysninger blir fulgt, og at feil og mangler blir rettet. Datatilsynet bistår bransjeor-ganisasjoner med å utarbeide bransjevise adferds-normer, og gir bransjer og enkeltvirksomheter råd om sikring av personopplysninger.

Sist, men ikke minst, har Datatilsynet også en viktig ombudsmannsrolle. I den forbindelse drives rådgivning og informasjon overfor enkeltpersoner som tar kontakt med tilsynet. Publikum generelt nås i første rekke gjennom aktiv mediekontakt og publisering på eget nettsted.

## 2 Rapport fra året 2003

---

### 2.1 Overordnede prioriteringer

Datatilsynet legger opp til en mest mulig samord-net bruk av ressurser og virkemidler mot utvalgte sektorer eller bransjer innen definerte perioder. Operativt tilsyn benyttes i kombinasjon med juri-disk utredning og saksbehandling, bransjekontakt, råd og veiledning, mediekontakt og annen informa-sjonsvirksomhet.

I 2003 ble innsatsen særlig fokusert mot tre om-råder:

- Helsesektoren
- Kommunesektoren
- Arbeidsliv

Disse tre områdene er valgt ut etter en vurdering av personverntuslene, blant annet mengde og type personopplysninger som behandles. Også antall klager og henvendelser fra publikum, samt saker som har vært tatt opp av media, har påvirket priori-teringene.

### Helsesektoren

Fokuset på helsesektoren er en videreføring fra 2002 fordi det her behandles mange og svært sensi-tive personopplysninger. Samtidig skjer det et ri-

vende teknologisk utviklingsarbeid, blant annet ved etablering av nasjonale helsenett og innføring av fullelektroniske pasientjournaler. I tillegg viste de operative tilsynene i 2002 at de databehandlingsansvarlige innen helseforetakene ikke var tilstrekkelig kjent med regelverket slik det fremkommer i personopplysningsloven og helseregisterloven. Et fortsatt fokus på sektoren har derfor vært nødvendig.

### Kommunesektoren

Også i kommunesektoren behandles det betydelige mengder personopplysninger, hvorav en stor del også er sensitive. Den teknologiske utviklingen og satsingen på døgnåpen forvaltning, service og tilgjengelighet har gjort at flere kommuner har lagt sine elektroniske journaler og dokumenter ut på Internett. Mangelfulle rutiner i forhold til dette innebærer store personvernetrusler. Flere kommuner satser også på forskjellige regionale samarbeidsløsninger. Dette stiller store krav til avklaring av ansvarsforhold og en dokumentert informasjonssikkerhet.

### Arbeidsliv

Arbeidsliv er et område med et betydelig potensial for overvåking og misbruk av personopplysninger. Gjennom operative tilsyn er det avdekket en utstrakt bruk av overvåkingsteknologi. I tillegg har en stor og økende andel av telefon- og brevhenvelselsene til Datatilsynet fra publikum dreiet seg om overvåking og kontroll i arbeidslivet. I 2003 konsentrerte Datatilsynet seg særlig om kundesentrene (også kalt callsentre/telefonsentre), fordi overvåkings- og kontrollpotensialet her oppfattes som særlig stort.

## 2.2 Økonomi og administrasjon

### Budsjett

Datatilsynet hadde 18,3 millioner kroner til rådighet i 2003. De rene lønnskostnadene utgjør 67 prosent av driftsbudsjettet. Utover dette har bevilgningen dekket faste driftsutgifter og utgifter til operativ tilsynsvirksomhet, informasjonsarbeid og representasjon i internasjonale organer. I 2003 har det også vært ekstra kostnader forbundet med arkivavlevering.

Datatilsynet hadde i 2003, i motsetning til forutgående år, ikke et definert inntektskrav med tilhørende merinntektsfullmakt knyttet til egen kurs- og seminarvirksomhet. Denne virksomheten ble der-

for avviklet og halvannet årsverk fjernet fra informasjonsavdelingen.

### Organisasjon

Datatilsynet ledes av direktør Georg Apenes og er organisert i fire avdelinger, juridisk, tilsyn og sikkerhet, informasjon og administrasjon. Juridisk avdeling utgjør med sine 12 medarbeidere den største organisatoriske enheten.

Det var i virksomhetsåret 26 fast tilsatte, hvorav 16 kvinner og 10 menn. Gjennomsnittsalderen er 42 år for menn og 34 år for kvinner.

Det har i perioder vært tilsatt ekstrahjelp og vikarer for å avhjelpe arbeidssituasjonen. To engasjementsstillinger er opprettet i juridisk avdeling i forbindelse med at det er etablert en førstelinjetjeneste. Denne består av tre saksbehandlere som tar seg av innkomne telefoner og e-post i tillegg til å ta seg av enklere saksbehandling. Det er også opprettet en engasjementsstilling i tilsyns- og sikkerhetsavdelingen som har til hovedoppgave å styrke tilsynsarbeidet og bistå med IT-driftsoppgaver. Informasjonsavdelingen hadde også deler av høsten en person tilsatt i engasjement.

I løpet av virksomhetsåret har én medarbeider sluttet i Datatilsynet for å gå over til ny arbeidsgiver. Flere engasjementer og vikariater har imidlertid gått til opphør og fast tilsatte er tilbake i arbeid etter svangerskapspermisjoner.

### Avtale om inkluderende arbeidsliv

Datatilsynet ble med virkning fra september 2003 knyttet til avtalen om et inkluderende arbeidsliv. Avtalen tydeliggjør samarbeidet mellom arbeidsgiver og arbeidstaker med det mål å skape et mer inkluderende og utviklende arbeidsmiljø.

### Arkiv

Etter en tilbudsinnbydelse inngikk Datatilsynet i september en avtale med Stiftelsen ASTA om ordning av arkivmateriale fra perioden 1979 til 2000. Grunnen til at dette materialet skal ordnes etter Riksarkivets regler for avlevering, er at ny lov om behandling av personopplysninger trådte i kraft 1. januar 2001. Datatilsynet har derfor ikke behov for å oppbevare saker etter gammel lov. Materialet som skal ordnes utgjør i alt ca. 160 hyllemeter. I tillegg kommer ca. 25 hyllemeter med kopibøker som Datatilsynet har bundet inn selv. Arbeidet skal være utført innen 31. desember 2004.

### Forenklet meldesystem

Datatilsynet fører en offentlig database over alle meldinger om behandling av personopplysninger. Den ligger tilgjengelig på Datatilsynets hjemmeside. Her kan interesserte søke på virksomhetens navn eller organisasjonsnummer. På den måten kan enhver undersøke hva slags behandling av personopplysninger som er meldt inn fra ulike virksomheter, herunder også kameraovervåking. Datatilsynet har i løpet av 2003 brukt en del ressurser på å utvikle en ny og mer brukervennlig versjon av det elektroniske meldesystemet. Antallet felt som skal fylles ut er sterkt redusert. Det bør derfor nå være enda enklere for de behandlingsansvarlige å etterleve plikten til å melde fra om behandling av personopplysninger.

### 2.3 Personvernombud

I januar 2003 ble det avholdt seminar for de seks første personvernombudene opprettet iht. personopplysningsloven. Formålet med seminaret var å gi grunnleggende opplæring i personopplysningsloven og helseregisterloven, samt å skape nettverk mellom personvernombudene.

Norsk samfunnsvitenskapelig datatjeneste, NSD, er det eneste personvernombudet som representerer flere virksomheter. På det tidspunktet ordningen med personvernombud ble opprettet, hadde NSD inngått avtale med ca. 40 forskjellige høyskoler, universiteter og forskningsinstitusjoner om å være personvernombud i forhold til behandling av deres forskningsvirksomhet. I løpet av meldingsåret har antallet avtaleparter for NSD vokst til nærmere 100, herunder de fleste sykehus i landet. Ullevål universitetssykehus har imidlertid valgt å gå en annen vei, og har opprettet et eget personvernombud for hele virksomheten.

I løpet av meldingsåret er det oppnevnt ett nytt personvernombud. Dette er i markedsføringssektoren Talk2me.

Datatilsynet hadde et håp om at flere virksomheter, herunder kommuner, ville opprette personvernombud i løpet av 2003. Det vil derfor i tiden fremover settes inn mer ressurser på dette arbeidet.

### 2.4 Saksbehandling

#### Ordinær saksbehandling

7 251 brev og andre dokumenter ble journalført i 2003, hvorav 3 893 innkomne dokumenter og 3 358 utgående brev ut fra Datatilsynet. Dette er noe mindre enn i 2002 hvor det kom inn ekstraordinært

mange søknader om konsesjon på slutten av året. Dette skyldtes at overgangsordningene til både personopplysningsloven og helseregisterloven opphørte. Begge lovene gjelder nå fullt ut fra 1. januar 2003. Forskning utgjør med sine over 1 000 innkomne dokumenter den største kategorien av saker.

Det er også fortløpende blitt besvart 2 118 henvendelser kommet inn via e-post.

E-posthenvendelser som er av en slik karakter at de krever en form for saksbehandling blir journalført og behandlet som øvrige arkivverdige dokumenter. Henvendelser som kan besvares uten ytterligere saksbehandling blir besvart straks og senest innen fem dager.

Datatilsynet hadde rundt 150 saker hvor problemstillingene som ble reist i hovedsak var av teknisk karakter. Hovedvekten av henvendelsene vedrørende tekniske problemstillinger skjer primært via andre kanaler som elektronisk post, telefon og via veiledningsmøter. Datatilsynet har lagt vekt på å gi råd og veiledning til virksomheter som arbeider med å sikre personopplysninger i samsvar med regelverket. I en del saker krever dette direkte veiledning i møter, mens mindre kompliserte spørsmål kan tas via telefon eller e-post.

Det ble via elektronisk post besvart rundt 500 henvendelser knyttet til tekniske problemstillinger. Etaten gjennomførte dessuten rundt 80 veiledningsmøter knyttet til å oppnå forholdsmessig sikring av personopplysninger. Tilsvarende antall telefoner er noe vanskeligere å anslå, men det er estimert at dette lå mellom 800 og 1 000 henvendelser i 2003.

Hovedvekten av henvendelsene er knyttet til behov for avklaring og fortolkning av kravet til forholdsmessig sikkerhet, samt råd om hvordan dette kan gjennomføres i praksis. En del konsulentseksjoner, produsenter og leverandører har også ønsket dialog for å oppnå en bedre forståelse for regelverkets krav.

### Konsesjonssøknader og meldinger

I 2003 ble det gitt 470 konsesjoner. Av dette var 196 konsesjoner gitt innen kategorien helse og forskning.

Datatilsynet har i meldingsåret fokusert på arbeidet med konsesjoner for bank, forsikring, finansieringsinstitusjoner og kredittopplysningsforetak. Disse vil være ferdigstilt første halvår 2004. Det er imidlertid særlig innen helse at de ressurskrevende konsesjonsbehandlingene ligger, som for eksempel Kreftregisteret og de store helseundersøkelsene. Dette arbeidet ble innledet i 2003, med ikrafttredel-

sen av de nye helselovene. Datatilsynet har i meldingsåret også konsesjonsbehandlet en rekke blodbanker, som et resultat av et kartleggingsprosjekt startet i 2002.

I 2003 kom det inn 6 210 meldinger. Totalt er det nå 15 854 meldinger i meldingsdatabasen. Kameraovervåking utgjør med sine 22 prosent den største kategorien.

## 2.5 Lov og forskrift, høringer og utvalgsarbeid

### Personopplysningsforskriften

Forskriftene til personopplysningsloven ble endret 23. desember 2003, med ikrafttredelse fra 1. januar 2004. Her er det blant annet gitt generelle forskrifter om forholdet til EU-kommisjonens beslutninger om beskyttelsesnivå i tredjeland. Tidligere har forskriften blitt endret etter hvert som EU-kommisjonen har akseptert beskyttelsesnivået i tredjeland. Nå er forskriften utformet slik at kommisjonens beslutninger også gjelder for Norge, med mindre reservasjonsadgangen er benyttet. Dette innebærer at forskriften ikke lenger vil ha noen oversikt over hvilke tredjeland som er godtatt. Datatilsynet vil derfor heretter ajourføre en oversikt over dette på sine hjemmesider.

Elev- og studentopplysninger ved skoler og universiteter, samt opplysninger om barn i barnehager og skolefritidsordninger er etter forskriftsendringen unntatt fra både konsesjons- og meldeplikten.

### Delegert forskriftskompetanse

Høsten 2003 delegerte Arbeids- og administrasjonsdepartementet sin forskriftskompetanse til Datatilsynet, med unntak av forhold som vedrører personopplysningslovens virkeområde og Personvernemnda. Det ligger også fortsatt til departementet å utferdige forskrifter i tilknytning til straffesaksjoner.

Delegeringen har skjedd i en naturlig prosess, hvor det organ som sitter med spisskompetansen innen personvern også naturlig gis kompetanse til å gi forskrifter. Det er all grunn til å tro at forskriftene vil bli mer oppdaterte og utfyllende som en følge av dette.

### Høringssaker

I meldingsåret kom det inn 135 høringssaker. De fleste av høringssakene som ble realitetsbehandlet fra Datatilsynets side var innen ansvarsområdene til Finansdepartementet, Justisdepartementet og Kommunaldepartementet.

Særlig merket Datatilsynet seg mange høringssaker i tilknytning til utlendingslovgivningen. Av andre høringssaker hvor Datatilsynet gav viktige innspill kan nevnes:

- forslag til endring av 10-årsfristen for sletting av opplysninger i Konkursregisteret
- utkast til forskrifter for MSIS og tuberkuloseregisteret SYSVAK og NORM
- endring av forskrift om klinisk utprøving av legemidler til mennesker
- forslag til ny forskrift om registrering og merking av småbåter
- forslag til forskrift om Reseptbasert legemiddelregister – Reseptregisteret
- utkast til prinsipper for allment tilgjengelig elektronisk postjournal fra departementene og direktoratene
- utkast til forskrift om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv.
- forskrift til personopplysningsloven
- forslag til valutaregistreringsloven
- endringer i reglene om offentliggjøring av skattemister
- forslag til ny organisering for behandling av søknader om adopsjon
- ny ILO-konvensjon om sjøfolks identitetsbevis

I mange av høringssakene har Datatilsynet merket seg at personvernet er noe stemoderlig behandlet. Ofte står det ikke annet i høringnotatet enn at personvernet er vurdert. Hva som nærmere skal ha vært vurdert, og en drøfting av hvordan personvernet er veid opp mot andre interesser, er som regel fraværende. Dette er en svakhet ved gjeldende lovarbeid, og gjør at Datatilsynet ofte må legge ned unødvendig mye ressurser i høringsuttalelsene. I tre av høringsforslagene fra Kommunaldepartementet var høringsfristen dessuten satt så kort at det i praksis var umulig å avgi uttalelse. Dette finner Datatilsynet bekymringsfullt, da forslagene ved en slik fremgangsmåte ikke blir tilstrekkelig belyst.

### Klagesaker

Personvernemnda er klageinstans for klager over Datatilsynets avgjørelser i forhold til både personopplysningsloven og helseregisterloven, men ikke når det gjelder de administrative sidene ved saksbehandlingen. Nemnda har sin egen hjemmeside hvor sakene de har behandlet er nærmere presentert. Adressen til hjemmesiden er: [www.personvernemnda.no](http://www.personvernemnda.no). Personvernemnda gir ut sin egen årsmelding.

I 2003 behandlet Datatilsynet 22 klagesaker. I 10 av klagesakene har Datatilsynet helt eller delvis

omgjort sitt vedtak. Åtte klager er oversendt til behandling i Personvernemnda og fire er under behandling i Datatilsynet.

### Deltakelse i offentlige råd og utvalg

Datatilsynet har i 2003 deltatt i følgende råd og utvalg:

#### *Politiregisterutvalget*

Utvalget hadde som mandat å fornye eksisterende lov om strafferegistrering. Utvalget la i august 2003 fram sin utredning med lovtkast i NOU 2003: 21 – *Kriminalitetsbekjempelse og personvern*.

#### *Utvalg for politimetoder i forebyggende øyemed*

Utvalget skal vurdere metoder politiet kan benytte for å forebygge og avverge kriminalitet, og foreslå nærmere regler for dette.

#### *Datakrimutvalget*

Utvalget er satt ned for å se på implementeringen av cybercrime-konvensjonen, slik at Norge kan ratifisere denne.

#### *Arbeidsgruppe for elektronisk postjournal*

Arbeidsgruppen så på i hvilken form prøveprosjektet om bruk av elektronisk postjournal i departementer og direktorater eventuelt skal videreføres og gjøres tilgjengelig for allmennheten på Internett. Arbeidsgruppen la i mars 2003 fram sitt forslag.

#### *Arbeidsgruppe for revisjon av personopplysningslov og forskrift*

Personopplysningsloven skal etterkontrolleres fire år etter at den ble satt i kraft. En slik bred revisjon skal dermed finne sted i 2005. Justisdepartementet har imidlertid satt ned en arbeidsgruppe som vurderer behov for å endre loven og forskriftene på enkelte punkter forut for denne større gjennomgangen. Dette er gjort i samråd med Arbeids- og administrasjonsdepartementet og Datatilsynet.

#### *Styringsgruppe for etablering av sertifiseringsordninger*

Datatilsynet er representert i styringsgruppen for etablering av sertifiseringsordninger for IT-sikkerhet i datasystemer.

#### *Forum for IT-sikkerhet*

Datatilsynet er fast medlem i Forum for IT-sikkerhet. Forumet er opprettet av Nærings- og handelsdepartementet og skal tjene som dialogforum mellom departementene, offentlige myndigheter og næringsliv.

#### *Arbeidsgruppe for evaluering av sikkerhetslovens bestemmelser om personellsikkerhet*

Datatilsynet er representert i en arbeidsgruppe nedsatt av Forsvarsdepartementet som skal se på mulige endringer i sikkerhetslovens kapittel seks. Dette skal særlig gjøres med sikte på å gi den enkelte bedre rettssikkerhet.

#### *Vurdering av uredelighetsutvalg for forskning*

Datatilsynet er representert i en arbeidsgruppe nedsatt av Undervisnings- og forskningsdepartementet. Arbeidsgruppen skal jobbe med en mulig lovfesting av et uredelighetsutvalg for forskning, samt de forskningsetiske komiteer.

## 2.6 Internasjonalt samarbeid

Personopplysninger utveksles i stadig større grad over landegrensene. For Datatilsynet er det derfor meget viktig å samarbeide med tilsvarende organer i andre land. Internasjonale samarbeidsfora er dessuten viktige arenaer for erfaringsutveksling.

### Artikkel 29-gruppen

Den norske personopplysningsloven reflekterer alle de grunnleggende og ufravikelige personvernprinsippene som er nedfelt i EU-direktivet om personvern. Sammen med kollegaer fra de 10 søkerlandene til EU-medlemskap, har det norske Datatilsynet deltatt som observatør i arbeidsgruppen opprettet etter direktivets artikkel 29.

Artikkel 29-gruppen er først og fremst rådgivende overfor kommisjonen, og står helt fritt når det gjelder å tolke og konkretisere direktivets innhold.

Gruppen møtes i Brussel fem-seks ganger pr. år, som oftest over to dager. Gruppen arbeider ofte med utgangspunkt i dokumenter fra uformelle arbeidsgrupper, der alle medlemslandene kan være med. Uten at det foreligger noe formelt vedtak, er det i praksis akseptert at også observatørland kan tiltre disse gruppene. Ut fra den betraktning at også EØS-land vil bli bundet av de endelige vedtak, er det åpnet for å kunne påvirke gjennom deltagelse. Det samme gjelder adgangen til å tale i plenum.

Den viktigste saken i 2003 har vært behandlin-



gen av amerikanske myndigheters krav om innsyn i, og adgang til å benytte, passasjeropplysninger innsamlet og oppbevart av flyselskaper som opererer transatlantisk og/eller innenfor USA. Se egen omtale senere i årsmeldingen.

Noen andre saker fra meldingsåret:

- bruk av offentlig innsamlede personopplysninger til kommersielle eller andre private formål
- bruk av biometriske data for identifisering av personer
- vurdering av personvernregimene i flere såkalte tredjeland, dvs. land som verken er EØS- eller EU-land. Dette er gjort med tanke på å kunne føre slike land, om de kvalifiserer, opp på en «hviteliste» over land med personvernlovgivning som er vurdert til å ha et forsvarlig nivå for behandling av personopplysninger

I løpet av 2003 gjennomførte kommisjonen dessuten en omfattende vurdering av resultatet av medlemslandenes implementering av personverndirektivet. Kommisjonens konklusjon var at det i overskuelig fremtid ikke er behov for et nytt eller supplerende personverndirektiv. Arbeidet med å harmonisere praktiseringen av de nasjonale lovene vil ha fortsatt prioritet.

Artikkel 29-gruppen har hjemmeside på: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy).

### Datatilsynsjef for EU

Den 22. desember 2003 utpekte EU-parlamentet og EU-kommisjonen et egen ombud for personvern i Unionen. Prosessen har tatt svært lang tid og har tiltrukket seg svært mange kompetente interessenter.

Valget falt på sjefen for det nederlandske Datatilsynet siden 1991, Peter J. Hustinx. Etter norsk vurdering er dette meget gunstig med tanke på samarbeidet mellom EØS-landene og medlemslandene når det gjelder spørsmål om personvern.

### Internasjonalt datatilsynsmøte

Datatilsynet deltok med én representant på det 25. internasjonale datatilsynsmøtet, som i september ble avholdt i Sydney, Australia.

Temaet for årets konferanse var *Practical privacy for people, government and business*. Her drøftet representanter for 50 datatilsynsmyndigheter fra hele verden, samt representanter fra myndigheter, internasjonale virksomheter og interesseorganisasjoner, hva som utgjør et godt personvern i praksis og hvordan dette i større grad kan kommuniseres ut til publikum. Det var til sammen ca. 350 deltakere på konferansen.

I forbindelse med konferansen ble det også holdt en lukket sesjon for de ca. 50 datatilsynsmyndighetene. Her ble det vedtatt fem resolusjoner:

- om hvordan offentlige og private virksomheter kan bedre sin informasjon om hvordan personopplysninger blir behandlet. Det er utarbeidet eksempler på hvordan globale aktører kan komme fram til en entydig og lett gjenkjennbar måte å kommunisere sin personvernpolicy på.
- om overføring av passasjerdata mellom land som ledd i kampen mot terrorisme
- oppfordring til internasjonale organisasjoner om offisielt å forplikte seg til å følge internasjonalt aksepterte prinsipper for personvern og databeskyttelse
- om automatiske softwareoppdateringer
- om bruk av *Radio-frequency identification* (RFID – radiobaserte identifikasjonsmidler)

Alle fem resolusjoner, og bakgrunnen for disse, kan leses på [www.privacyconference2003.org](http://www.privacyconference2003.org).

### Berlinggruppen

Berlinggruppen er en arbeidsgruppe utledet av det internasjonale datatilsynsmøtet og arbeider i første rekke med tekniske problemstillinger knyttet til personvern innen telekommunikasjon. Norge deltok med representant på ett av årets to møter. Sentralt i drøftelsene var:

- diskusjon om personvernproblematikk knyttet til RFID
- digitale videoovervåkningssystemer, samt hvordan bruk av avansert programvare kan nyttes til å analysere slikt materiale
- WLAN – trådløse nettverk. Innføring av denne teknologien har reist utfordringer for virksomheter når det gjelder å sikre personopplysninger på en forsvarlig måte.
- video-on-demand. Dette er et konsept som synes å være på full fart inn i markedet. Lagringstid for kjøpsinformasjon er her en sentral problemstilling
- *spam* som fenomen og sett i relasjon til personvern. Det er ulike meninger landene i mellom når det gjelder spørsmålet om i hvor stor grad personvernmyndighetene bør engasjere seg i dette temaet

### Nordisk datatilsynsmøte

Nordisk datatilsynsmøte ble i 2003 holdt i Helsingfors. Av sentrale tema som ble tatt opp på møtet var personlige ID-kort, elektronisk overvåking på arbeidsplassen og konsesjonsbehandling av personopplysninger innen genforskning.

### Internasjonalt saksbehandlermøte

To saksbehandlere fra Datatilsynet deltok i 2003 på to møter i regi av det internasjonale samarbeidsforumet for saksbehandlere, complaint workshop. Møtene ble holdt i henholdsvis Warszawa og Roma, med deltakere fra 25 land.

På vårmøtet fortsatte drøftelsene fra 2002 om overføring av personopplysninger til andre land. Kredittopplysninger/svartelister og generelle saksbehandlerrutiner i de enkelte land var også sentrale punkter på møtet. I Roma ble bruk av biometriske data og klinisk utprøving drøftet.

### Nordisk saksbehandlermøte

Nordisk saksbehandlermøte ble holdt i Stockholm. Datatilsynet var representert med tre juridiske saksbehandlere. Av sentrale tema som ble tatt opp var blant annet behandling av personopplysninger på Internett og ved forskning.

### Nordisk møte innen tilsyns- og sikkerhetsfaglige spørsmål

Møtet er opprettet for å skape en god kontakt mellom de teknologiske miljøene hos personvernmyndighetene i de nordiske land. Formålet med møtene er blant annet å diskutere aktuelle tekniske problemstillinger med sikte på å komme frem til omforent håndhevelse av regelverket. Møtet holdes en gang pr. år og ble denne gang avviklet i Oslo. Blant de mest sentrale problemstillinger som ble tatt opp var:

- sikkerhetsproblemer med ansattes fjernaksess til en virksomhets mailsystemer og informasjonssystemer generelt
- virus, ormer og trojanere. Hvordan kan myndighetene gi gode råd?
- sikkerhetskopiering. Et verktøy som ofte kommer i konflikt med krav om sletting
- krav til kryptering på GSM, UMTS, GPRS
- innholdet i tekniske tilsyn – hva tilsynsmyndigheten bør legge vekt på

### OECD

Direktør Apenes holdt i oktober foredrag på konferansen *Towards a Global Culture of Security* som ble arrangert i Oslo i regi av OECD. Seminaret hadde 160 deltagere. Foredragets tittel var *Balancing security needs and democratic values*. Apenes la særlig vekt på problemer som kan oppstå når strategier og tiltak for sikkerhet, i tillegg til å bli bygget på nasjonale verdier og holdninger, også må reflektere

en sikkerhetsagenda som er under sterk innflytelse fra andre land og kulturer.

### Europol

I meldingsåret deltok Datatilsynet med en representant i et orienteringsmøte i Europol's felles tilsynsorgan JSB (Joint Supervisory Body). I tillegg deltok Datatilsynet på et todagers besøk i Europol's hovedkvarter i Haag, Nederland. Begge initiativene har vært nyttige, da Norges samarbeidsavtale med Europol ikke har gitt Datatilsynet den ønskede rollen som deltaker i JSB.

### Joint Supervisory Authority (JSA)

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengenområdet eller er straffedømt i et av medlemslandene. Årlig avholdes normalt fem møter i Brussel, og Datatilsynet er representert med en observatør. JSA har også i år arbeidet med uttalelser i forbindelse med ønsker om utvidelse av SIS. En egen arbeidsgruppe ble satt ned for å utforme et veikart i forhold til personvernutfordringer som oppstår ved foreslåtte utvidelser. Utvidelse av SIS var også tema ved en konferanse EU-parlamentet holdt i oktober. JSA har i tillegg planlagt en felles undersøkelse i de respektive Schengenland i forbindelse med registrering av utlendinger som nektes innreise. Det er Schengenkonvensjonens artikkel 96 som gir hjemmelsgrunnlag for slike registreringer. Datatilsynet har også deltatt med en representant i JSAs inspeksjonsgruppe som førte tilsyn med informasjonssikkerheten ved den sentrale databasen (CSIS) i Strasbourg.

Nasjonalt gjennomførte Datatilsynet også tilsyn mot et politidistrikt, uten at det ble avdekket vesentlige avvik fra regelverket.

### 2.7 Informasjonsvirksomheten

Dagens personvernlovgivning legger i stor grad ansvaret på den enkelte når det gjelder å ivareta sitt eget personvern. Samtidig er alle som behandler personopplysninger, enten det er offentlige etater eller næringsdrivende, pålagt vesentlige plikter i forhold til denne behandlingen. Datatilsynet er derfor avhengig av å oppnå synlighet i samfunnet og å skape en aktiv debatt og oppmerksomhet omkring sentrale personvernspørsmål. Aktiv kommunikasjonsvirksomhet er dermed et virkemiddel som vektlegges sterkt i Datatilsynet.

## Stor medieoppmerksomhet

Datatilsynets virksomhet følges med stor interesse av aviser, radio, TV, ulike nettsteder og bransjeblader. Sett i forhold til organisasjonens størrelse og administrative ressurser er Datatilsynet en meget synlig aktør i samfunnsdebatten og i mediebildet.

I 2003 kom det inn 89 bestillinger fra pressen og andre om til sammen 430 dokumenter fra den offentlige postjournalen. Det er videre registrert over halvannet tusen nyhetsinnslag på mediernes nettsider. Det reelle antallet nyhetsoppslag omkring Datatilsynet og personvernrelaterte saker antas imidlertid å være betydelig høyere enn dette, da mange nyheter kommer i trykk eller på radio/tv uten at mediene samtidig gjør dem tilgjengelig via Internett. Det er, ikke uventet, NRK og Aftenposten som har hatt flest omtaler av Datatilsynets virksomhet.

## Datatilsynets hjemmeside

På Datatilsynets egen hjemmeside, [www.datatilsynet.no](http://www.datatilsynet.no), ble det i 2003 publisert 72 egenproduserte nyhetsartikler og notiser. I tillegg er også temaside-ene ajourført. Det er utarbeidet nye veiledninger når det gjelder:

- plikten til å søke konsesjon eller sende melding om behandling av personopplysninger
- reservasjon mot direkte markedsføring
- adressemekling
- innsamling og bruk av personopplysninger via Internett. Veiledningen ble utarbeidet i samarbeid med Forbrukerombudet
- private nettsider og personopplysningsloven
- publisering av bilder på Internett

I underkant av 2 000 personer står på en abonnentliste for melding om nyhetsoppdateringer på nettstedet. Estimert antall daglig besøkende på hjemmesiden er i overkant av 700, som utgjør en økning på om lag 100 i forhold til året før.

Det ble utgitt ett nummer av det elektroniske fagtidsskriftet SPOR, som utelukkende fokuserte på temaet *barn, unge og Internett*. Bakgrunnen for dette var at Datatilsynet har vært en aktiv bidragsyter til Internettportalen Saftonline.no. Denne portalen ble våren 2003 etablert i forbindelse med et prosjekt ledet av Statens filmtilsyn som retter seg mot nettopp problemstillinger knyttet til barn og unges bruk av Internett.

SPOR er for øvrig avviklet som kommunikasjonsiltak. Datatilsynet har i stedet konsentrert innsatsen mot i større grad å ajourføre og utvikle temainformasjonen, slik at de besøkende på nettstedet finner relevant og oppdatert temainformasjon.

Målsettingen er også å etablere en helt ny hjemmeside hva angår struktur, organisering og layout, slik at nettstedet fremstår som en levende nyhetskanal hvor det er lett å finne fram relevant informasjon.

## Seminarer og foredragsvirksomhet

I 2001 og 2002 organiserte Datatilsynet sin egen kurs- og seminarvirksomhet, hvor det var satt av øremerkede midler og tilhørende inntektskrav for å finansiere denne virksomheten. Denne finansieringen falt bort med virkning fra 2003-budsjettet, og kursvirksomheten i Datatilsynets egen regi er derfor opphørt. Datatilsynet har i stedet satset på å stille opp med foredragsholdere på konferanser og seminarer i regi av andre. Dette har vært en vellykket strategi, og Datatilsynet stilte i 2003 med foredragsholdere på 78 ulike seminarer og konferanser. Det er en markert økning i forhold til året før.

## Veiledningsmøter

Representanter for de behandlingsansvarlige får gjennom egne veilednings- og dialogmøter bistand når det gjelder å kunne oppnå en forholdsmessig sikring av personopplysninger, for eksempel i forbindelse med større utviklingsprosjekter. Det ble i 2003 gjennomført 80 slike veiledningsmøter.

## Sentralisert betjening av telefon- og e-posthenvendelser

Datatilsynet bruker en betydelig del av ressursene til å betjene spørsmål som kommer inn via brev, e-post og telefoner. De aller fleste henvendelsene blir kanalisert til en profesjonalsert førstelinjetjeneste, frontservice, bestående av tre jurister som også trekker på teknologisk kompetanse når de ser behov for det. Dette sikrer at publikum raskt og enkelt får den faglige rådgivning som er nødvendig. I november ble det satt i gang systematisk registrering av telefon- og e-posthenvendelsene når det gjelder antall henvendelser og hvilke temaer publikum ønsker veiledning om. Dette gir et godt grunnlag for å gjøre endrede prioriteringer når det eksempelvis gjelder kommunikasjonsiltak. Den foreløpige statistikken viser at Datatilsynet får desidert mest henvendelser når det gjelder reservasjon mot direkte markedsføring. Arbeidsliv er også et tema hvor det kommer mange henvendelser.

## 2.8 Tilsyns- og sikkerhetsarbeid

Både personopplysningsloven og helseregisterloven vektlegger tilsynsarbeid som et viktig virke-

Tabell 1.1 Oversikt over gjennomførte tilsyn (se vedlegg 1 for detaljert oversikt):

Sektor	Delsektor	Antall tilsyn
Helsesektoren	Primærhelsetjeneste .....	9
	Større helseforetak .....	10
	Andre .....	2
Kommunesektoren	Primærkommuner .....	31
	Fylkeskommuner .....	0
Arbeidsliv	Kundesentre, butikk, taxi mv. ....	11
Annet	Markedsførere .....	3
	Kameraovervåking .....	10
	Schengen informasjonssystem .....	2
	Telekom .....	1
Sum .....		79

middel for å sikre et godt personvern i samfunnet. Datatilsynet bruker operative tilsyn i kombinasjon med andre virkemidler for på den måten å oppnå en mest mulig samlet effekt.

Grunnlaget for tilsynsarbeidet er nedfelt i dokumentet *Strategi og metodikk for operative tilsyn*. Strategien omtaler Datatilsynets forvaltningsområde som helhet og legger føringer for hvordan de operative tilsynene organiseres og gjennomføres. På basis av dette underlaget, og de føringer som følger av Datatilsynets virksomhetsplan, utarbeides halvårlige tilsynsplaner.

I tråd med de overordnede prioriteringene ble tilsynsarbeidet i 2003 konsentrert om behandling av personopplysninger i helsesektoren, kommunene og arbeidslivet.

Det ble gjennomført 79 tilsyn. Dette representerer en nedgang i forhold til året før på 25 prosent. En hovedårsak til reduksjonen er at Datatilsynet i meldingsåret hadde en redusert ressursramme, og dermed også begrenset handlefrihet.

Tilsynsvirksomheten avdekket at et flertall av de besøkte virksomhetene hadde liten kunnskap om regelverket og de prinsippene dette er tuftet på. Kunnskap er en nødvendig betingelse for etterlevelse av de pliktene som personopplysningsloven og helseregisterloven setter opp. Kunnskap er imidlertid ikke tilstrekkelig. Det må også være en underliggende motivasjon og et ønske om å prioritere dette arbeidet i en ellers travelt hverdag. Mange virksomheter ser ut til å oppfatte arbeidet med eksempelvis å etablere et internkontrollsystem som en tung prosess, der man ikke riktig vet hvor man skal starte. Det blir til at man skyver arbeidet foran seg.

Ser man alle tilsyn under ett, er følgende avvik typiske:

- uryddighet knyttet til ansvar og myndighet
- brudd på bestemmelser om internkontroll
- brudd på bestemmelser om informasjonssikkerhet

Til forskjell fra tidligere år er ikke lenger brudd på meldeplikten så fremtredende. Det kan skyldes at plikten til å melde behandling av personopplysninger inn til Datatilsynet er blitt bedre kjent som følge av en informasjonskampanje ved inngangen til 2003.

### Uryddighet knyttet til ansvar og myndighet

Det ble avdekket flere tilfeller hvor virksomhetens ledelse ikke hadde sørget for å definere klare rammer for ansvars- og myndighetsforhold omkring behandlingen av personopplysninger. Det var også en manglende helhetsoversikt over hva slags personopplysninger som faktisk behandles.

Det at en virksomhet setter bort deler av sin behandling av personopplysninger til underleverandører betyr ikke at man samtidig setter bort *ansvaret* for oppfyllelse av personopplysningsloven eller helseregisterloven. Virksomheten beholder fortsatt ansvaret, ved den behandlingsansvarlige. Gjennom tilsynene har det imidlertid vist seg at ansvarsforholdene ofte ikke er tilstrekkelig avklart mellom behandlingsansvarlig og underleverandør, kalt databehandler. Dette skal gjøres gjennom en databehandleravtale.

### Brudd på bestemmelser om internkontroll

Personopplysningsloven og helseregisterloven krever at virksomheter som behandler personopplysninger skal etablere et system for internkontroll. Dette innebærer at den behandlingsansvarlige skal sørge for å ha kjennskap til gjeldende regler for behandling av personopplysninger. Det skal også foreligge en tilstrekkelig og oppdatert dokumentasjon for de rutiner og tiltak som er satt i gang for å sikre etterlevelse av regelverket.

Å få etablert et system for internkontroll synes imidlertid å være et gjennomgående problem for virksomhetene. I overraskende grad er det også i flere av de store virksomhetene kun satt i gang fragmenterte arbeider med å dokumentere at virksomheten har kontroll over sin behandling av personopplysninger.

Avvik med hensyn til internkontroll er:

- at arbeidet med internkontroll ikke har tilstrekkelig forankring i toppledelsen
- at virksomheten ikke har identifisert krav og plikter etter personvernlovgivningen
- at internkontrollsystemet ikke er konsistent, og at det kun foreligger sporadiske rutiner med hensyn til å sikre et godt personvern
- at behandlingene av personopplysninger i virksomheten ikke er systematisk kartlagt
- at relevante rutiner ikke er kjent blant ansatte (manglende implementering)
- at rutiner for periodisk gjennomgang og for avvikssituasjoner mangler. Hvis rutinene finnes blir de i liten grad fulgt

Fra flere tilsynsobjekters side ble det uttrykt at de har problemer med å få bygget opp et enhetlig internkontrollsystem. Man finner det vanskelig å etablere en struktur i systemet og å ta stilling til hva som faktisk skal inngå i dette.

### Brudd på bestemmelser om informasjonssikkerhet

Den behandlingsansvarlige skal, gjennom planlagte og systematiske tiltak, sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Tiltakene skal vurderes ut fra hensynet til konfidensialitet, integritet og tilgjengelighet. Tiltakene skal også dokumenteres. Alle som behandler personopplysninger skal derfor gjøre en risikovurdering. I denne risikovurderingen skal man ta utgangspunkt i de personopplysningene som behandles, holdt opp mot det trusselbildet som virksomheten ut fra sin egenart står overfor. Vanligste avvik med hensyn til bestemmelsene om informasjonssikkerhet er:

- manglende sikkerhetsmål og sikkerhetsstrategi
- manglende risikovurdering
- manglende konfigurasjonskontroll
- uavklart ansvar og myndighet mht. informasjonssystemet
- manglende implementering av organisatoriske og tekniske sikkerhetstiltak
- driftsmessige forhold slik som autorisasjonsrutiner (tilgangskontroll) og bruk av sikkerhetslogger

Det ble observert noe bedring knyttet til etablering av sikkerhetsmål, sikkerhetsstrategi og konfigurasjonskontroll. I dette ligger at virksomhetene har fastsatt rammer for informasjonssikkerheten. Imidlertid varierer det mye i hvilken grad disse rammene faktisk er implementert. Det ble på tilsynene gitt uttrykk for at regelverket innen informasjonssikkerhet er noe vanskelig å forstå. Videre ble det, spesielt hos de mindre virksomhetene, hevdet at regelverket er for pretensiosøst og omfattende i forhold til virksomhetens størrelse.

Mange virksomheter ser ut til å oppfatte personopplysningsloven til kun å gjelde informasjonssikkerhet. Dette fører til at regelverkets øvrige plikter lett blir neglisjert, for eksempel når det gjelder å ha rutiner for innsyn, retting og sletting av personopplysninger.

### Oppfølgende tiltak

Datatilsynet ser klart behov for en fortsatt tett oppfølging av de tre sektorene som har vært i fokus i 2003. Tilsynet vil i tiden fremover satse på målrettede tiltak mot de aktuelle sektorene, for på den måten å bidra til en positiv utvikling. Dette innebærer blant annet:

- å spisse og målrette de operative tilsynene mot bestemte objekter og typer behandling av personopplysninger. Dette vil særlig gjelde innen helsesektor og arbeidsliv
- å utarbeide veiledninger knyttet til informasjonssikkerhet og internkontroll
- å utarbeide retningslinjer som berører personvern innen arbeidslivet, og distribuere disse til partene i arbeidslivet
- å delta i ulike seminarer, samarbeidsfora og arbeidsgrupper hvor de mest relevante problemstillinger tas opp og behandles
- å utarbeide artikler til bransjetidsskrifter
- å bistå med råd og veiledning ovenfor sentrale aktører

Se for øvrig nærmere omtale av tilsynsvirksomheten innen henholdsvis helsesektor, kommunesektor og arbeidsliv.

### 3 Nærmere om de tre fokusområdene

#### 3.1 Helsesektoren

Helsesektoren var et av Datatilsynets satsningsområder i 2003. Datatilsynet så i kontrollbesøk at helseforetak og primærleger fortsatt sliter med å tilpasse seg det systematiske personvernarbeidet lovverket krever. I tillegg reiste konsesjonssøknader og høringsforslag en rekke problemstillinger innen helseforskning.

#### Helseregistre og helseforskning

Helseregisterloven slår fast at det bare er seks eksplisitt navngitte registre som har lov til å bruke helseopplysninger som kan spores tilbake til enkeltpersoner uten at den enkelte blir spurt først. Disse er kreftregisteret, dødsårsaksregisteret, medisinsk fødselsregister, et register for vaksinasjonskontroll samt to registre som er opprettet for å følge med på spesielt alvorlige sykdommer. Andre registre som ikke er samtykkebaserte må enten pseudonymiseres eller aidentifiseres, eller – for mindre omfattende registre – ha konsesjon fra Datatilsynet.

I meldingsåret gav Datatilsynet tidsbegrensede konsesjoner til noen av Folkehelseinstituttets større forskningsregistre. Registerne er såpass omfattende og sensitive at Datatilsynet anbefaler forskriftsregulering fremfor konsesjonsregulering.

Reseptregisteret ble opprettet i 2003 som det første pseudonymiserte registeret hjemlet i helseregisterloven. I høringsrunden til dette registeret var Datatilsynet i tvil om det var Stortingets intensjon at registrene forvaltningen ble gitt kompetanse til å opprette, skulle få et slikt omfang. Det samme spørsmålet ble stilt i forbindelse med et forslag til et nytt pleieregister (IPLOS).

#### Konsesjoner til Nasjonalt folkehelseinstitutt

Datatilsynet gav i 2003 tidsbegrensede konsesjoner til Folkehelseinstituttet for en rekke store registre for epidemiologisk forskning.

Nasjonalt folkehelseinstitutt (FHI) ble opprettet 1. januar 2002. Instituttet har blant annet til oppgave å drive epidemiologisk forskning, og har i den forbindelse fått overført til seg en mengde forskningsmateriale, fra blant annet Statens helseundersøkelser (SHUS).

I desember 2002 mottok Datatilsynet søknad om konsesjoner for mer enn 60 forskningsprosjekter og -registre fra FHI, og det ble gitt tidsbegrensede konsesjoner til de fleste av disse. Konsesjonene er gitt med virkning til eventuell forskrift for helseundersøkelser trer i kraft, og senest til 1. juli 2006.

En rekke av forskningsregistre ble samlet i en felles hovedkonsesjon, *Konsesjonen for landsomfattende helseundersøkelser*. Dette gjelder blant annet konsesjonen for Landsomfattende helseundersøkelser som ble gitt til SHUS i år 2000, Helseundersøkelsen i bydeler og regioner i Oslo (HUBRO) med tilleggsundersøkelser, Helseundersøkelsen i Hedmark og Oppland (OppHed), og Helseundersøkelsene i Oslo.

Formålet med disse registrene er å fremskaffe ny epidemiologisk kunnskap, redusere risiko for sykdom i tidlig stadium og skaffe bedre plangrunnlag for å tilpasse helsetjenesten etter befolkningens behov. Videre er det et formål å skaffe oversikt over helseutviklingen lokalt, regionalt og nasjonalt. Registerne skal bare brukes til forskning i tråd med formålet, generell planlegging og utarbeidelse av statistikk.

Andre forskningsregistre er gitt egne konsesjoner. Dette gjelder blant annet *Konsesjonen for den norske mor- og barnundersøkelsen*. Konsesjonen erstatter den tidligere konsesjonen *Bedre helse for mor og barn – Norsk nyfødtkohort*, som ble gitt til Statens institutt for folkehelse i 1996. Datatilsynet gav konsesjon, men presiserte at mors samtykke på vegne av barnet bare har gyldighet til barnet selv får samtykkekompetanse, i dette tilfellet ved fylte 18 år. For videre behandling av opplysningene må det derfor innhentes samtykke fra barnet selv.

Datatilsynet har konsekvent avslått å gi konsesjon til frafallsanalyser, med mindre de inviterte har samtykket spesielt til dette. Frafallsanalyser er forskning der for eksempel trygdeytelser, utdanning og andre forhold vurderes hos henholdsvis deltakere og frafalne for å beregne hvilken betydning frafallet har. Forskning skal som hovedregel basere seg på deltagerens frivillige og informerte samtykke. Samtykket sørger for at sentrale personvernprinsipper som diskresjon, fullstendighet og innsyn blir ivaretatt. Den enkelte skal ha kontroll over opplysninger om seg selv, og må derfor selv få bestemme hvorvidt han/hun vil bli forsket på. Dette kravet styrkes jo mer sensitiv informasjon det dreier seg om.

#### Abortregisteret

Datatilsynet gav i meldingsåret en tidsbegrenset konsesjon på ett år til abortregisteret.

Abortregisteret ble overført fra Statens helsetilsyn til Nasjonalt Folkehelseinstitutt (FHI) primo 2002. Mot utgangen av 2002 søkte folkehelseinstituttet om konsesjon for dette registeret.

I forarbeidene til helseregisterloven fremgår det at Datatilsynet bare kan gi konsesjon til oppret-

telse av sentrale helseregistre med få og ikke spesielt sensitive helseopplysninger.

Opplysningene i abortregisteret er å anse som svært sensitive. Provosert svangerskapsavbrudd har vært og er omdiskutert. Opplysninger om at noen har bedt om og foretatt abort vil derfor kunne være svært stigmatiserende for den det gjelder. Lov om svangerskapsavbrudd gir kvinner rett til selv å bestemme om et svangerskap skal avbrytes eller fullføres. Dersom opplysninger om at man har valgt å avbryte svangerskapet blir registrert, så vil dette etter Datatilsynets skjønn kunne virke begrensende på denne selvbestemmelsesretten.

Datatilsynet fant heller ikke at dagens abortlov kan hjemle registeret. Abortregisteret bør derfor etter Datatilsynets mening hjemles direkte i lov. Konesjonen er gitt med virkning frem til lovhjemmel foreligger, men senest frem til 1. juni 2004.

### **Twisten mellom Ullevål universitetssykehus og forsker Trond P. Leren**

I 2003 kom Personvernemnda til en annen konklusjon enn Datatilsynet i en sak som gjaldt disposisjonsrett til biologisk forskningsmateriale.

Trond P. Leren var ansatt på Ullevål universitetssykehus og drev et forskningsprosjekt der. Da han sluttet, oppstod det uenighet om disposisjonsretten til biologisk materiale som hadde vært benyttet i prosjektet. Leren mente at materialet måtte være en del av forskningsprosjektet, noe Datatilsynet støttet. Ullevål hevdet at dette måtte oppbevares i sykehusets pasientjournal. Tilsynet påla Ullevål å utlevere blodprøvene til forskeren.

Personvernemnda behandlet klagesaken fra Ullevål i april 2003, og kom til et vesentlig annet resultat enn Datatilsynet. De konkluderte blant annet med at biologisk materiale (blodprøver) i seg selv ikke er personopplysninger og derfor ikke er underlagt Datatilsynets kompetanseområde. Et pålegg må knytte seg til opplysninger som er utledet fra materialet, typisk analysedata. Videre påla nemnda Ullevål å slette alle personopplysninger som oppbevares i tilknytning til det biologiske materialet. Dette til tross for at ingen av partene i saken har anført sletting som et alternativ. Nemndas begrunnelse er at verken personopplysningsloven eller helseregisterloven gir Datatilsynet hjemmel til å pålegge overføring til en tredjepart.

Datatilsynet er uenig i nemndas tolkning på flere punkter og mener at vedtaket medfører en vesentlig innskrenkning av Datatilsynets mandat. Dette på et område hvor personverntrustelsen stadig øker ettersom man får metoder og teknologi som gjør utnyttelsen av biologisk materiale bedre

og enklere. Tilsynet ba derfor Justisdepartementets lovavdeling, som tolkningsansvarlig for personopplysningsloven, om en uttalelse i sakens anledning. Lovavdelingen ble også bedt om å vurdere behovet for en eventuell lovendring. Justisdepartementet konkluderte at behovet for lovendring vil bli vurdert i forbindelse med et pågående arbeid med revisjon av personopplysningsloven.

Trond P. Leren anmodet Personvernemnda om en ny vurdering av saken, men i et møte i november 2003 konkluderte nemnda at den ønsket å opprettholde vedtaket.

### **Slagpasienter og samtykke**

Datatilsynet gav i meldingsåret en forsker fra Ullevål Universitetssykehus delvis avslag på sin konsekusjonssøknad om uttesting av trombolytisk behandling ved hjerneslag. Forskeren ønsket å kunne inkludere slagpasienter som ikke kunne samtykke selv, og som ikke hadde pårørende som kunne samtykke for dem. Dette punktet i søknaden ble avslått av Datatilsynet.

Avslaget ble begrunnet med at deltakelse i denne studien kan ha alvorlige konsekvenser for pasienten. Personopplysningsloven krever at Datatilsynet vurderer hvorvidt behandlingen av personopplysninger til oppgitt formål, i dette tilfellet forskning, innebærer en ulempe for den enkelte som ikke oppveies av hensyn som taler for behandlingen.

Datatilsynet pekte i merknadene til konsesjonen på at forskningsinteressene og pasientens interesse for helsehjelp i denne saken ikke nødvendigvis ville være sammenfallende: Pasienten ville løpe en risiko for fellesskapets interesser ved å delta i prosjektet. Hvorvidt pasienten ville ha ønsket dette, var etter Datatilsynets mening pasientens pårørende langt nærmere til å vurdere enn den behandlingsansvarlige lege.

### **Sletting fra historiske helseregistre: Psykoseregisteret**

I meldingsåret omgjorde Personvernemnda en sak som gjaldt et ønske fra en privatperson om sletting i fra *Sentralkartoteket for alvorlig sinnslidende* (psykoseregisteret). Dette registeret er ikke lenger i bruk; det ble overført til Riksarkivet da man antok at det var av forskningsmessig interesse, og at videre oppbevaring derfor kunne forsvares. Datatilsynet var ved den anledning i mot at registeret skulle oppbevares.

Datatilsynet vedtok i utgangspunktet sletting av navnet til privatpersonen i registeret. Avgjørelsen ble påklaget, fordi vedkommende syntes det var

meget belastende at resten av opplysningene fortsatt skulle være lagret der. Personvernemnda, ankeinstansen, vedtok at alle opplysninger om klageren skulle slettes. Begrunnelsen var at opplysningene var spesielt belastende, og at dette måtte ha større vekt enn at registeret som helhet ble vurdert som bevaringsverdig for forskningsformål. Datatilsynet var meget fornøyd med avgjørelsen.

### **Pseudonymiserte helseregistre: reseptregisteret og IPLOS-registeret**

I 2003 har Datatilsynet avgitt høringsuttalelser til forslag til forskrifter om opprettelse av sentrale helseregistre – *reseptregisteret* og *register for individbasert pleie- og omsorgstatistikk* (IPLOS). Reseptregisteret trådte i kraft 20. oktober 2003 etter en rask behandling i Statsråd. IPLOS-registeret er ved utgangen av meldingsåret ikke trådt i kraft.

Pseudonymiserte registre er i prinsippet registre der enkeltpersoners identitet er kodet, slik at registreieren ikke skal kunne vite hvem de enkelte opplysningene gjelder. Reseptregisteret ble gjort pseudonymisert og obligatorisk fordi man ønsker å følge befolkningens legemiddelbruk over meget lang tid, og også sammenkoble opplysningene med andre registre. IPLOS-registeret er tenkt gjort pseudonymisert og obligatorisk fordi man ønsker å lage statistikk over pleietrengende pasienter i eget hjem, og at dette skal være umulig dersom noen skulle nekte å la seg registrere. Også forslaget til IPLOS-forskrift inneholdt bestemmelser som gjør sammenkobling med andre registre mulig.

#### *Lagring til «evig tid»*

Datatilsynet ser en personvernrisiko i at landsomfattende registre med store ansamlinger av sensitive opplysninger om mange personer blir opprettet som pseudonymiserte registre for «evig» tid. Reseptregisteret og IPLOS-registeret bør etter Datatilsynets oppfatning helst baseres på at borgerne gis anledning til å samtykke, eller at registeret gis uttrykkelig hjemmel i lov.

Da helseregisterloven ble vedtatt, uttalte sosialkomiteen at det skal stilles strengere krav til opprettelse av et helseregister til bruk for forvaltningen enn til bruk for helsetjenesten: «*Fordi forvaltningens behov for informasjon ut fra ønsket om bedre forebyggingsstrategier egentlig ikke har noen grenser, kan i prinsippet hele befolkningens livsførsel registreres,*» sa komiteen i sin innstilling til Odelstinget. Sosialkomiteen ba videre om tilbakeholdenhet med opprettelsen av slike registre, og presiserte at de burde opprettes avidentifisert eller pseudonymi-

sert. Datatilsynet forstår dette slik at Stortinget uansett har forutsatt at forvaltningen skal være tilbakeholden, også når det er snakk om pseudonymiserte registre.

Datatilsynet er i tvil om det var Stortingets intensjon at registrene som forvaltningen ble gitt kompetanse til å opprette, skulle bli så omfattende. Da helseregisterloven ble vedtatt, viste sosialkomiteen til at det er viktig å sikre en demokratisk prosess ved opprettelsen av store, sentrale helseregistre. En stortingsbehandling ville ha sikret demokratisk kontroll med forvaltningens åpenbart raskt økende behov for opplysninger om landets borgere.

#### *Ikke anonymt*

Pseudonymisering er ikke et trylleformular som fjerner alle personvernulemper, men et middel som vil kunne avhjelpe noen av dem. Jo større datamengde man har om en bestemt person, jo nærmere vil man komme identifiserbarhet, selv med pseudonym. Selv om det på det nåværende tidspunkt ikke er lov, vil det også være mulig å koble opplysningene til den navngitte, eller på annen måte identifiserbare, enkeltpersonen de stammer fra.

Det faktum at pseudonymiserte registre ikke sikrer anonymitet, gjør at man må kunne stille strenge krav til begrunnelsen for hvert enkelt register. Personvernulempene ved registeret må også bli tilstrekkelig utredet, og avvies mot fordelene man ønsker å oppnå.

Datatilsynet mente i høringsrundene at begrunnelsene som skulle godtgjøre opprettelsen av reseptregisteret og IPLOS-registeret var mangelfulle.

### **Helseforetak og primærleger**

Helseforetak og primærleger var blant de prioriterte gruppene for tilsyn i 2003. Begge gruppene blir sterkt oppfordret til å knytte seg til forskjellige helsenettverk som skal gjøre det mulig å utveksle helseopplysninger mer effektivt. Datatilsynet advarer mot å kaste seg inn i slike prosesser uten først å ha avklarte ansvarsforhold, viten om hvordan man internt behandler personopplysninger, og kjennskap til hvilke krav som ligger i helseregisterloven og personopplysningsloven.

#### *Nasjonale og regionale helsenett*

I september 2003 ble det nasjonale helsenettet satt i drift, uten at det foreløpig er klart definert hva det konkrete innholdet i nettet skal være. En ny tiltaksplan for utvikling av helsenettene ble sendt ut på



høring mot slutten av meldingsåret, og dette arbeidet skal peke ut retningen videre. Det nasjonale helsenettet består nå av en sentral infrastruktur for sammenkobling av de fem regionale helsenettene, som på sin side binder sammen helseforetak i hver enkelt region, samt leger, apoteker mv.

Det er ulik praksis i de fem regionale helsenettene med hensyn til hvordan virksomhetene utveksler helseopplysninger. Helsenettene tilbyr ulike tekniske løsninger. Noen av de regionale helsenettene har prioritert enkel tilgang til Internettjenester og e-post. Datatilsynet har også sett at enkelte foretak har lagt til rette for direkte tilgang til journaler for andre foretak. I andre regionale helsenett har man vært tilbakeholdne med dette. Datatilsynet har i en rekke sammenhenger vist til regelverkets krav med hensyn til tilgangskontroll og utlevering av helseopplysninger. Den forskjelligartede praksisen gjør det vanskelig å vite hvilke oppgaver det sentrale nettet skal få. Sosial- og helsedirektoratet ser imidlertid ut til å prioritere at det nasjonale nettet får et spesielt fokus på utveksling av henvisninger, epikriser, svar på prøver fra laboratorium og sykemeldinger. Videre diskuteres det bruk av helsenettene i forbindelse med telemedisin.

#### *Lav bevissthet rundt ansvar*

Datatilsynet avdekket under tilsynene at de fleste helseforetakene manglet avklaringer i forhold til ansvar for behandlingen av personopplysninger. I tillegg hadde de mangler i forhold til dokumentasjon av internkontroll og informasjonssikkerhet. Ansvarsforholdet ved tilkobling til helsenettene er også uklart definert hos noen av virksomhetene. Datatilsynet er derfor bekymret over aktørenes iver etter å koble seg til. Før det kan anses som forsvarlig å knytte seg til eksterne nett, må virksomheten ha et forsvarlig sikkerhetsnivå selv. Dette innebærer at virksomheten må kunne sannsynliggjøre tilfredstillende sikkerhet med en risikovurdering av løsningene. Virksomhetene må også forvise seg om at sikkerheten fortsatt blir ivaretatt etter tilkoblingen.

Datatilsynet fant ved tilsyn i meldingsåret at noen legekantor var tilknyttet regionale helsenett uten at dette var sikkerhetsmessig vurdert fra legekantorenes side. Legekantorene forventet at sikkerheten ble ivaretatt av helsenettene, uten at dette gikk frem av avtaler. Et legekantor vil bare kunne forvise seg om slik ivaretakelse ved en dekkende databehandler- eller leverandøravtale med helsenettet. I et tenkt tilfelle, der legekantoret ikke har en slik avtale på plass, og personopplysninger kommer på avveie, kan det enkelte legekantor bli gjort ansvarlig for brudd på helseregisterloven.

Det pågår nå et arbeid for å lage retningslinjer og avtalevilkår for helsenettene. Datatilsynet følger denne utviklingen nøye, og forutsetter at avtalene får en god utforming. Datatilsynet forutsetter også at personvernprinsippene som ligger til grunn for helseregisterloven blir vektlagt.

#### *Hvem skal få lese journalene?*

Journaler skal ikke leses av uvedkommende. I begrepet uvedkommende ligger også helsepersonell som ikke har tjenstlig behov for tilgang til helseopplysningene. Det må ligge begrensninger i tilgangen. Hvordan tilgangskontrollen skal skje er et viktig og sentralt spørsmål som den behandlingsansvarlige må ta stilling til ut fra en medisinsk faglig vurdering. Dette skal også avveies mot personverninteressen.

Helsepersonell kan komme til å trenge opplysninger fra journalene uten at de i utgangspunktet er autorisert for tilgang. Internt i helseforetaket avgjør ofte den enkelte lege selv at han trenger tilgang. Ved tilgang på tvers av helseforetakene begrunnes gjerne tilgang til opplysninger med administrative behov, eller at det foreligger grunnlag for såkalt «blålys-tilgang» til journalen. Tilgangsbegrunnelsen er ofte mangelfull, og Datatilsynets erfaring er at tilgangsloggene sjelden analyseres forsvarlig. Dette gjør at man ikke har reelle muligheter til å avdekke tilgang uten medisinsk begrunnelse.

Tilsynene i 2003 avdekket at det var vanlig praksis på legekantorene at alle leger og administrativt personell har tilgang til alle pasientjournaler. Dette gjelder uavhengig av hvordan legekantoret var organisert. Måten kontoret er organisert på, utpeker den som er rettslig ansvarlig for opplysningene. Tilgangspraksisen kan bety at personer uten et avklart tjenstlig behov til opplysningene likevel gis tilgang. Datatilsynet har rettet henvendelse til helsemyndighetene for å få en del avklaringer om måten dette blir gjort på, og har i denne sammenheng også vist til at praksisen kan være i strid med grunnleggende personvernrettigheter. Svaret foreligger ikke per januar 2004.

#### **Lovende tiltak fra bransjen selv**

Datatilsynet har i meldingsåret også sett lovende tiltak fra bransjen selv. Disse kan bidra til å ivareta personvernet for pasientene bedre, og etterlevelsen av lovkravene enklere. Datatilsynet har bl.a. gitt uttalelser i forbindelse med systemet *Trinnvis* som er under utvikling i regi av Legeforeningen. Systemet skal hjelpe legekantorene til å opprette en tilfredsstillende internkontroll.

Datatilsynet er også positiv til at det er under utvikling en bransjenorm som har til hensikt å bringe informasjonssikkerheten i en sentral posisjon i helsesektoren.

### 3.2 Kommunesektoren

Kommunene kjennetegnes ved å være tilbyder av et vidt spekter av tjenester og oppgaver overfor sine innbyggere. Omfanget og bredden i kommunens tjenestespekter gjør at det i en rekke av fagetatene er behov for å behandle også sensitive personopplysninger.

Den teknologiske utviklingen og satsingen på service og tilgjengelighet, kombinert med krav til effektivisering, har gjort at det i mange kommuner foregår et betydelig utviklingsarbeide. Det legges opp til selvbetjeningsløsninger via Internett, samlokalisering av etater og etablering av offentlige servicekontorer. Flere kommuner satses også på regionale samarbeidsløsninger. Dette stiller store krav til avklaring av ansvarsforhold og en dokumentert informasjonssikkerhet.

#### Lite systematisk tilnærming i kommunene

Det ble i 2003 gjennomført operative tilsyn hos 31 kommuner spredt over hele landet. Ved tilsynene ble det i første rekke kartlagt i hvor stor grad kommunene etterlever de krav som personopplysningsloven stiller til at det skal være etablert et system for internkontroll. Gjennom internkontrollsystemet skal det foreligge dokumentasjon for at det er iverksatt rutiner og tiltak som sikrer at kommunen virkelig etterlever de formelle kravene som gjelder for behandling av personopplysninger.

I den gamle personregisterloven var kommunene underlagt konsesjonsplikt for sin behandling av personopplysninger. Kommunene er derfor stort sett godt kjent med de *prinsippene* som ligger til grunn også for dagens personvernlovgivning. Gjennomgående gjøres det derfor i praksis mye korrekt, idet saksbehandlere og mellomledere i kommunen ser ut til å være bevisste sitt ansvar når det gjelder å sikre at personopplysninger blir behandlet på en betryggende måte. For eksempel er taushetsplikten i medhold av forvaltningsloven og annen særlovgivning godt innarbeidet. Det mangler imidlertid en systematisk tilnærming og dokumentasjon når det gjelder hvordan personopplysninger blir behandlet. Det oppstår lett misforståelser og feil, for eksempel når det kommer nye medarbeidere som ikke har god nok kjennskap til de ikke-dokumenterte rutinene.

#### Manglende oversikt

Kommunene må forholde seg til regelverket som helhet og derigjennom iverksette de pliktene som kommer til anvendelse. For i det hele tatt å kunne ha mulighet til å identifisere og gjennomføre sine plikter, må kommunene ha definert klare ansvars- og myndighetsforhold. Videre må det eksistere en oversikt over hvilke behandlinger av personopplysninger kommunen faktisk utfører. Ved tilsynene ble det funnet mange avvik i forhold til disse helt elementære forutsetningene.

Ivaretagelse av et lovfestet personvern vil i slike tilfeller bero mer på tilfeldigheter og de enkelte medarbeideres holdninger til personvern. Dette er lite tilfredstillende.

#### Rådmannens ansvar

Rådmannen, dvs. kommunens øverste administrative leder, er vanligvis den funksjonen som ivaretar behandlingsansvaret i kommunen. Rådmannen vil naturlig nok måtte delegerer ansvar og myndighet videre til respektive etatsledere når det gjelder å effektivere de enkelte pliktene. Det er imidlertid rådmannen som behandlingsansvarlig som skal fastsette rammene som de øvrige aktørene skal forholde seg til. Det kan ikke overlates til andre.

Hos kun et mindretall av tilsynsobjektene var det etablert en god formell struktur i forhold til ansvar og myndighet. I flere tilfeller synes rådmannen å ha svært liten medvirkning i forhold til implementering av regelverket. I andre tilfeller var det uklare rammer for ansvar og myndighet. Betydningen av orden og en ledelsesmessig struktur kan ikke understrekes nok.

#### Internkontroll ikke etablert

Det ble påvist mangler i forhold til etablering av internkontrollsystem hos et flertall av de kommunene som ble besøkt. Det var imidlertid store variasjoner med hensyn til hvor omfattende manglene var. Noen av kommunene hadde ikke i det hele tatt startet prosessen med å etablere et internkontrollsystem, mens noen få var nær ved å ha et fullt ut dokumentert internkontrollsystem på plass. Hos de fleste kommunene var situasjonen noe i mellom disse to ytterpunktene; det var etablert kun sporadiske rutiner for enkelte plikter i regelverket. Rutinene var ikke forankret i et helhetlig system.

#### Hvilke behandlinger foretas?

Behandlingsansvarlig må ha oversikt over hvilke behandlinger som foretas for å vite hvilke plikter

den behandlingsansvarlige har, og hvilke rettigheter lovverket gir den registrerte. Plikter og rettigheter er knyttet til selve behandlingen og kan derfor variere fra virksomhet til virksomhet, avhengig av hvilke behandlinger som finner sted.

Gjennom tilsynsvirksomheten ble det avdekket at mange kommuner mangler en samlet oversikt over hvilke behandlinger som foretas i kommunens regi. Dette innebærer i praksis at rådmannen som behandlingsansvarlig har liten reell kontroll med hvilke behandlinger vedkommende står ansvarlig for. Dette avskjærer den behandlingsansvarlige fra å ivareta sine plikter på en tilstrekkelig måte. En rekke kommuner sitter følgelig nå i den situasjon at de behandler en rekke personopplysninger uten at behandlingsansvaret er ivaretatt slik regelverket krever.

#### *Mangelfulle avtaler med databehandlere*

Regelverket krever at databehandler kun kan behandle personopplysninger i samsvar med det som er fastsatt i avtale med behandlingsansvarlig. Det ble påvist mangler i forhold til avtale med databehandler hos en rekke kommuner. I noen tilfeller kunne ikke avtale eller kontrakt med databehandler fremlegges, mens i andre tilfeller inneholdt avtalen få eller ingen elementer som berørte databehandlers behandling av personopplysningene.

#### **Meldeplikten overholdes ikke**

I motsetning til den gamle personregisterloven, gir dagens personvernlovgivning i stor grad kommunene fritak for konsesjonsplikt når det gjelder behandling av personopplysninger. Vilkåret er imidlertid at behandlingen har hjemmel i lov. Det er eksempelvis fortsatt konsesjonsplikt når det gjelder elektronisk behandling av sensitive personopplysninger som ikke er hjemlet i lov. Selv om konsesjonsplikten stort sett er falt bort, er den erstattet av en meldeplikt. På Datatilsynets hjemmeside er det publisert en veileder som orienterer nærmere om konsesjons- og meldeplikten kommunene skal forholde seg til.

Naturlig nok er kommunene svært ensartede med hensyn til hva slags tjenester de yter, og hva slags type personopplysninger de behandler. Dette skulle tilsi at de behandlingene av personopplysninger som er meldepliktige til Datatilsynet, også burde være tilsvarende ensartet. Kommunestørrelsen eller geografisk plassering bør i liten grad gi forskjeller med hensyn til hva som meldes inn til Datatilsynet. Gjennom tilsynsvirksomheten ble det imidlertid avdekket at antallet meldinger som kommu-

nene hadde sendt inn til Datatilsynet, varierte fra null til over tretti. Gjennomgående var det sendt for få meldinger i forhold til hva regelverket forutsetter. Brudd på denne plikten henger tydelig sammen med en manglende oversikt over hvilke behandlinger som foretas i kommunen.

#### **Samlokalisering av fagetater og offentlige servicekontorer**

I en del kommuner er det samlokalisert ulike fagetater. Dette innebærer gjerne også felles arkiv, skrivere mv. Selv om dette ut fra hensynet til effektivisering og helhetlig betjening av den enkelte bruker kan synes fornuftig, reises imidlertid en rekke prinsipielle spørsmål knyttet til innbyggernes personvern. Taushetsplikten som følger av de enkelte særlover kan stå i fare ved denne typen organisering. Taushetsplikten gjelder også overfor egne kollegaer uten tjenstlig behov for tilgang til opplysningene, så vel som overfor andre uvedkommende. I små kommuner er denne problemstilling særlig relevant fordi mye og detaljert informasjon om den enkelte bruker lett blir tilgjengelig for hele personalet som holder til i de samlokaliserte tjenestene. Kommunene synes gjennomgående å være klar over denne problemstillingen. I den praktiske virkelighet er det imidlertid bare i varierende grad tatt hensyn til dette.

#### **SATS**

Det er også i enkelte kommuner planer om å samlokalisere etter den såkalte SATS-modellen (samordning trygd, sosial og arbeidsformidling).

Denne typen behandling av sensitive personopplysninger i servicekontorer, hjemlet i ulike særlover, kan skape særlige personvernmessige utfordringer. Datatilsynet vil derfor følge utviklingen nøye.

#### **Interkommunalt samarbeid**

I økende grad etablerer kommunene samarbeidsløsninger på tvers av kommunegrensene som innebærer felles bruk av informasjonsteknologi. For små kommuner vil det ofte være vanskelig å etablere en IT-infrastruktur som ivaretar kommunens behov for fleksibilitet, samtidig som en tilfredsstillende informasjonssikkerhet opprettholdes. Datatilsynet ser derfor positiv på at kommunene etablerer samarbeidsløsninger. Imidlertid må den felles infrastrukturen som etableres ivareta at hver enkelt kommune fortsatt har et selvstendig ansvar i forhold til sin behandling av personopplysninger.

Klargjøring av ansvar er derfor en viktig forutsetning for å lykkes med slike interkommunale samarbeidsprosjekter.

### Ikke rutiner for sletting

Gjennom tilsynene ble det avdekket at mange av kommunene hadde mangelfulle rutiner for sletting av personopplysninger. Det ble særlig gjort denne typen funn innen barnevernet. Bekymringsmeldinger ble ikke slettet, selv om det ikke lenger var grunnlag for å beholde dem. Datatilsynet påpekte avviket overfor de aktuelle kommunene, slik at forholdet er rettet. Det er likevel grunn til å tro at dette med manglende rutiner for sletting av personopplysninger er et gjennomgående problem i kommunesektoren.

### Tilgangskontroll og sikkerhetslogger

Datatilsynet avdekket ingen alvorlig brudd på regelverket knyttet til tilgangskontroll. Imidlertid var det en del kommuner som opererte med *singel logon*. Dette gir den ansatte tilgangsrettigheter som også omfatter fagapplikasjoner. Dette, kombinert med en noe svak autentisering av bruker, og mangler i forhold til kontroll av sikkerhetslogger, kan sette personvernet i fare. Datatilsynet kunne ikke direkte påvise brudd hvor nevnte kombinasjoner var tilstede. Mange kommuner er også flinke til å seksjonere brukere til henholdsvis sikker og administrativ sone, hvilket kan begrense konsekvensene ved eventuelle brudd. Datatilsynet anbefaler likevel at kommunene setter fokus på denne problemstillingen.

Kommunene synes i varierende grad å forholde seg til kravene om at det skal foretas sikkerhetslogging. Dette var knyttet både til bruk av loggene og hvor lenge de skal oppbevares. Det ble også påvist problemer med å håndtere loggene for visse fagapplikasjoner. Struktur og anvendelse av sikkerhetslogger er derfor noe sikkerhetslederne i kommunene bør se nærmere på.

### Hva gjør Datatilsynet?

Gjennom de 31 tilsynene hos kommunene i 2003 har Datatilsynet dannet seg et godt bilde av hvor skoen trykker i forhold til kommunenes behandling av personopplysninger. Datatilsynet vil derfor nå prioritere arbeidet med å få utarbeidet nytt veiledningsmaterieell om internkontroll og informasjonssikkerhet. I tillegg vil tilsynet bidra med foredragsholdere på kurs- og seminarer rettet mot kommunene. Datatilsynet har i den forbindelse tatt initiativ til et samarbeid med Kommunenes sentral-

forbund om blant annet å arrangere et seminar om personvern i kommunesektoren.

Som en følge av den økte oppmerksomheten omkring kommunenes behandling av personopplysninger har flere kommuner gått sammen og etablert Foreningen kommunal informasjonssikkerhet, ([www.kins.no](http://www.kins.no)). Datatilsynet deltok på stiftelsesmøtet våren 2003, og var også bidragsyter på foreningens første konferanse om kommunal informasjonssikkerhet. Datatilsynet ser svært positivt på at noen aktive kommuner på denne måten har skapt en felles arena for de utfordringene kommunene står overfor når det gjelder å ivareta en god informasjonssikkerhet.

### Bruk av offentlige registre til andre formål

Datatilsynet erfarer i økende grad at personopplysninger fra offentlige registre som er opprettet for helt spesifikke formål ønskes tatt i bruk også i andre sammenhenger. Det kan fremføres mange, og i og for seg gode, argumenter for en ny bruk av opplysningene. Det er imidlertid et sentralt grunnkrav i personvernlovgivningen at opplysninger i offentlige registre hvor enkeltindivider er pliktig til å være registrert, bare skal brukes til det formålet de er samlet inn for. Dette vil gjelde med mindre den enkelte samtykker til annen bruk. Når det opprinnelige formålet med registeret er oppfylt, skal personopplysningene slettes, dersom de ikke må oppbevares etter andre lovbestemmelser, for eksempel arkivloven. Unntak gjelder kun dersom den enkelte gir sitt samtykke til fortsatt lagring, eller samfunnets interesse i å fortsatt lagre opplysningene for historiske, statistiske eller vitenskapelige formål *klart* overstiger de ulempene det kan føre til for den enkelte.

To saker fra meldingsåret illustrerer at disse sentrale prinsippene i personvernet i mange sammenhenger blir satt på prøve:

#### *Kartlegging av ulovlige boliger i Stavanger*

I 2000 vedtok Stortinget at det skulle iverksettes et boligadresseringsprosjekt. Sammen med folke- og boligtellingsprosjektet var formålet med prosjektet å samle data som grunnlag for best mulig *statistikk* om levekår og boforhold i Norge. Samtidig skulle prosjektene bidra til en heving av kvaliteten i de to sentrale basisregistrene, folkeregisteret og GAB-registeret (register over grunneiendom, adresse og bygninger). Boligadresseringsprosjektet innebar en innføring av bolignummer som del av offisiell adresse. Statistisk Sentralbyrå, Statens kartverk og Skattedirektoratet samarbeidet nært med kommunene i selve gjennomføringen av prosjektet.

Etter at GAB-registeret som følge av boligadresseringsprosjektet var blitt utvidet til også å inneholde opplysninger om *boligtype*, koplet Stavanger kommune disse opplysningene opp mot opplysninger i folkeregisteret og telefonkatalogen. I de tilfeller kommunen ved å sammenstille dataene fant at det var flere boenheter i en bygning enn hva boligtypen i følge GAB-registeret skulle tilsi, ble boenheten registrert som ikke-byggegodkjent. Eier eller beboer ble deretter kontaktet av kommunen for å få en avklaring på om det forelå ulovligheter eller ikke.

#### *Kommunen pålagt å slette*

Datatilsynet påla Stavanger kommune å stoppe behandlingen av personopplysninger innhentet i boligadresseringsprosjektet til kartlegging av mulig ulovlige boliger. Kommunen ble også pålagt å slette eventuelle registre over ulovlige boliger, dersom de var opprettet med bakgrunn i opplysninger fra boligadresseringsprosjektet. Datatilsynet mente at bruk av personopplysningene til kontrollformål slik Stavanger kommune hadde tatt dem i bruk, var i strid med det uttalte formålet for boligadresseringsprosjektet om å utarbeide statistikk om boforhold i Norge. Å delta i prosjektet var ikke frivillig, men pålagt ved lov, under trusler om mulig tvangsmulkt om man ikke svarte på spørreskjemaet fra Statistisk Sentralbyrå. I den informasjonen som ble gitt fra myndighetene i forbindelse med prosjektet ble det også understreket at hensynet til den enkeltes personvern stod sentralt, og at svarene i hovedsak skulle brukes til å utarbeide statistikk. Etter Datatilsynets vurdering var Stavanger kommunes bruk av opplysningene rett og slett ikke forenlig med det formålet som ble oppgitt i forbindelse med boligad

Stavanger kommune klaget vedtaket inn for Personvernemnda, som opprettholdt Datatilsynets vedtak.

#### *Billedopptak av pasienter ved Emma Hjort*

På daværende Emma Hjort skole ble det i perioden 1978 til 1991 gjort videoopptak av pasienter. Det opprinnelige formålet med videoopptakene var diagnostisk arbeid og behandling. I tillegg ble opptakene benyttet til institusjonens egen undervisning og forskning.

Akershus fylkeskommune og Emma Hjort skole hadde rammekonsesjoner for videoopptak etter den gamle personregisterloven. Etter nedleggelsen av Emma Hjort var konsesjonene for opptakene ikke lenger gyldige. Fylkeskommunen lagret videoopptakene i sine arkiver etter nedleggelsen av

Emma Hjort, og tok i 2003 kontakt med Datatilsynet for avklaring av hvorvidt materialet kan oppbevares videre hos Statsarkivet i Oslo, for blant annet forskningsformål.

Datatilsynet vurderte spørsmålet om sletting av materialet etter personopplysningsloven, som nå regulerer behandlingen av videoopptakene.

#### *Ulovlig lagret*

Det klare utgangspunktet er at oppbevaring ut over de to årene som var satt som begrensning i konsesjonsvilkårene, krevde at klienten eller dens foresatte hadde samtykket til det. Slike samtykkeerklæringer skal ha vært innhentet, men det kunne ikke dokumenteres. Det er heller ingen grunn til å tro at samtykkeerklæringer ble gitt for oppbevaring også etter at skolen var lagt ned. Datatilsynet konkluderte derfor med at opptakene i mer enn ti år har blitt oppbevart uten gyldig samtykke, og dermed har vært ulovlig lagret.

Datatilsynet kom til at videre oppbevaring ville være i strid med det opprinnelige formålet for opptakene. Personopplysningsloven åpner imidlertid for at personopplysninger som er samlet inn for et bestemt formål likevel kan brukes til historiske eller vitenskapelige formål. Det er imidlertid her en forutsetning at samfunnets interesse klart overstiger ulempene dette kan medføre for den enkelte. Datatilsynet la til grunn at det ikke er usannsynlig at klienten eller de pårørende ville kunne føle ubehag ved å vite at opptakene fortsatt eksisterer. Opptakene er knyttet til forhold som ligger langt tilbake i tid, og mange vil ønske å lukke denne døren bak seg. Riksarkivarens egen vurdering av at han ikke vil gå inn for bevaring ble også tillagt stor vekt.

Etter å ha foretatt en interesseavveining kom Datatilsynet til at det ikke forelå noe hjemmelsgrunnlag for fortsatt oppbevaring av opptakene, og gav derfor pålegg om at de skulle slettes.

Vedtaket ble ikke påklaget.

#### **Småbåtregisteret – frivillig registrering for alle**

Småbåtregisteret ble i 1998 opprettet for å oppnå pålitelige, fullstendige og lett tilgjengelige data om fritidsbåter. I tillegg til en rekke andre uttalte formål, blant annet som hjelpemiddel ved etterforskning av tyverier eller forsikringssvindel, skulle registeret også danne grunnlag for en eventuell miljøbegrunnet båtavgift. Fra opprettelsen av registeret og frem til 1. januar 2003 var det registreringsplikt for den enkelte småbåteier. Pr. juni 2003 stod 334 354 båter registrert.

En ny forskrift gjør at ordningen med registrering i småbåtregisteret er blitt frivillig. Dette innebærer at båteierne som tidligere hadde en pliktig registrering, nå må kunne velge om de fortsatt vil være i registeret eller ikke. Datatilsynet har derfor anmodet Tollvesenet om at personopplysningene slettes, med mindre de båteierne som stod oppført etter den gamle ordningen blir kontaktet og gis en frist til å melde fra at de fortsatt ønsker å være registrert.

#### *Men hva er egentlig formålet nå?*

Datatilsynet uttrykte i sin høringsuttalelse i forbindelse med den nye forskriften at Datatilsynet har problemer med å se hvordan formålene i lov om fritids- og småbåter skal kunne oppfylles når registerordningen nå er blitt frivillig. Når man oppretter et register, er det som regel basert på at den ansvarlige har oppgaver, plikter eller rettigheter overfor den registrerte. Datatilsynet undrer i høringsuttalelsen på hvilke oppgaver Tollvesenet nå skal ha i denne sammenheng, foruten å utstede båt kort.

Dette reiser videre spørsmål om behovet for selve loven og forskriften, da et register over småbåteiere i alle tilfeller også vil være regulert av personopplysningsloven. Dersom andre hensyn enn de som er formulert i fritids- og småbåtloven nødvendiggjør registeret, for eksempel som et redskap for å forenkle arbeidet med etterforskning av båtulykker, bør det vurderes å overføre ansvaret for registeret til en instans som har en mer direkte interesse i registeret og kvaliteten på de registrerte opplysningene.

#### **Sosialkontorer kan ikke rutinemessig kreve kontoutskrifter**

I forbindelse med at mange sosialkontor rutinemessig krevde detaljerte kontoutskrifter fra klienter, mottok Datatilsynet i 2002 en rekke klager fra ulike kanter av landet. Kontoutskriftene var ønsket som en del av dokumentasjonen for utbetaling av sosialstøtte. Tilsynet bad derfor Sosialdepartementet om umiddelbart å utforme klare retningslinjer for i hvilke tilfeller sosialtjenesten kan innhente kontoutskrifter.

På bakgrunn av henvendelsen fra Datatilsynet utarbeidet Sosialdepartementet i 2003 et eget rundskriv overfor landets kommuner om sosialtjenestens adgang til å kreve kontoutskrift fremlagt ved søknad om økonomisk stønad. Det fremgår uttrykkelig av rundskrivet at mye av informasjonen som kommer fram på kontoutskriften ikke vil være relevant for sosialtjenestens behandling av søknad om økonomisk stønad. Av denne grunn skal det ikke

være hovedregelen å kreve kontoutskrift. Dersom det i konkrete situasjoner er nødvendig å be om kontoutskrift, skal det gjøres klart for klienten hvilke opplysninger det er behov for og hvorfor, slik at klienten kan slukke andre opplysninger fra utskriften før den legges frem for sosialtjenesten.

Sosialdepartementet presiserer til slutt at de lovbestemmelsene og prinsippene det redegjøres for i rundskrivet også gjelder for sosialtjenestens innhenting og bruk av andre typer personopplysninger.

Datatilsynet er tilfreds med at Sosialdepartementet har gitt sosialkontorene klare retningslinjer om bruk av kontoutskrifter. Dette bidrar til ensartede rutiner på et område som berører helt grunnleggende personvern hensyn.

#### **3.3 Arbeidsliv**

Problemstillinger knyttet til personvern i arbeidslivet er et av de områdene Datatilsynet mottar flest henvendelser om, både fra arbeidsgiver- og arbeidstakersiden. Det skyldes i stor grad de mulighetene ny teknologi gir, til detaljoppfølging, kontroll og overvåking av arbeidstakere.

Henvendelsene dreier seg for det meste om innsyn i e-post, og kontroll av telefonbruk og Internett. Arbeidsgivers registrering av detaljerte opplysninger om de ansatte, fra tradisjonelle opplysninger i personalmapper til kompetansekartlegging og personlighetstester, oppfattes også som unødig og krenkende.

Datatilsynet gjennomførte i meldingsåret 11 operative tilsyn knyttet til arbeidslivet, med særlig fokus på kundesenterbransjen (også betegnet som callsenter/telefonsenter). I likhet med tilsyn på øvrige sektorer var det et gjennomgående trekk at virksomhetene ikke kunne fremlegge et dokumentert internkontrollsystem. Virksomhetene kunne dermed ikke sannsynliggjøre at de har tilfredsstillende rutiner når det gjelder ivaretagelse av den enkeltes rett til innsyn i hva som er registrert av opplysninger. Om de registrerte ikke vet hva som er registrert, kan de heller ikke ivareta sine rettigheter når det gjelder retting og sletting av opplysningene. Kjennskapen til personopplysningsloven var også gjennomgående lav i de virksomhetene som ble besøkt.

#### **Kundesentre med mye detaljkontroll**

Gjennom tilsyn hos kundesentre er det blitt synliggjort et behov for å trekke opp tydelige grenser for

hvilke kontrolltiltak og registrering av personopplysninger som kan gjennomføres på denne typen arbeidsplass. Dette arbeidet var det fra Datatilsynets side ønskelig å gjøre i samråd med bransjen.

Våren 2003 ble derfor et notat om problemstillingene sendt ut til en rekke organisasjoner innen både arbeidstaker- og arbeidsgiversiden. Det ble deretter holdt et møte med organisasjonene hvor problemstillingene ble nærmere diskutert. Datatilsynet oppfattet møtet som nyttig, og så at en nærmere avklaring av problemstillingene ville være hensiktsmessig. I etterkant av møtet oppfordret Datatilsynet organisasjonene til å komme sammen og forhandle frem nærmere retningslinjer. Svarene fra arbeidstakersiden var gjennomgående positive, mens arbeidsgiversiden hadde innvendinger. Retningslinjer på forbundsnivå antas derfor ikke å komme i overskuelig framtid.

Siden partene i arbeidslivet ikke har forhandlet frem nærmere retningslinjer, opprettholder Datatilsynet sin tolkning av hvordan slike detaljregistreringer skal behandles for å kunne aksepteres i ulike situasjoner. Etter Datatilsynets oppfatning vil dette i rimelig grad ivareta både arbeidsgivers interesser og hensynet til de ansattes personvern. På grunn av parallelle problemstillinger også i andre bransjer, har tolkningene relevans for andre arbeidsplasser.

### Tre formål

Opplysningene fra detaljerte registreringer benyttes etter Datatilsynets erfaring i de fleste tilfeller til tre formål:

1. Beregning av prestasjonslønn
2. Ressurs- og bemanningsplanlegging
3. Måling og individuell oppfølging

#### *Beregning av prestasjonslønn*

Ansatte må informeres om *hvilke* opplysninger som skal registreres, og ikke minst også om *hvordan* disse skal brukes. De samme opplysningene brukes ofte også til andre formål enn beregning av prestasjonslønn. Datatilsynet anbefaler at arbeidsgiver, sammen med representanter for de ansatte, avtaler nærmere rutiner som sikrer at opplysningene ikke brukes på feil måte.

#### *Ressurs- og bemanningsplanlegging*

Det bør være tilstrekkelig å vite hvordan teamet eller gruppen totalt sett presterer. Selv om eksempelvis telefonsystemet registrerer trafikken på individnivå (antall telefoner, hvorav andel besvarte/ube-

svarte, vente- og svartider mv.), bør statistikken ikke taes ut pr. ansatt, men på gruppenivå.

#### *Måling og individuell oppfølging*

Bruk av personopplysninger til måling og individuell oppfølging av den enkelte ansatte må, etter Datatilsynets oppfatning, i utgangspunktet baseres på samtykke. Samtykket har imidlertid en noe spesiell karakter i arbeidslivet. Datatilsynet stiller spørsmål ved graden av frivillighet ved inngåelse av arbeidskontrakt. Dette gjør seg særlig gjeldende i et stramt arbeidsmarked.

### Avtaler mellom arbeidsgiver og arbeidstakerrepresentanter

Utgangspunktet for behandling av personopplysninger er normalt samtykke fra den enkelte. Det å inngå avtaler mellom arbeidsgiver og representanter for de ansatte om hvilke personopplysninger som skal registreres og benyttes, vil likevel kunne bidra til akseptable løsninger. Slike avtaler vil normalt redusere personverntrusselen og gi en større grad av forutsigbarhet og trygghet for den enkelte.

### Medlytting fremfor avlytting

Flere virksomheter har muligheter for at ledere kan gå inn og overhøre telefonsamtaler mellom medarbeider og kunde/respondent. Formålet er opplæring, eller å videreutvikle de ansatte i måten de utfører arbeidet på. Dette kan skje på to måter: *Medlytting* defineres som de tilfellene der samtalen overhøres ved at det kobles et ekstra telefonsett direkte på den ansattes telefon. Medlyttingen skjer i umiddelbar nærhet av den ansatte. *Avlytting* skjer derimot ved at man kobler seg inn på samtalen fra et annet sted, eller at samtalen taes opp og overhøres i ettertid. Den ansatte er da ikke nødvendigvis oppmerksom på dette mens samtalen pågår.

Datatilsynet vurderer personverntrusselen til å være større ved avlytting enn ved medlytting. Avlytting skjer mer i det skjulte, mens det ved en medlytting fremstår som klart og tydelig at kontrolltiltaket faktisk foregår. Medlytting forutsettes derfor benyttet så langt som mulig, fremfor avlytting.

### Nei til karakterfastsetting i arbeidslivet

Datatilsynet mottok i meldingsåret henvendelser fra tillitsvalgte når det gjaldt lovligheten av at arbeidsgiver benytter systemer for evaluering av de ansattes arbeidsutøvelse, i form av rene karakterfastsettinger. Disse karakterfastsettingene bygger

på subjektive vurderinger fra nærmeste leders side, med liten grad av påvirkningsmulighet for arbeidstaker.

Etter Datatilsynets vurdering er det naturlig at det i forbindelse med medarbeidersamtalene foregår en dialog mellom den ansatte og nærmeste leder omkring arbeidsinnsats og resultatoppgjør. Imidlertid kan Datatilsynet ikke se at det foreligger saklig begrunnelse for å ta i bruk systemer hvor nærmeste leder gir subjektive karakterfastsettelser på en skala fra *eksepsjonelt bra* til *bør gis sparken*. Bruk av denne typen rene karaktersystemer i arbeidslivet vurderes derfor til å være i strid med personopplysningsloven.

#### Utlevering av lønnsopplysninger – igjen

I 2001 avgjorde Datatilsynet at arbeidsgiver på generelt grunnlag, og uten samtykke fra arbeidstaker, ikke kan utlevere lønnsopplysninger til tillitsvalgte i forkant av lønnsforhandlingene. Unntak fra dette er utlevering med grunnlag i offentlighetsloven, eller utlevering av opplysninger til arbeidstakers egen arbeidstakerorganisasjon.

Datatilsynets vurderinger i saken ble ikke godt mottatt av arbeidstakersiden, blant annet når det gjelder de tillitsvalgtes muligheter til å kontrollere at arbeidsgiver ikke bryter ufravikelighetsprinsippet. Prinsippet innebærer at ingen skal forskjellsbehandles fordi de er uorganisert, eller er organisert i et annet forbund enn sine kolleger.

Høsten 2003 ble saken igjen tatt opp fra LOs side i møter med Datatilsynet. LO la i møtene fram nye momenter som Datatilsynet vil ta med i en ny vurdering av saken. En ny avklaring ventes å foreligge tidlig i 2004.

## 4 Andre temaer

### 4.1 Terror- og kriminalitetsbekjempelse

Personvern blir i stadig mindre grad et rent nasjonalt anliggende fordi vi i økende grad påvirkes av andre land og kulturer. Dette gjelder fremfor alt fra USAs side. Svært mye av hva amerikanerne pålegger seg selv og sine gjester i krigen mot terror, får også en bestemmende innflytelse på våre egne, nasjonale disposisjoner når det gjelder bruk av personopplysninger, og vern av privatlivets fred.

De amerikanske tiltakene synes også å ha vært til inspirasjon for norske myndigheter som dels bruker kampen mot terror som begrunnelse for å samle inn og gjøre bruk av stadig flere personopplysninger om oss alle.

### USAs krav om utlevering av passasjeropplysninger

Kort tid etter 11. september 2001 vedtok amerikanske myndigheter enkelte nye lover som innebærer at flyselskaper som flyr til USA må gi de amerikanske toll- og immigrasjonsmyndighetene tilgang til passasjerlister og bookinginformasjon fra sine reservasjonssystemer. Det vil på denne måten bli samlet inn personopplysninger for mer enn 10 millioner passasjerer pr. år.

Disse PNR-dataene (*Passenger Name Record*) inneholder opplysninger om blant annet passasjerens navn, adresse, reiserute, hvem vedkommende reiser sammen med, bestemmelsessted, fakturaadresse, telefonnummer og betalingsmåte. I tillegg kan det også være registrert ønsker om spesialmat eller medisinsk assistanse, det vil si opplysninger som iht. personopplysningsloven og EUs personverndirektiv er sensitive.

Opplysningene skal lagres i amerikanske databaser og vil bli sammenliknet med informasjon i andre databaser før de reisende kommer inn i USA. Opplysningene kan i noen grad også leveres ut til andre føderale organer.

Flyselskaper som ikke følger amerikanernes krav risikerer å ikke få landingstillatelse i USA.

Flere europeiske flyselskaper har allerede underlagt seg kravene fra USA, selv om overføringen av personopplysningene strider mot det europeiske personverndirektivet og nasjonal personvernlovgivning. Også flyselskapet SAS fikk opprinnelig en frist på 30 dager til å tilpasse seg de amerikanske kravene, men denne fristen ble senere utsatt.

I slutten av desember kom det til en midlertidig forhandlingsløsning mellom representanter for USAs departement for innenlandssikkerhet og EU-kommisjonen, som blant annet innebærer at:

- listen over PNR-data som skal overføres er blitt redusert fra det opprinnelige kravet på alle de ca. 50 elementene, til maksimalt 34
- sensitive personopplysninger (rase, tro, helse mv.) skal så langt mulig filtreres ut og slettes
- lagringstiden er blitt begrenset fra det opprinnelige kravet på 50 år til 3,5 år. Dette tilsvarende for øvrig også den midlertidige avtalens varighet.
- bruk av opplysningene skal begrenses til bekjempelse av terror og internasjonal organisert kriminalitet
- representanter for datatilsynsmyndigheter i Europa kan rette henvendelser til departementet for innenlandssikkerhet på vegne av EU-borgere som mener at deres klager ikke har blitt tilfredsstillende håndtert fra amerikanernes side



- amerikanerne, sammen med representanter for europeiske myndigheter, vil ha en årlig gjennomgang av avtalevilkårene faktisk blir gjennomført
- avtalen er midlertidig for en periode på 3,5 år. Partene er enige om at det innen den tidsrammen er nødvendig å arbeide frem et internasjonalt avtaleverk som flere berørte land eventuelt kan slutte seg til.

Også flere andre såkalte tredjeland stiller tilsvarende krav overfor flyselskapene. Dog har for eksempel Australia vist at det likevel er mulig å ivareta de fundamentale personvernprinsippene i noen grad, blant annet ved å ha sletterrutiner for overflødig informasjon.

#### *Strider mot europeiske personvernprinsipper*

Europakommisjonens forhandlere har oppnådd vesentlige innrømmelser i forhold til de meget vidtgående kravene som opprinnelig ble fremsatt fra amerikanernes side. Imidlertid er det fra Datatilsynets side nødvendig å peke på at en overføring av passasjeropplysninger til USA, innebærer et brudd med helt sentrale personvernprinsipper i den europeiske og norske personvernlovgivningen.

USA er ikke blant de land som EU-kommisjonen har vurdert til å ha et forsvarlig nivå for behandling av personopplysninger. Det foreligger heller ikke tilstrekkelig med garantier for at det blir etablert uavhengige kontrollmekanismer i forhold til hvordan de amerikanske myndighetene faktisk behandler de personopplysningene som blir overført. Videre er det ikke etablert rettigheter som sikrer at de reisende kan få innsyn i hvilke opplysninger som faktisk er blitt registrert hos amerikanske myndigheter. Retten til innsyn, og ev. påfølgende retting av feilregistreringer, står helt sentralt i europeisk personvernlovgivning, men er i liten grad ivare tatt gjennom den foreløpige avtalen. Reisende kan dermed risikere å bli nektet innreise til USA, eller på andre måter oppleve ubehageligheter, basert på feil og mangler i de registrerte dataene.

#### *Internasjonale avtaler nødvendig*

Lufttrafikk er et internasjonalt fenomen. Selv om avtalen ikke er bindende for Norges del, har vi i praksis ikke annet valg enn å følge de avtalene som EU-kommisjonen inngår på vegne av EU-landene, dersom vi fortsatt skal ha flytrafikk fra Norge til USA. Slike spørsmål bør derfor løses gjennom internasjonale avtaler, fremfor at et enkelt land innleder prosessen med å sette ultimate krav, slik USA har gjort i denne saken.

#### *SAS må gi reisende informasjon*

Datatilsynet forutsetter at vårt eget flyselskap SAS ikke starter utlevering av PNR-dataene før etter at avtalen mellom EU og USA er implementert, og Norge deretter formelt har sluttet seg til denne. Videre må de reisende, i forbindelse med bestilling av reisedokumentene, bli informert om hvilke opplysninger som overføres og formålet med utleveringen. Man skal rett og slett gis mulighet til å kunne, i den grad det er mulig, velge å ikke gjennomføre reisen.

Det må også tilrettelegges for tekniske løsninger som innebærer at kun de relevante personopplysningene overføres til USA etter forespørsel, fremfor at amerikanske myndigheter gis direkte aksess til flyselskapenes registre.

#### **Biometriske ID-kort til sjømenn**

Med bakgrunn i en ILO-konvensjon er det bestemt at sjømenn skal få utstedt biometriske ID-kort som skal identifisere personen, i tillegg til å bekrefte at vedkommende virkelig er sjømann.

ID-kortet skal erstatte den nåværende sjøfartsboken. De biometriske dataene vil, i tillegg til bilde, bestå av den enkeltes fingeravtrykk omformet til et unikt nummer. Nummeret skal lagres både i ID-kortet og i en nasjonal database.

Konvensjonen kom som et resultat av den økte beredskapen mot terror og hensynet til nasjonal sikkerhet.

Datatilsynet har lite imot utstedelse av ID-kort inneholdende biometriske data. Når det samtidig skal opprettes nasjonale databaser med de samme biometriske data, vil imidlertid personvernetrussele øke. Når en slik samling med biometriske data først er tilgjengelig, vil andre instanser kunne ønske å bruke disse opplysningene også til andre formål. Av personvern hensyn bør den nasjonale databasen derfor ikke inneholde biometriske data. Datatilsynet kan dessuten vanskelig se at hvorvidt en person gjennom ID-kortet kan sannsynliggjøre at han virkelig er sjømann, er noen særlig garanti for at vedkommende ikke er med i et terrornettverk.

Regjeringen skal innen 19. juni legge frem sin anbefaling vedrørende ratifikasjon av avtalen overfor Stortinget.

#### **Toll samarbeid mellom Norge og Israel**

I forbindelse med en forestående avtaleinngåelse om tollsamarbeid mellom Norge og Israel, bad Finansdepartementet Datatilsynet å vurdere et forslag fra Israel om tilføyelser i avtaleteksten. Tilføy-

elsene gjaldt overføring av opplysninger også til andre formål enn rene tollsaker.

I utgangspunktet setter tollsamarbeidsavtalen strenge krav til at opplysningene bare skal brukes til å oppfylle selve avtalen. Ved eventuell annen bruk skal avgiverlandet konsulteres og gi samtykke til bruken. Det presiseres videre i avtalen at bruken ikke må være i strid med nasjonal lovgivning.

Israels foreslåtte tilføyelser til tollsamarbeidsavtale innbærer imidlertid at personopplysningene også skal kunne benyttes i saker som berører nasjonal sikkerhet. I følge forslaget skal Norge ikke konsulteres dersom opplysningene tas i bruk i forbindelse med saker som kan innebære vesentlig skade for Israels økonomi, folkehelse, sikkerhet eller andre vitale interesser.

Datatilsynet mener at utveksling av opplysninger med nasjonal sikkerhet som formål, ligger så fjernt fra tollsamarbeid at tollovens bestemmelser om slikt samarbeid ikke oppfyller de krav som personopplysningsloven stiller til en klar lovhjemmel for utlevering av personopplysninger. Når bruken av personopplysninger innebærer en stor trussel mot enkeltmenneskers personverninteresser, er kravene til klar lovhjemmel strengere enn dersom trusselen mot personvernet er mindre.

Datatilsynet er selvsagt ikke imot at det inngås samarbeidsavtaler på tollområdet i tråd med internasjonale avtaler. Derimot ser Datatilsynet ikke noe grunnlag for å akseptere at opplysninger innsamlet av det norske tollvesenet skal brukes til annet enn tollrelaterte formål.

### **Forskrift om tiltak mot hvitvasking**

I årsmeldingen for 2002 omtalte Datatilsynet et forslag til lov om hvitvasking, som da hadde vært på høring. Datatilsynet uttrykte den gang at grunnlaget for loven var mangelfullt, idet verken kontrollbehovet eller sentrale personvern hensyn var drøftet og veid mot hverandre. Datatilsynet savnet også en nærmere redegjørelse for hvilke trusler som gjorde tiltaket nødvendig.

Datatilsynet måtte senere likevel konstatere at loven, slik den ble vedtatt, ikke avviker vesentlig fra Finansdepartementets opprinnelige høringsforslag.

I 2003 sendte Finansdepartementet så ut et utkast til forskrift om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. Datatilsynet kunne dessverre konstatere at det heller ikke ved forskriftsarbeidet er antydning noe om omfanget av de truslene det norske samfunnet er utsatt for, og som kan legitimere forslagene.

### *Store mengder overskuddsinformasjon*

I sin høringsuttalelse gav Datatilsynet uttrykk for at den utvidede rapporteringsplikten ville føre til store mengder med overskuddsinformasjon hos Økokrim. Økokrim har da også ved årsskiftet bekreftet at de i løpet av 2003 mottok nærmere fire tusen henvendelser om mulig hvitvasking, hvilket representerer tre ganger flere meldinger enn året før. Imidlertid har hele 90 prosent av meldingene blitt liggende urørt i Økokrims databaser. Politiet har ikke hatt de ressurser som er nødvendige for å nyttiggjøre seg meldingene som næringsdrivende, under trussel av sanksjoner, har vært pålagt å rapportere.

Datatilsynet hadde også vesentlige innvendinger til forskriftsforslaget når det gjelder rapporteringspliktiges undersøkelse av transaksjoner, elektroniske overvåkingssystemer, og mangel på rettigheter for de personene det rapporteres opplysninger om.

Hvitvaskingsloven og de tilhørende forskriftene trådte i kraft 1. januar 2004.

### **Forslag til valutareregistreringslov**

Finansdepartementet fremmet et lovforslag som er ment å sikre kontroll- og etterforskningsorganer fortsatt tilgang til opplysninger om valutavekslinger og pengestrømmer inn og ut av landet. Formålet er å forebygge og bekjempe økonomisk kriminalitet, og dermed også hindre finansiering av terrorisme. Dette skal oppnås gjennom et sentralt elektronisk register, med en samordnet rapportering til både kontroll-, etterforsknings- og statistikkformål. Registeret skal være direkte personidentifiserbart, og innebærer i praksis at all bruk av betalingskort i utlandet blir registrert.

Datatilsynet var i høringsuttalelsen negativ til forslaget som helhet. Etter Datatilsynets vurdering var det heller ikke i dette lovforslaget godtgjort at nytten av overvåkingen er proporsjonal med krenkelsen av lovlydige borgeres integritet og grunnleggende demokratiske rettigheter.

Det var i høringsnotatet lagt til grunn at registeret ikke vil inneholde sensitive opplysninger. Datatilsynet er uenig i dette, idet registrerte opplysninger kan knyttes til kjøp av eksempelvis apotekvarer, legebesøk og sykehusopphold. Det vil også kunne tenkes registrert opplysninger om seksuelle preferanser og straffbare forhold.

Etter Datatilsynets vurdering var det også foreslått en svært vid adgang til de registrerte opplysningene. Datatilsynet påpekte derfor nødvendigheten av å utarbeide klare retningslinjer for hvem

som skal ha tilgang til registeret, og når man skal kunne gjøre søk.

Det ble også foreslått unntak for den rett til innsyn i registeret som normalt følger av personopplysningsloven. Et slikt forslag oppfatter Datatilsynet som unødvendig og lite skjønnsomt. Det er ingen hensyn som tilsier at den registrerte ikke skal ha rett til innsyn i opplysninger om seg selv. Retten til innsyn er viktig for å sikre at opplysningene er korrekte.

### Ekomloven og lagringsplikt for trafikkdata

I forbindelse med Stortingets behandling av forslaget til lov om elektronisk kommunikasjon (Ekomloven), fant Datatilsynet grunn til å gjøre samferdselskomiteen oppmerksom på at tilsynet ikke hadde fått anledning til å vurdere forslaget til lovens § 2–8 om *tilrettelegging for lovbestemt tilgang til informasjon*. I en forskriftshjemmel åpnes det for at man kan pålegge teleoperatørene plikt til å lagre trafikkdata for en bestemt periode.

Etter Datatilsynets vurdering ble den foreslåtte forskriftshjemmelen utvidet etter at lovforslaget hadde vært ute på alminnelig høring. Datatilsynet ble dermed ikke gitt mulighet til, gjennom høringsdokumentene, å gi merknader til at forskriftshjemmelen også skulle innebefatte en mulighet til å pålegge lagringsplikt.

Kontroll av trafikkdata kan være et effektivt virkemiddel i forhold til kriminalitetsbekjempelse. Deler av påtalemyndigheten ønsker derfor å pålegge teleoperatørene en lengre lagringstid. Det vil innebære oppbevaring av såkalt overskuddsinformasjon til et annet formål enn det opprinnelige, som er at tjenestetilbyderne skal kunne fakturere for tjenestene de gir sine kunder.

### Formålsbestemthet

Det er et grunnleggende personvernprinsipp at opplysninger som er ment å skulle brukes til et formål ikke skal benyttes til andre formål. Når formålet er oppfylt, skal opplysningene slettes. Unntak fra dette er der den opplysningene knytter seg til samtykker til annen bruk, eller det finnes lovhjemmel.

Lagring av trafikkdata ut over det som er nødvendig for gjennomføring av tjenesten, vil bety at det lagres mange trivielle opplysninger om mange abonnenter. Store mengder informasjon om en hel befolknings bruk av elektronisk kommunikasjon vil bli lagret, for at en liten del som gjør noe kriminelt skal kunne etterforskes mer effektivt. Dette rokker ved den grunnleggende rett det er å kunne bevege

seg fritt uten at man blir iakt tatt, slik det også går fram av menneskerettighetene.

### Bør bestemmes direkte i lov

Datatilsynet gav overfor samferdselskomiteen uttrykk for at en lagringsplikt vil være et så inngripende virkemiddel at dette bør besluttes i lovs form, og ikke gjennom en svært vid forskriftshjemmel. Datatilsynet oppfordret også til at man burde avvente innstillingen til datakrimutvalget, som vil drøfte en eventuell lagringsplikt.

### Hyppige endringer i utlendingslovgivningen

Datatilsynet har vært høringsinstans i forbindelse med mange forslag til endringer i utlendingslovgivningen. Enkelte av forslagene har vært motivert ut ifra ønske om å motvirke kriminalitet. I løpet av 2003 mottok Datatilsynet hele 15 høringsbrev fra Kommunal- og regionaldepartementet. I tre av de utsendte endringsforslagene var høringsfristen imidlertid satt så kort at det i praksis var umulig å avgi noen uttalelse. Dette finner Datatilsynet bekymringsfullt, da forslagene ved en slik fremgangsmåte ikke blir tilstrekkelig belyst.

Tilsynet har også reagert på at de hyppige endringene på feltet skjer parallelt med at et lovutvalg (utlendingslovutvalget) arbeider frem en ny utlendingslov. Som høringsinstans er det vanskelig å danne seg et inntrykk av den samlede effekten av de foreslåtte endringene, når fragmenter av lovverket til stadighet foreslås endret. I sum vil dette skape en uoversiktlig situasjon, som kan gå på bekostning av viktige demokratiske prinsipper som forutsigbarhet, rettssikkerhet og likebehandling.

### Registrering og dokumentasjon i forbindelse med politikontroller

Stortinget fattet i 2002 et vedtak der Regjeringen ble bedt om å «*fremme forslag om en kvitteringsordning for politiet som sikrer at personer som visiteres får en kvittering på stedet, hvor type kontroll, dato for kontrollen, tid, sted og tjenestenummer til den som kontrollerer, framgår av kvitteringen*». Hensikten med ordningen skulle være å sikre at politiet likebehandler alle grupper i samfunnet, og at politiets kontakt med publikum blir registrert.

Politidirektoratet utredet saken, og deres rapport ble sendt på høring.

Datatilsynet hadde ingen sterke oppfatninger av hvorvidt det forelå et behov for slik registrering og dokumentasjon som ble drøftet i rapporten. Tilsynet var imidlertid noe forundret over at arbeids-

gruppen ikke var bredere sammensatt. Dersom flere interesser hadde vært representert i arbeidsgruppen, ville man muligens også fått en klarere oppfatning av behovet for de tiltak som ble drøftet.

Videre advarte Datatilsynet mot registrering av enkeltindivider dersom formålet er å sikre politiets likebehandling av alle grupper i samfunnet. For det første bør en kvalitetssikring av politiets arbeid kunne gjennomføres ved at det registreres anonyme eller statistiske opplysninger. For det andre kan en registrering på identitet virke mot sin hensikt, idet det vil kunne virke mistenkelig i seg selv dersom en person hyppig er registrert i forbindelse med politikontroller. Man risikerer på den måten en stigmatisering av enkeltpersoner, selv om det motsatte var intensjonen med tiltaket.

### Sikkerhetsklarering mot terror

Forsvarsdepartementet sendte høsten 2003 et forslag til endring i sikkerhetsloven, og en tilhørende forskrift om objektsikkerhet, på høring.

Forslaget innebærer blant annet at flere personer må sikkerhetsklareres, og at behovet for adgangskontroll og kameraovervåking øker.

Datatilsynet pekte i høringsuttalelsen på en rekke forhold som etter tilsynets mening ikke er tilstrekkelig vurdert av arbeidsgruppen. Dette gjelder i særlig grad forslaget om økt bruk av sikkerhetsklarering. Bruk av sikkerhetsklarering har tidligere vært knyttet til hvorvidt vedkommende skal kunne få tilgang til skjermingsverdig informasjon. Å utvide bruken av sikkerhetsklarering til også å gjelde alle personer som vil kunne få adgang til skjermingsverdige objekter, innebærer at betydelig flere personer enn tidligere må finne seg i å bli gransket i detalj, for eksempel i en jobbsøkersituasjon. Skjermingsverdige objekter vil for eksempel si en rekke offentlige bygninger, oljeinstallasjoner mv. Prosessen med sikkerhetsklarering innebærer en forpliktelse for den enkelte til å formidle detaljer om privatlivet til klareringsmyndigheten, herunder helseproblemer, økonomiske vanskeligheter og eventuelle ungdomssynder.

I tillegg til at muligheten til å legge negative forhold i sin fortid bak seg begrenses, kan økt bruk av sikkerhetsklarering også føre til at personer med utenlandsk statsborgerskap, eller personer som har utenlandsk ektefelle, i praksis får yrkesforbud i forhold til store deler av arbeidslivet. Dette fordi utenlandske statsborgere som utgangspunkt ikke gis sikkerhetsklarering.

### 4.2 Kameraovervåking

Stadig flere iverksetter kameraovervåking, og oftere enn før velges det digitale opptaks- og lagringsløsninger. Utviklingen forsterkes ved at tilbydere av overvåkingskameraer driver en aggressiv markedsføring. Dette er særlig observert innen utelivsbransjen. Overvåkingstiltakene begrunnes som regel med at kameraovervåking skal virke preventivt i forhold til hærverk og voldsepisoder.

Det ble i 2003 gjennomført syv operative tilsyn knyttet til kameraovervåking. Det observeres en økende bruk av såkalte "doom-kameraer". Dette er fjernstyrte kameraer med 360 graders dekningsområde og som regel også med zoom-funksjon. I tillegg er kameraene lite synlige for publikum. Oslo City er eksempel på et område hvor slike doom-kameraer benyttes. Kameraene er plassert slik at de ikke bare dekker fellesområdene i kjøpesenteret. De kan også benyttes til å zoome inn aktiviteter i de enkelte utsalgsstedene.

De digitale overvåkningssystemene befester sin stilling i markedet. Dette skyldes både systemenes brukervennlighet og funksjonalitet, men også at den digitale teknologien stadig blir billigere. I en kleskjede var det installert web-kameraer på mange av utsalgsstedene, hvor bilder ble overført til hovedkontoret. Et uanmeldt tilsyn ble gjennomført etter at en fagforeningsrepresentant gjorde Datatilsynet oppmerksom på at de ansatte opplevde dette som integritetskrenkende. Datatilsynet varslet at kameraovervåkingen, slik den var innrettet i forhold til de ansatte, måtte stanses umiddelbart.

Datatilsynet kom ved tilsyn også over to tilfeller hvor det var iverksatt kameraovervåking i forrommet til kundetoalettene. Da dette er en type sted hvor de fleste forventes å ha et ekstra behov for diskresjon, gav Datatilsynet pålegg om at overvåkingen skulle opphøre.

#### *Mer kunnskap og engasjement er nødvendig*

Tilsynene har avdekket at mange av de virksomhetene som tar i bruk kameraovervåking har et lite reflektert forhold til formålet med overvåkingen, i tillegg til hvilket ansvar og hvilke plikter man påtar seg i forhold til personopplysningsloven. Et synlig tegn på dette er at svært mange ikke har meldt fra om kameraovervåkingen til Datatilsynet. Meldeplikten er den letteste av alle bestemmelsene i personopplysningsloven å etterleve. Brudd på meldeplikten er derfor en indikasjon på at ledelsen i virksomheten heller ikke har satt seg inn i det øvrige regelverket omkring kameraovervåking.

For å gjøre informasjon om regelverket mer tilgjengelig vil Datatilsynet utarbeide et nytt veiledningsmaterieell om kameraovervåking. Her skal de som har planer om å sette opp overvåkingsutstyr få hjelp til å gjøre de nødvendige vurderinger, før de eventuelt iverksetter tiltaket.

Datatilsynet skulle gjerne se at det var en større interesse for personvern på lokalplan, og ønsker derfor å bidra til tiltak som kan vitalisere debatten i kommunene om bruk av kameraovervåking på offentlige steder.

### 4.3 Direkte markedsføring

#### Reservasjonsregisteret

Stadig flere benytter seg av muligheten til å reservere seg mot direkte markedsføring pr. brev eller telefon gjennom reservasjonsregisteret i Brønnøysund. I løpet av 2003 økte antallet reserverte med nær 250 000, og ved utgangen av året var 599 425 reserverte. Av disse har over 99 prosent reserverte seg mot markedsføring pr. telefon. Selv om det er mulig å unnta reservasjon for markedsføring fra humanitære organisasjoner, er dette en mulighet som i liten grad blir benyttet. Bare 13 prosent av de reserverte har gitt en åpning for at humanitære organisasjoner likevel kan ta kontakt.

Datatilsynet mottar ukentlig om lag 50 henvendelser om at reservasjonen ikke respekteres. Dette gjelder i alt overveiende grad direkte markedsføring pr. telefon. I mange av tilfellene viser det seg å være naturlige forklaringer på hvorfor reservasjonen ikke har fungert. Dette kan for eksempel være fordi den reserverte ikke har meldt flytting i folkeregisteret, eller at ikke alle i husstanden har reserverte seg. Imidlertid kommer det dessverre også kreative forklaringer fra selgers side på hvorfor man likevel har tatt kontakt. Det påstås gjerne at reservasjonen kun gjelder for ett år av gangen, eller at det er feil i registrene hos Brønnøysund. Ofte vises det også til at det foreligger et løpende kundeforhold.

#### *Løpende kundeforhold – hva er det?*

Har man et løpende kundeforhold til en person, slipper markedsfører å sjekke reservasjonsregisteret. Dette fordi lovgiver har antatt at slike kundeforhold ofte må sidestilles med et samtykke til å motta markedsføringshenvendelser og annen kundeinformasjon. Lovgiver har ikke definert begrepet, men peker i forarbeidene på avtaleforhold av mer langvarig karakter, eksempelvis bank- og forsikringsavtaler og abonnementer. Hva som kan regnes som et løpende kundeforhold i bransjer der denne type av-

taler stort sett er fraværende, for eksempel hos ideelle organisasjoner, er imidlertid vanskeligere å definere.

Det skal likevel mer til enn å kjøpe lodd to til tre ganger i løpet av et år for å etablere et løpende kundeforhold til en ideell organisasjon. Det må ligge en eller annen form for avtale i bunn, der man aksepterer å motta denne type henvendelser.

Etter at Datatilsynet høsten 2003 utarbeidet en ny fortolkning av hva som ligger i begrepet løpende kundeforhold, kom det inn massive protester fra bransjen. Markedsførerne hevder at den nye fortolkningen vil ødelegge inntektsgrunnlaget for bransjen. Datatilsynet mener på sin side at tolkningen er relativt vid, sett i forhold til at det i lovforarbeidene sies at unntaket skal gjelde langvarige og permanente avtaleforhold.

#### Kundeforhold når du ikke kan velge?

Datatilsynet fikk en periode inn flere klager fra tidligere kunder i Telenor. De mottok markedsføringshenvendelser fra selskapet på tross av at de hadde reserverte seg i reservasjonsregisteret.

Telenor hevdet at selskapet hadde et løpende kundeforhold også til personer som hadde gått over til en konkurrerende leverandør av teletjenester. Dette fordi Telenor fortsatt er eier og leverandør av nettaksessen, dvs. selve kabelen som telefontrafikken går i.

Datatilsynet er imidlertid av den oppfatning at de kundene som selv aktivt har valgt å si opp sitt telefonabonnement hos Telenor, ikke lenger kan sies å ha et løpende kundeforhold til virksomheten, selv om nettet eies av Telenor. Når det gjelder aksessleverandør har den enkelte ikke noe valg. Ved å gå fra Telenor til en annen tjenesteleverandør, har kundene imidlertid gitt uttrykk for at de ikke lenger ønsker å ha et kundeforhold til selskapet.

Datatilsynet påla derfor Telenor å stoppe sin direkte markedsføring mot tidligere kunder som har reserverte seg i reservasjonsregisteret.

#### Utleie av adresselister

Utleie av adresselister har en sentral plass i direkte markedsføring, og innebærer at en virksomhet leier ut sin adresseliste til en annen virksomhet for bruk i markedsføring, som hovedregel gjennom en mellommann; adressemekleren.

I 2003 ble nye retningslinjer for adressemekling formidlet til berørte parter, og lagt ut på tilsynets nettside. En langvarig og stort sett etablert praksis er opprettholdt i disse retningslinjene.

### Kort om retningslinjene

Dersom adresselistene bare inneholder såkalte grunndata, det vil si navn, adresse, telefonnummer og fødselsdato, trenger markedsførerne ikke å innhente samtykke fra de registrerte. Videreformidling av adresselister inneholdende opplysninger om barn under femten år, eller hvor opplysningene kan indikere sensitive forhold, er ikke tillatt uten samtykke.

Selv om det i de fleste tilfellene ikke er nødvendig med samtykke fra den enkelte, har virksomheten plikt til å opplyse kundene sine om at formidling av personopplysninger vil skje, og hva slags opplysninger som formidles. Dette skal gi forbrukeren mulighet til å reservere seg lokalt hos den enkelte virksomhet.

Den som leier adresselistene skal alltid sjekke listene opp mot reservasjonsregisteret før bruk, slik at de som har reservert seg ikke mottar uønsket markedsføring. Når forbrukerne mottar direkte markedsføring har de også krav på å få vite hvor opplysningene er hentet fra, uten aktivt å måtte be om det.

## 4.4 Samferdsel og teknologi

Informasjonsteknologi benyttes i stadig større utstrekning på flere områder innen samferdselssektoren. På en rekke områder er det, eller planlegges det, etablert systemer som gjør at den enkeltes bevegelser i trafikken registreres. Som reisende legger man dermed igjen mange spor etter seg, enten man benytter bil eller andre transportmidler.

Ved hjelp av elektroniske billetterings- og betalingsystemer, GPS, videokameraer osv., vil detaljerte opplysninger om den enkeltes bevegelser kunne være tilgjengelige, f.eks.:

- geografisk lokalisering (hvor er du?)
- tidspunkt (når er du der?)
- reisemåte (hvordan kommer du deg dit?)
- handlemåte (hva gjør du der?)

Ofte er registreringen begrunnet i gode formål. I Samferdselsdepartementets IKT-strategi *Fra A til B... Bedre, tryggere og mer effektiv transport – med IKT (2002, N-0526)*, er det en uttalt målsetning at økt bruk av IKT innen samferdsel skal bidra til å gi bedre sikkerhet og kapasitetsutnyttelse på sektoren, i tillegg til å øke nytten for brukerne. Også økonomiske og miljømessige hensyn kan gjøre seg gjeldende. Men utviklingen reiser også problemstillinger av betydning for personvernet. Et økende krav om ulike former for registrering reduserer den enkeltes mulighet til å kunne ferdes anonymt i

samfunnet. Økt registreringsnivå med innsamling av store mengder personopplysninger på nye felter, øker også risikoen for at opplysningene kan komme på avveie eller misbrukes.

Det er Datatilsynets inntrykk at personvernhen-syn bare i begrenset grad er vurdert når nye tiltak etableres på samferdselssektoren. Datatilsynet har derfor satt i gang et prosjekt for å få en mer systematisk oversikt over registreringsomfanget på sektoren, herunder hvilke opplysninger som samles inn, og hvilke situasjoner det gjelder. Både eksisterende og planlagte tiltak skal omfattes. Det skal også foretas en nærmere vurdering av retten til anonym ferdsel. Prosjektet er planlagt ferdigstilt i februar 2004.

### Bomring – anonym mulighet?

Vegdirektoratet har hatt under utvikling en løsning for helautomatiske bomstasjoner, som i første omgang er planlagt innført i Tønsberg og Bergen. Det var her lagt opp til to mulige betalingsformer, enten abonnement basert på AutoPass-brikke eller etter-skuddsfakturering basert på videoopptak av bilens registreringsnummer. Dette ville innebære at enhver passering av bomstasjonen ville bli registrert.

Datatilsynet mente at det må finnes sporingsfrie alternativer for passeringer i bomstasjoner i Norge slik at den enkelte har mulighet til å velge hvorvidt passeringsopplysninger skal registreres. Retten til i størst mulig grad å kunne ferdes fritt uten å legge igjen spor eller bli registrert, er et av de av grunnleggende personvernprinsippene både nasjonalt og internasjonalt.

Etter innspill fra Datatilsynet har Vegdirektoratet startet arbeidet med å utvikle et alternativt betalingsystem som skal gjøre det mulig å passere bomringen anonymt.

### RFID – små sladrebrikker med store muligheter

Radio-frequency identifikasjon (RFID) er en gammel teknologi som er i ferd med å få vid utbredelse. RFID er brikker som sender informasjon om seg selv etter forespørsel, slik at enheten brikken er festet på kan identifiseres unikt. Disse brikkene kan ha mange utforminger og funksjoner. Vanlig bruk i dag er brikker innebygd i bilnøkler som en elektronisk startspærre, og brikker til bruk i bomringer. RFID er i ferd med å etablere seg som en erstatning for de tradisjonelle strekkodene for logistikkformål. I detaljhandelen vil det for eksempel være mulig å gi hvert enkelt produkt en unik kode, i motsetning til dagens praksis hvor det er produktgruppen som identifiseres.

Sett fra et personvernmessig synspunkt medfører RFID-brikkene muligheter til å følge med uten at den som kontrolleres nødvendigvis er klar over det. Identitetskort eller pass med RFID-teknologi plassert i lommeboken vil kunne gi beskjed til en kontrollpost selv, slik at innehaveren ikke får vite at ID-kortet ble sjekket. Et klesplagg merket med en RFID brikke vil kunne identifisere seg, og kanskje dermed også sin bærer, så lenge klesplagget eksisterer.

Bevisst bruk av RFID for å kontrollere personer blir også vurdert benyttet i ulike situasjoner. Det kan for eksempel være merking av pasienter og ansatte på et sykehus for å holde rede på hvor den enkelte befinner seg. Dette er en bruk av teknologien som i noen få, avgrensede tilfeller kan være akseptabel, men som i mange andre situasjoner vil innebære et uakseptabelt innhogg på våre personverninteresser.

På den internasjonale konferansen for datatilsynsmyndigheter i Sydney ble det i meldingsåret vedtatt en resolusjon som omhandler RFID. I hovedsak ble det uttrykt en bekymring for mulighetene som ligger i systemet, og at personvernet må vurderes ved design av systemer som benytter RFID.

#### 4.5 Internett og personvern

Personlige forhold som bør tilhøre privatlivets fred er beskyttet i lov. Når de trivielle opplysningene blir mange, kan imidlertid summen av informasjon viske ut grensene mot det private. Datatilsynet har lenge snakket om profiler i forbindelse med handelsstandens innsamling av personopplysninger. Nå har profilverktøyene blitt bedre og bedre, og de er også blitt tilgjengelige for alle. Man kan nå danne seg et omfattende bilde av enkeltpersoner ved enkle søk på Internett.

Internett har en del særpreg i forhold til andre kilder for informasjon. Det er blant annet svært begrensede muligheter til å gi tilsvaret eller til å få slettet informasjon som er feilaktig. På de nettstedene der tilsvaret godtas, kan man heller ikke sikre at tilsvaret i alle sammenhenger følger med det opprinnelige utsagnet.

Ved publisering på Internett har man ingen garanti for at personopplysninger kun vil være å finne på det nettstedet de opprinnelig ble lagt ut. Opplysningene blir også kopiert, spesielt av store søkemotorer, og i praksis er det umulig å vite hvor de blir lagret for senere, ubegrenset bruk.

Dette betyr at opplysninger som publiseres på Internett i praksis finnes der langt utover den tiden de ligger på sitt opprinnelige nettsted. Det er ikke bare mulig, men også sannsynlig, at kommersielle,

historiske databaser vil ha et marked i fremtiden.

Ingen kontroll med egne personopplysninger, manglende tilsvaretsrett og fraværende slettemuligheter er problematisk i forhold til grunnleggende personvernprinsipper.

De aktuelle Internett-kildene for informasjonssøk er mange, og problemstillinger i tilknytning til noen av disse kildene til informasjon har på ulike måter vært aktuelle for Datatilsynet i meldingsåret. I de påfølgende artiklene får man en oversikt over de mest sentrale Internett-relaterte sakene fra meldingsåret, delt inn i det offentliges dokumenter og privates hjemmesider.

#### Det offentliges dokumenter på nett

Datatilsynet ser en trend når det gjelder regjeringens og forvaltningens ønske om å ta i bruk Internett. Ønsket om tilgjengelighet og samtidsorientering er så sterkt at man begynner i feil ende: Først bestemmer man at de aktuelle opplysningene skal være tilgjengelige via Internett, og så utreder man konsekvensene. I de verste tilfellene er det ikke vurdert hvorvidt publisering på Internett fører til behov for nye begrensninger eller premisser. Personvernet er det rettsgodet som må vike.

Om offentlige organer publiserer hele dokumenter i saker som skulle ha vært taushetsbelagte, kan konsekvensene bli meget store. Tusenvis av potensielle mottakere har tilgang til opplysningene med en gang, både i inn- og utland, og det offentlige har mye informasjon om saker som er av vanskelig, personlig og privat karakter.

#### Konkursregisteret på Internett

Justisdepartementets forslag til endringer i konkursloven og konkursregisterforskriften vil medføre til dels store endringer i forhold til dagens tilstand der kun noen få opplysninger er publisert på Internett. Forslaget legger opp til at alle stadier av bobehandlingen skal gjøres kjent via Internett, og at registeret skal være tilgjengelig for alle, uten begrensninger. Publisering av konkursregisteret i sin helhet innebærer en trussel mot personvernet i større grad enn før. Opplysningene som er publisert i dag er færre, og de er også underlagt en viss beskyttelse, blant annet krav om passord og identifikasjon av etterspøreren.

Datatilsynet mente at tiltaket som ble foreslått hadde uforholdsmessige ulemper i forhold til formålet man ønsket å oppnå. Mens formålet var å redusere kostnadene ved bobehandlingen, ville man samtidig gi mer eller mindre fri tilgang for alle til konkursregisterets opplysninger.

Opplysninger om konkurs er som regel ikke opplysninger om straffbare forhold. Oppfattelsen blant folk flest er imidlertid en noe annen, og dette bør man ta hensyn til når slike opplysninger vurderes publisert på Internett. At opplysninger som lagres blir kopiert til andre nettsteder, og derfor ikke forsvinner når en forskrift måtte bestemme sletting, er også en faktor man må ta med i vurderingen.

### Skattelister

I Norge har de offentlige skattelister lang tradisjon. Skattelister har vært lagt ut til årlig gjennomsyn i mer enn 100 år. De siste årene har utleggingen imidlertid fått et nytt preg. Diverse nettsteder og nettaviser har valgt å la skattelister ligge tilgjengelige hele året i søkbar form. I 2003 kom et forslag til innstramminger i praksisen med videreformidling av opplysningene.

Datatilsynet har ved flere anledninger gått inn for innstramming i bruk av skattelister.

I meldingsåret kom Finansdepartementet med innstramminger i bruken av likningsopplysningene, og et lovforslag som kan føre til at spredningen begrenses noe.

Finansdepartementet uttrykte i høringsbrevet bekymring for den enorme spredningen likningsopplysningene har fått de siste årene, en problematikk som også Skattedirektoratet hadde kommunisert inn til departementet. Departementet viste blant annet til at opplysningene ble brukt av kriminelle til å peke ut ofre, og at listene i noen grad ble brukt til uønskede kommersielle formål.

Departementet besluttet at det fra og med høsten 2003 skulle være en forutsetning for å få skattelister at opplysninger om fødselsdag og -måned, skatteklasser samt gateadresse, ikke skulle offentliggjøres. I tillegg ble det satt en begrensning på videreformidling på tre uker, samme tidsrom som papirlister ligger til gjennomsyn på ligningskontoret. I lovforslaget la departementet opp til at det kun var Skattedirektoratet som skulle tilby skattelister til publikum over Internett.

Datatilsynet mente at forslagene var ønskelige og nødvendige, men at endringene også muligens forutsatte en for stor grad av normlojalitet.

Medio desember i meldingsåret hadde flere aviser fremdeles skattelister utlagt, flere uker etter at de i følge retningslinjene fra Finansdepartementet skulle tatt bort opplysningene fra Internett. I VG ble man for eksempel lovet å få utlevert opplysninger fra skattelister ved hjelp av sms mot betaling, Bergens Tidende gav likningsopplysninger fra 2000, 2001 og 2002, og Romerikes Blad hadde søkemuligheter i skattelister for 2002.

### Sosialsaker

I meldingsåret publiserte stiftelsen Lovdata dokumentene fra den såkalte Svanhild-saken, en sak der en ung mor ble fratatt foreldreansvaret for to små barn. Navn og adresser ble slettet fra dokumentet før publisering. Dette var i tråd med at barne- og familiedepartementet i 2002 bestemte at fylkesnemndenes vedtak for sosiale saker kunne legges ut på Internett dersom navn og enkelte andre opplysninger ble sladdet. Denne konkrete saken var etter Datatilsynets mening ikke godt nok anonymisert; hvem som helst i det avislesende Norge kunne forstå hvem det var snakk om.

Datatilsynet pekte på at det var nødvendig å bedre rutineene for anonymisering før offentliggjøring. Det ble også stilt spørsmål om det var etisk rett at norske myndigheter presset på for å offentliggjøre svært intime detaljer om mennesker i såpass spesielle situasjoner.

For å unngå at tilsvarende skulle skje i fremtiden, svarte departementet at de ville be lederne av fylkesnemndene vurdere om anonymiteten er tilstrekkelig ivaretatt i hver enkelt sak som skal sendes til Lovdata. Eventuell medieeksponering skal også inngå som en del av denne vurderingen.

### Departementenes postjournaler

I meldingsåret har Datatilsynet avgitt høringsuttalelse til et forslag fra Arbeids- og administrasjonsdepartementet om å legge postjournalene til departementer og direktorater åpent tilgjengelig for alle på Internett.

Det har betydning for personvernet når man nå vurderer å gå fra en ordning hvor pressen ble gitt tilgang til postjournalene etter å ha fått utdelt et passord, til å legge postjournalene ut på Internett slik at de uten videre blir tilgjengelig for allmennheten her og i andre land. Potensialet for spredning og misbruk er langt større i det siste tilfellet. Det er svært viktig at forvaltningen ikke innretter seg på et vis som gjør at befolkningen kvier seg for å ta kontakt med offentlige organer av redsel for at opplysninger om dem skal komme på avveie. Det er i denne sammenheng viktig å stille spørsmål om Internett er et egnet medium for oppfyllelse av offentlighetslovens intensjon. Dersom man velger en slik ordning, er det essensielt at befolkningen gis grundig informasjon om dette før ordningen igangsettes.

Datatilsynet mener at det er behov for en nærmere utredning av om det er mulig å opprette en kobling mellom den elektroniske postjournalen og de bakenforliggende dokumentene. Det ble i hø-



ringsuttalelsen understreket at en slik sammenkobling potensielt utløser stor fare for at personopplysninger kommer på avveie. Tilsynet ba også Justisdepartementets lovavdeling om å se på om en slik offentliggjøring av dokumenter ville falle inn under offentlighetslovens regler.

### **Gjelder personopplysningsloven ved utlegging av forvaltningens dokumenter på Internett?**

Datatilsynet sendte i meldingsåret en forespørsel til Justisdepartementets lovavdeling om tolkningen av personopplysningsloven i forhold til offentlighetsloven.

Personopplysningsloven skal ikke begrense innsynsretten etter offentlighetsloven. Men innsynsretten etter offentlighetsloven er knyttet opp mot en bestemt, avgrenset sak eller dokument: Den som ber om innsyn i en bestemt sak skal få det så sant ikke taushetsbestemmelsene som gjelder for saken, gjør at saken likevel ikke kan publiseres. Meroffentlighetsprinsippet sier i tillegg at forvaltningen skal vurdere om dokumenter som *kan* unntas likevel kan utleveres, for eksempel ved å sladde enkelte opplysninger.

Kan en offentlig instans, for eksempel en kommune, publisere fulltekstdokumenter på Internett kun i medhold av offentlighetsloven, og uten å måtte forholde seg til personopplysningslovens krav og rettigheter? Datatilsynet er av den oppfatning at offentlighetsloven gir rett til innsyn i spesifikke saker, men at loven ikke regulerer publisering av personopplysninger. Det ser for Datatilsynet ut som flere offentlige instanser praktiserer prinsippet om meroffentlighet på en slik måte at dokumenter som ikke er underlagt taushetsplikt, publiseres uten at offentliggjøringen vurderes i forhold til personopplysningsloven. Legges dette til grunn, vil det etter Datatilsynet oppfatning bare være taushetsplikten i særlover som regulerer hvorvidt opplysninger kan publiseres eller ikke. Datatilsynet antok i sin forespørsel at dette ikke var i samsvar med intensjonene i personopplysningsloven, og ba om Justisdepartementets vurdering.

Ved utgangen av meldingsåret foreligger ikke svaret fra Justisdepartementet.

### **Private hjemmesider, ikke helt private**

I en lovtolkningssak 6. november 2003 slo EF-domstolen fast at privatpersoners hjemmesider omfattes av personverndirektivet. En konsekvens av denne tolkningen er at flere hjemmesider på Internett som Datatilsynet til nå har sett på som rent private,

vil omfattes av direktivet, og dermed også av personopplysningsloven.

### *Lindqvist-dommen*

Bakgrunnen for Lindqvist-dommen var den svenske konfirmantlederen Bodil Lindqvists hjemmeside på Internett. Sidene inneholdt, i tillegg til opplysninger om Lindqvist selv, blant annet navn, arbeidsoppgaver og fritidsinteresser til flere av hennes kolleger. Det ble også omtalt at en kvinnelig kollega hadde skadet foten og derfor var delvis sykmeldt. De ansatte hadde verken fått informasjon om nettsidene, eller anledning til å samtykke i publiseringen på forhånd. Noen av de ansatte mislikte dette, og Lindqvist anmeldte seg selv til politiet for å få en gjennomgang av lovligheten av sine handlinger.

Lindqvist ble i *Eksjö tingsrätt* dømt til bøter for overtredelse av den svenske personvernlovgivningen. Begrunnelsen var at hun hadde behandlet personopplysninger elektronisk uten å ha meldt fra til den svenske *Datainspektionen*, at hun hadde behandlet sensitive personopplysninger uten at vilkårene for det forelå, og at hun hadde overført opplysninger til tredjeland.

Saken ble anket inn for *Göta hovrätt*, som forela spørsmålet om hvorvidt Lindqvists handlinger var i strid med bestemmelsene i EUs personverndirektiv for EF-domstolen.

Direktivet åpner for at privatpersoners behandling av opplysninger som ledd i rent personlige eller familiemessige aktiviteter, kan falle utenfor direktivets virkeområde. Den samme avgrensningen finner vi i den norske personopplysningsloven der det heter: *Loven gjelder ikke behandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål.*

### *EF domstolens tolkninger*

EF-domstolen slo fast at avgrensningen bare omfatter aktiviteter som gjelder den enkeltes privat- eller familieliv. Behandling av personopplysninger som blir offentliggjort på Internett vil derfor ikke falle inn under unntaket, fordi personopplysningene da blir gjort tilgjengelige for et ubestemt antall personer.

Domstolen kom også til at direktivet ikke er i strid med ytringsfrihetsprinsippet slik det er nedfelt i EMK artikkel 10. Domstolen understreket at grensen mellom ytringsfrihet og personvern i hvert enkelt tilfelle må trekkes opp av nasjonale myndigheter og domstoler. De nasjonale domstolene skal bruke de nasjonale bestemmelsene til gjennomføringen av direktivet, og sikre en rettferdig balanse.

Den enkeltes rett til ytringsfrihet må derfor i denne sammenhengen veies opp mot de registrertes rett til personvern.

Domstolen vurderte videre om publisering av personopplysninger på en hjemmeside i et medlemsland innebærer en overføring av opplysninger til tredjeland. Her ble konklusjonen at selv om opplysninger er *tilgjengelige* for personer i tredjeland, vil ikke det si det samme som at de er *utlevert* til tredjeland. Dette betyr at publisering av personopplysninger på Internett fra en server som ligger innen EU/EØS-området, ikke innebærer en overføring til utlandet i personopplysningslovens betydning.

#### *Konsekvenser av dommen*

Konsekvensene av dommen er at privatpersoner som lager hjemmesider med opplysninger om andre personer, må forholde seg til reglene i personopplysningsloven. Tolkningen reiser en lang rekke spørsmål, blant annet som nevnt om avgrensning mot ytringsfrihet, litterære og kunstneriske uttrykk, og om ansvarsforholdet ved publisering av personopplysninger. Dette er spørsmål Datatilsynet kommer til å starte arbeidet med i 2004.

#### **Bilder på Internett**

Digitale fotoapparater og mobiltelefoner med kamera har gjort det meget enkelt å ta bilder som kjapt kan legges ut på nettet. Bilder av personer defineres også som personopplysninger. Enhver som publiserer bilder av personer som direkte eller indirekte kan identifiseres, må derfor også forholde seg til personopplysningsloven. Datatilsynet formulerte i meldingsåret noen retningslinjer for publisering av bilder på Internett.

Mange glemmer at det man legger ut på Internett er tilgjengelig for millioner av brukere plassert over hele verden. Bilder som publiseres kan enkelt hentes og brukes i et annet land, og man har absolutt ingen oversikt over hvem som vil benytte disse til hva. Når bildene først er publisert kan de lastes ned av hvem som helst, og det hjelper lite å fjerne bildene fra hjemmesiden om man senere angres.

#### *Situasjonsbilder*

Situasjonsbilder kan defineres som bilder der selve situasjonen eller aktiviteten er det egentlige formålet med bildet. Akkurat hvem som er med på bildet er da mindre viktig enn hovedinnholdet i bildet. Utgangspunktet her er at situasjonsbilder kan offentliggjøres uten samtykke fra de avbildede så lenge

bildene er harmløse og ikke på noen måte krenkende for de som er avbildet. Det skal alltid foreligge en helhetsvurdering bak offentliggjøringen, der man vurderer formålet opp mot hensynet til de som er avbildet. I en slik helhetsvurdering er det viktig å tenke på at bildene heller ikke skal virke krenkende ut fra sammenhengen de benyttes i.

#### *Portrettbilder*

I portrettbilder er derimot hovedformålet å avbilde en eller flere bestemte personer. Hovedregelen er da at man alltid skal ha samtykke fra de avbildede før bildet legges ut på nett. Regelen er begrunnet i at en slik publisering vil kunne medføre ulemper for de som er avbildet da noen vil føle det ubehagelig at bilder, gjerne sammen med opplysninger om navn eller lignende, gjøres tilgjengelig for alle. Denne ulempen vil normalt veie tyngre enn interessen i offentliggjøringen. Det betyr at om man vil offentliggjøre bilder på sine hjemmesider, kan det bare skje om et samtykke på forhånd er innhentet fra alle de avbildede, eventuelt fra deres foresatte om de på bildet er under 15 år. Det er den som har publisert bildene som skal bevise at et frivillig, uttrykkelig og informert samtykke i den konkrete situasjonen virkelig foreligger.

#### **Kameramobiler**

Salget av mobiltelefoner med digitalt kameraer i ferd med å ta helt av. Bare her i Norge vil det ifølge elektro- og elektronikkbransjen ha blitt solgt nærmere 150.000 slike telefoner innen årsskiftet, og det er særlig hos ungdom i tenårene at kameramobilene er populære.

Datatilsynet ser med bekymring på potensialet for misbruk av disse telefonene. Årsaken er at kameraene er så diskrete at man uten større problem kan ta bilder i skjul. Bildene kan så spres via mms eller legges ut på nett bare ved noen få tastetrykk. Stadig flere TV-program arrangerer for eksempel diverse konkurranser der seerne skal sende inn bilder via mms, og bildene legges så enten ut på nett, eller vises i løpet av programmene. Det foreligger få retningslinjer for disse programmene utenom de selvpålagte etiske reglene. Er det sikkert at de som sender inn bilder av seg selv virkelig er de som er avbildet? Sjekkes det godt nok om de som er avbildet virkelig har godkjent at bildet offentliggjøres?

Ettersom disse kameramobilene stadig blir flere og mer vanlige, vil man se et økende behov for klare retningslinjer på området. Det fryktes misbruk av slike telefoner i blant annet dusjer, garderober og på offentlige toaletter, og det finnes eksem-

pler på skoler her i landet der kameramobiler er forbudt å ta med i svømmehallen. Kripos følger det økende problemet nøye, og har blant annet registrert bilder med erotiske og seksuelle motiver som er lagt ut på nettet etter brudd i forhold mel-

lom kjæresten. Flere land har allerede innført totalforbud mot å ta med mobiltelefoner i offentlige badeanlegg eller i treningsstudioer på grunn av faren for misbruk.

Tabell 1.2 Gjennomførte tilsyn 2003

Saksnummer	Tilsynsobjekt	Poststed	Kjerneområde	Bransje/sector
2003/0826	Taxisentralen i Bergen BA	Kokstad	Hordaland	Arbeidsliv
2003/0988	Norges Informasjonsteknologiske høyskole	Bekkestua	Akershus	Arbeidsliv
2003/1018	Komplett Data AS	Sandefjord	Vestfold	Arbeidsliv
2003/1021	Norsk Statistikk Markedsundersøkelser	Oslo	Oslo	Arbeidsliv
2003/1073	Oslo Taxi AS	Oslo	Oslo	Arbeidsliv
2003/1080	Computerland Norge AS	Kolbotn	Akershus	Arbeidsliv
2003/1126	Leatherman Drift AS	Oslo	Oslo	Arbeidsliv
2003/1415	Enter forsikring AS	Oslo	Oslo	Arbeidsliv
2003/1416	Elkjøp Norge AS – Callsenter	Lørenskog	Akershus	Arbeidsliv
2003/1417	Sparebank 1	Oslo	Oslo	Arbeidsliv
2003/1424	Hermelin Research AS	Halden	Østfold	Arbeidsliv
2003/1103	Vital Eiendomsforvaltning AS	Oslo	Oslo	Fjernsynsovervåking
2003/1104	Car Park – Oslo City	Oslo	Oslo	Fjernsynsovervåking
2003/1420	Sameiet Glasshuset AS	Bodø	Nordland	Fjernsynsovervåking
2003/1425	Radisson SAS Bodø	Bodø	Nordland	Fjernsynsovervåking
2003/1426	Cardinal AS	Bodø	Nordland	Fjernsynsovervåking
2003/1427	Coop Mega City Nord	Bodø	Nordland	Fjernsynsovervåking
2003/1855	Bergen Storsenter AS	Bergen	Hordaland	Fjernsynsovervåking
2003/1865	Finnegaarden AS	Bergen	Hordaland	Fjernsynsovervåking
2003/1987	Musikkbar Garman AS	Stavanger	Rogaland	Fjernsynsovervåking
2003/2004	Welhavensgate borettslag	Oslo	Oslo	Fjernsynsovervåking
2003/0827	Finansnæringens Hovedorganisasjon – sentralregister	Oslo	Oslo	Helsesektoren
2003/0909	Helse Finnmark HF, Hammerfest sykehus	Hammerfest	Finnmark	Helsesektoren
2003/0975	Sykehuset Buskerud HF	Drammen	Buskerud	Helsesektoren
2003/0976	Aker universitetssykehus	Oslo	Oslo	Helsesektoren
2003/0977	Sykehuset innlandet HF	Hamar	Hedmark	Helsesektoren
2003/1022	Statens vegvesen – Vegdirektoratet – Statens biltilsyn	Oslo	Oslo	Helsesektoren
2003/1081	Asker og Bærum HF – Blakstad sykehus	Rud	Akershus	Helsesektoren
2003/0854	Os kommune	Os	Hordaland	Kommune
2003/0902	Sarpsborg kommune	Sarpsborg	Østfold	Kommune
2003/0907	Kristiansund kommune	Kristiansund	Møre og Romsdal	Kommune
2003/0908	Hammerfest kommune	Hammerfest	Finnmark	Kommune
2003/0916	Froland kommune	Froland	Aust-Agder	Kommune
2003/0917	Gjerstad kommune	Gjerstad	Aust-Agder	Kommune
2003/0947	Bergen kommune	Bergen	Hordaland	Kommune
2003/0948	Steinkjer kommune	Steinkjer	Nord-Trøndelag	Kommune

## Datatilsynets og Personvernemndas årsmeldinger for 2003

Saksnummer	Tilsynsobjekt	Poststed	Kjerneområde	Bransje/ sektor
2003/0978	Nittedal kommune	Nittedal	Akershus	Kommune
2003/0987	Bodø kommune	Bodø	Nordland	Kommune
2003/0998	Halden kommune	Halden	Østfold	Kommune
2003/1072	Arendal kommune	Arendal	Aust-Agder	Kommune
2003/1394	Drammen kommune	Drammen	Buskerud	Kommune
2003/1395	Larvik kommune	Larvik	Vestfold	Kommune
2003/1397	Sande kommune	Sande	Vestfold	Kommune
2003/1398	Namsos kommune	Namsos	Nord-Trøndelag	Kommune
2003/1399	Overhalla kommune	Overhalla	Nord-Trøndelag	Kommune
2003/1400	Grong kommune	Grong	Nord-Trøndelag	Kommune
2003/1401	Vågen kommune	Svolvær	Nordland	Kommune
2003/1402	Nedre Eiker kommune	Mjøndalen	Buskerud	Kommune
2003/1403	Vestvågøy kommune	Leknes	Nordland	Kommune
2003/1405	Elverum kommune	Elverum	Hedmark	Kommune
2003/1406	Kongsvinger kommune	Kongsvinger	Akershus	Kommune
2003/1407	Stange kommune	Stange	Hedmark	Kommune
2003/1409	Fet kommune	Fetsund	Akershus	Kommune
2003/1410	Rælingen kommune	Fjerdingby	Akershus	Kommune
2003/1411	Sandnes kommune	Sandnes	Rogaland	Kommune
2003/1412	Sola kommune	Sola	Rogaland	Kommune
2003/1413	Strand kommune	Jørpeland	Rogaland	Kommune
2003/1414	Klepp kommune	Klepp	Rogaland	Kommune
2003/1422	Sortland kommune	Sortland	Nordland	Kommune
2003/0900	Norges Astma- og allergiforbund	Oslo	Oslo	Markedsførere
2003/1442	Catosenteret/Stiftelsen Sofienlund	Son	Østfold	Markedsførere
2003/1444	TV2 AS	Oslo	Oslo	Markedsførere
2003/1428	Hudklinikken	Oslo	Oslo	Primærhelsetjenesten
2003/1429	Lillestrøm Legesenter	Kjeller	Akershus	Primærhelsetjenesten
2003/1430	Søndre Frydenlund Legesenter	Sortland	Nordland	Primærhelsetjenesten
2003/1431	Robrygga legekontor	Namsos	Nord-Trøndelag	Primærhelsetjenesten
2003/1432	Byåsen legesenter	Trondheim	Sør-Trøndelag	Primærhelsetjenesten
2003/1433	Din doktor	Trondheim	Sør-Trøndelag	Primærhelsetjenesten
2003/1434	Fagerborg-legene	Oslo	Oslo	Primærhelsetjenesten
2003/1436	Centrum fastlegegruppe	Oslo	Oslo	Primærhelsetjenesten
2003/1438	Lege Cato A. Guldberg	Stavanger	Rogaland	Primærhelsetjenesten
2003/0000	Central Schengen Information System	Strasbourg	Strasbourg	SIS kontroll
2003/1892	Vestfold Politidistrikt	Tønsberg	Vestfold	SIS kontroll
2003/1404	Stokmarknes Sykehus	Stokmarknes	Nordland	Større helseforetak
2003/1421	Akershus Universitetssykehus HF	Norbyhagen	Akershus	Større helseforetak
2003/1439	Haraldsplass Diakonale sykehus	Bergen	Hordaland	Større helseforetak
2003/1440	Betanien Hospitalet	Fyllingsdalen	Hordaland	Større helseforetak
2003/1441	Jæren Distriktpsikiatriske senter	Bryne	Rogaland	Større helseforetak
2003/1418	Chess Communication AS	Bergen	Hordaland	Telekom

## Vedlegg 2

# Personvernemndas årsmelding for 2003

## 1 Sammendrag

Dette er Personvernemndas (PVNs) tredje årsmelding. I løpet av året er det kommet åtte klager, hvorav seks er ferdigbehandlet. Nemnda begynner å få et visst erfaringsgrunnlag. Klagesakene er selv sagt konkrete, men flere av dem har likevel vært prinsipielle.

I de i alt åtte sakene som kom inn til PVN i 2003, er Datatilsynets vedtak omgjort helt eller delvis i to av sakene. Blant klagesakene vil det naturlig nok være en forholdsvis stor andel som det knytter seg tvil til tolkningen av bestemmelsene i personvernlovgivningen eller de vurderinger de forutsetter. PVN søker å ha for øyet at de konkrete vedtakene også skal bidra til en avklaring av gjeldende rett.

## 2 Innledning

PVN er opprettet med hjemmel i lov om behandling av personopplysninger (2000:31). Loven trådte i kraft 1. januar 2001 og PVN skal behandle klager på vedtak som Datatilsynet fatter etter personopplysningsloven. PVN skal også behandle klager på vedtak som Datatilsynet fatter etter helseregisterloven (2001:24).

Personvernemnda er et uavhengig forvaltningsorgan administrativt underlagt Kongen og Arbeids- og administrasjonsdepartementet.

PVNarbeid reguleres av personopplysningsloven, forskrifter til denne, samt en instruks som Arbeids- og administrasjonsdepartementet har utarbeidet. Forvaltningsloven og offentlighetsloven kommer også til anvendelse som for forvaltningen for øvrig.

Selv om Arbeids- og administrasjonsdepartementet utarbeider instruks, innebærer dette ikke noen form for instruksjonsmyndighet i enkeltsaker. Departementet kan ikke gi generelle instruksjoner om lovtolkning eller skjønnsutøvelse.

Personvernemnda skal årlig orientere Kongen om behandling av klagesakene.

## 3 Oppnevning av medlemmer

Personvernemnda har syv medlemmer som oppnevnes for fire år med adgang til oppnevning for ytterligere fire år. Første gangs oppnevning skjedde i 2001. Personvernemndas leder og nestleder oppnevnes av Stortinget, mens de øvrige medlemmer utnevnes av Kongen.

PVN består av følgende personer:

Jon Bing, leder

Gro Hillestad Thune, nestleder

Per Anders Stalheim

Dag Elgesem

Siv Bergit Pedersen

Sidsel Røgde

Hanne I Bjurstrøm

I tillegg er det oppnevnt personlige vararepresentanter.

## 4 Øvrige organisatoriske forhold

PVN holder sine møter i lokaler utenfor Datatilsynet og Regjeringskvartalet for også på denne måten å markere uavhengighet. AAD utlyste og gjennomførte en anbudskonkurranse for oppdraget som PVNs sekretariat. Kontrakt ble tildelt advokat Camilla Sivesind Tokvam, og gjelder for ett år med mulighet for fornyelse for ytterligere et år.

Personvernemnda har egen hjemmeside, [www.personvernemnda.no](http://www.personvernemnda.no), hvor blant annet vedtakene er publisert. Hjemmesiden har lenke fra Datatilsynets hjemmeside, og lenker til personvernrelatert materiale tilgjengelig på Nettet.

I 2003 har PVN arbeidet med et prosjekt for sikker e-post utveksling mellom medlemmene og sekretariatet. Prosjektet forventets ferdigstilt i mars 2004, og innebærer at alle saksdokumenter oversendes elektronisk.

## 5 Møter og seminar i 2003

PVN har i 2003 hatt i alt syv møter. Møtene ble i hovedsak nyttet til å behandle klagesaker, men også

administrative forhold som arbeidsform og saksbehandling, samt vurdering av budsjett og budsjettforslag for 2004 har blitt behandlet i møtene. I tillegg til nemndmøter har det vært forberedende møter med sekretariat og en eller flere medlemmer, samt enkelte tilsvarende møter i forbindelse med behandling av klagesaker.

PVN har hatt to møter med AAD.

PVN arrangerte seminar 10. oktober hvor tema var «Personvern og helseopplysninger».

Seminar tok sikte på å belyse enkelte sider av bruk av personopplysninger i helsesektoren og til medisinsk forskning. Det var ca. 50 deltagere. Programmet var som følger:

- Professor dr. juris Erik Boe (Institutt for offentlig rett, Universitetet i Oslo) «Helseregisterloven – historikk og forventninger»
- Professor Aslak Syse (Institutt for offentlig rett, Universitetet i Oslo) «Moderne bioteknologi og rettslig regulering. Forskningens behov og individets beskyttelse. Etske og juridiske grenser»
- Førstemanuensis dr. juris Lee A Bygrave (Institutt for rettsinformatikk, Universitetet i Oslo) «Personopplysninger og biologisk materiale»
- Direktør Frøydis Langmark (Kreftregisteret) «Medisinsk forskning og behovet for personlige opplysninger».

## 6 Klagesaksbehandling

PVN behandlet i 2003 totalt åtte klagesaker. Seks av disse var ferdigbehandlet ved utgangen av året. Oversikt over vedtak, og vedtakene selv er lagt ut på PVNs hjemmesider, samt at vedtakene oversendes elektronisk til Datatilsynet som publiserer disse på egne hjemmesider.

Antallet saker i 2003 er det samme som i 2002. Erfaringene fra Justisdepartementet som var klageorgan under den tidligere personregisterloven antyder et årlig antall på ca 10 saker.

Saker som er behandlet i 2003 er:

**Sak nr. 1/2003:** Personvernemnda sluttet seg til Datatilsynets vurdering at hvis man baserte et sentralt låneregister på samtykke av de registrerte, ville registeret knapt møte kravet til datakvalitet i personregisterloven § 11, 1.ledd litra d og e. Personvernemnda mente at å gjøre samtykke til en forutsetning for å få lån, ville gjøre at samtykket ikke ville møtet kravet i personregisterloven § 2 nr 7 om bl.a. frivillighet. Personvernemnda antok at etablering av et slikt sentralt register vanskelig kan etableres uten hjemmel i lov.

**Sak nr. 2/2003:** Klager var registrert i Sentralkartoteket for alvorlig sinnslidende (»Psyko-

registeret») med Riksarkivaren som behandlingsansvarlig. Bakgrunnen for registreringen var en frivillig innleggelse med diagnosen «depressiv nevrose». Personvernemnda kom til at klagen måtte behandles etter personopplysningsloven, ikke helseregisterloven. Personvernemnda fant at registreringen var å betegne som sterkt belastende for den registrerte etter personopplysningsloven § 28. Etter en vurdering av forholdet til samfunnsmessige interesser kom Personvernemnda til at hele innførselen i registeret angående den registrerte måtte slettes. Dissens (5–2). Datatilsynets vedtak ble omgjort.

**Sak nr 3/2003:** I forbindelse med boligadresseringsprosjektet innførte Statens kartverk et attributt i registeret over grunneiendom, adresse og bygning (GAB) kalt «boligtype». Dette ble innført fordi et annet attributt i registeret, «bygningstype», i sin definisjon anga hvor mange boliger bygningen hadde. Særlig for boliger oppført før 1983 var det en viss inkonsistens mellom denne definisjonen og det antall boliger som faktisk fantes i bygningen. Boligadresseringsprosjektet hadde bl a som formål å tildele en unik adresse til hver bolig, og det var derfor nødvendig at GAB reflekterte det antall boliger som bygningen faktisk inneholdt. Av praktiske og tekniske årsaker, innførte derfor Statens kartverk et nytt attributt i GAB (uten samtidig å endre GAB-forskriften tilsvarende). Stavanger kommune utnyttet disse opplysningene ved samkjøring med andre registre for å identifisere ulovlige boliger. Personvernemnda finner at opplysningene avgitt til boligadresseprosjektet med formål å utarbeide statistikk og forbedre kvaliteten på enkelte registre, bl.a. GAB, ikke kan benyttes til slike kontrollformål, jf. personopplysningsloven § 11. 1.ledd *litra* c. Datatilsynets vedtak om å forby slik bruk av opplysningene opprettholdes.

**Sak nr 4/2003:** Klager ønsket slettet opplysninger om seg selv i en journal ført i forbindelse med en barnevernjournal. Klager var ikke selv part i saken, men opptrådte av og til på vegne av parten, som var klagers barn. Selve barnevernsaken gjaldt klagers barnebarn. Journalen var omfattende (nær 400 dokumenter) og klager påpekte en rekke opplysninger som ble hevdet å være uriktige, f.eks. hvordan klagers adferd ble oppfattet på møter, tidspunkter for møter og telefoner mv. Personvernemnda manglet grunnlag for å vurdere hva som var uriktige opplysninger, og gjennomføringen av sletting ved overstrykning i papirdokumenter ville være praktisk vanskelig. Dokumentene var også relevante i en barnevernssak som på vedtakstidspunktet ikke var avsluttet, jf. personopplysningsloven § 27, 2 ledd. Personvernemnda opprettholdt

Datatilsynets vedtak om at klagers anførsler skulle supplere journalen, slik at vedkommende som ser journalen, vil kunne gjøre seg kjent med klagers fremstilling. Nemnda presiserte vedtaket dit hen at to brev til nemnda med kommentarer også skulle supplere journalen, forutsatt at klager samtykket i dette.

**Sak nr 5/2003:** Spørsmål om konsernkunde-register skal kunne inneholder opplysninger om produkttype. Datatilsynet tillater at registeret inneholder opplysninger om produktkategori (betalingsformidling, spare- og innskuddsprodukter, lån og kredittgivning), men ikke produkttype (f.eks. at lånet er et fastrente lån). Personvernemnda peker på at en endring i gjeldende praksis vil ha store praktiske konsekvenser, ettersom registrene da må endres. Spørsmålet vil bli lovregulert på grunnlag av NOU 2001:23 *Finansforetakenes virksomhet*, og lovproposisjon ventes i løpet av våren 2004. På denne bakgrunn omgjør Personvernemnda Datatilsynets vedtak og tillater inntil videre fortsatt registrering av produkttype i konsernkunderegisteret. (ferdigbehandlet i 2004)

**Sak nr 6/2003:** Norsk Rikstoto ønsket å bruke fødselsnummer for identifikasjon av spillere. Etter personopplysningsloven § 12 kan fødselsnummer bare brukes «når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering» I likhet med Datatilsynet fant Personvernemnda at det forelå saklig grunn for sikker identifisering, men – også i likhet med Datatilsynet – at den metoden som ble benyttet ikke ga sikker identifisering. Jf. klagesak 07/2002. Klagen ble ikke tatt til følge.

**Sak nr. 7/2003:** Spørsmål om Tuberkuloseregisteret regelmessig skal påføres opplysninger fra UDI for å sikre kvaliteten på opplysningene. Tuberkuloseregisteret er et sentralt register opprettet i medhold av lov. Personvernemnda anser at vurderingen om innhenting av opplysninger må foretas i henhold til denne loven, og at det er et prinsipielt spørsmål som Helsedepartementet må vurdere, og eventuelt hjemle ved endringer i forskriften for registeret. Datatilsynets vedtak opprettholdt. (ferdigbehandlet i 2004)

**Sak nr 8/2003:** Krav om omgjøring av Personvernemndas vedtak i klagesak 08/2002 – Ullevål sykehus, avvist.

Vedtakene er lagt ut på PVNs hjemmeside, <http://www.personvernemnda.no>. Inntrykket av klagesakene er at selv om de alle er konkrete, kan man likevel peke på to hovedsaker.

For det første er enkelte av årets saker av prinsipiell karakter. PVN peker her særlig på sak 2/2003, som angikk sletting av opplysninger fra det såkalte «Psykoseregisteret», og hvor Riksantikvaren er behandlingsansvarlig. Sak 3/2004 gjaldt bruk av opplysninger fra Boligadresseinnhentingprosjektet av en kommune til kontroll, og belyste forholdet til de gjeldende forskriftene. Sak 7/2003 gjaldt overføring av opplysninger fra UDI for å sikre kvalitet i Tuberkuloseregistret, her henviste PVN til at dette måtte ordnes ved endring av de forskrifter som gjelder for registeret.

For det andre har det gjort inntrykk på PVN det betydelige engasjement som den enkelte klager legger i saken. Dette understreker hvordan den enkelte kan føle sitt personvern krenket, og den betydning det vern som loven gir har i praksis. PVN peker her på sak 2/2003 om det såkalte «Psykoseregisteret» og sak 4/2003 om opplysninger i en barnevernjournal.

## 7 Regskap og budsjett for 2003

Personvernemnda hadde i 2003 en budsjetttramme på 1,2 mill kroner, og fremkommer under kap 1500 Arbeids- og administrasjonsdepartementet i statsbudsjett for 2002.

Totalt forbruk: kr 864.766. Personvernemnda disponerte sin bevilgning til innkjøp av nødvendig litteratur, utstyr, tjenester, gjennomføring av seminar, deltagelse på konferanse for tilsynsmyndigheter, arbeidsgodtgjørelse og reisegodtgjørelse til nemndas medlemmer, godtgjørelse til sekretariat og leie av møtelokaler.

For Personvernemnda

Jon Bing, leder