



DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT

Meld. St. 5

(2010–2011)

Melding til Stortinget

Datatilsynets og Personvernemndas årsmeldinger for 2009





DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT

Meld. St. 5

(2010–2011)

Melding til Stortinget

Datatilsynets og Personvernemndas
årsmeldinger for 2009

Innhold

1	Fornyings-, administrasjons- og kirkedepartementets innledning.....	5	Vedlegg	
			1	Datatilsynets årsmelding for 2009 11
			2	Personvernemndas årsmelding for 2009 46
2	Fornyings-, administrasjons- og kirkedepartementets merknader til Datatilsynets årsmelding for 2009.....	7		
3	Fornyings-, administrasjons- og kirkedepartementets merknader til Personvernemndas årsmelding for 2009.....	9		
4	Administrasjon og ressurser	10		



DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT

Meld. St. 5

(2010–2011)

Melding til Stortinget

Datatilsynets og Personvernemndas årsmeldinger for 2009

*Tilråding fra Fornyings-, og administrasjons- og kirkedepartementet av 15. oktober 2010,
godkjent i statsråd samme dag.
(Regjeringen Stoltenberg II)*

1 Fornyings-, administrasjons- og kirkedepartementets innledning

Personvern er en grunnleggende rettighet som beskytter den enkeltes personlige integritet og privatliv. Inngrep i enkeltindividets personlige integritet forutsetter lovhjemmel eller samtykke fra den det gjelder. EMK artikkel 8 setter også grenser for inngrep i den enkeltes rettssfære. Videre må det personlige integritetsvernet ses i sammenheng med våre rettsstatsverdier som legalitetsprinsippet, rettssikkerhet og ytringsfrihet. Disse grunnleggende verdiene utfordres blant annet i møte med bruk av IKT, som i større grad er fundert på samfunnsøkonomiske hensyn. En utfordring med økt bruk av teknologi i et personvernperspektiv, er muligheten til å samle inn, lagre og bruke personopplysninger i et omfang vi knapt kunne forestille oss for noen tiår siden. Det er lett å se at interesseavveininger mellom gode løsninger for fellesskapet og enkeltindividets krav på integritetsbeskyttelse kan være krevende. Det er derfor viktig at personvernutfordringer og -vurderinger settes på dagsordenen tidlig i planleggings- og utviklingsarbeid når det er behov for å benytte personopplysninger.

Norge er et foregangsland i Europa for bruk av IKT i samhandling mellom forvaltning og befolkning. Dette gir et godt grunnlag for også å bli et foregangsland for ivaretagelse av personvern og utvikling av personvervennlig teknologi.

Sikker identitetsforvaltning, gode autorisasjons- og loggløsninger, og et generelt høyt sikkerhetsnivå er viktige tiltak for å redusere negative konsekvenser ved bruk av personopplysninger. Ytterligere personvernutfordringer er knyttet til bruk av Internett med globale systemer som nødvendigvis krever avklaringer vedrørende landenes jurisdiksjon. Internasjonalt personvernarbeid på flere plan er derfor viktig.

Personvern har vært et hyppig tema i den offentlige debatt i løpet av meldingsåret. Mange er opptatt av å sikre retten til å ha kontroll over egne opplysninger og unngå massiv kartlegging av bevegelses- og handlemønstre samt våre personlige egenskaper og preferanser. Debatten dreier seg om avveiningen mellom personvern og andre viktige samfunnshensyn. Ut fra en rekke gode formål er det ikke vanskelig å argumentere for behovet for å benytte personopplysninger. Men det skal alltid foretas gode, helhetlige konsekvensvurderinger slik at den samlede effekten av ulike personverninngrep vurderes i forbindelse med hvert nytt inngrep, og veies opp mot fordelene man vil oppnå med tiltaket. Datatilsynet påpeker i sin årsmelding, at personverngarantiene i praksis vil smuldre bort med tiden dersom personvernet blir sett som en hindring som helst bør ryddes av veien. Det er viktig at personvernet har status som et gode med selvstendig egenverdi.

At personvern er fremtredende i media i så stor grad som det har vært i løpet av meldings-

året, viser at svært mange oppfatter temaet som viktig. Debatten bidrar til økt bevissthet om at personvernet utfordres fra flere hold. Dette vil kunne bidra til å sette personvernet inn i en større sammenheng, slik at nye inngrep ses i sammenheng med eksisterende inngrep. Ønske om et mer helhetlig perspektiv på personvernet var bakgrunnen for at Personvern-kommisjonen ble nedsatt, jf. St.meld.nr.17(2006-2007).

Den videre veien etter Personvernkommissjonens rapport

I arbeidet med oppfølgingen av Personvernkommissjonens rapport ønsker departementet å legge bedre til rette for en helhetlig tilnærming til personvernet. Målet er å ta tak i sektorovergripende problemstillinger og arbeide fram en omforent, tverrsektoriell strategi for å oppnå en mer helhetlig tenkning rundt personvernutfordringene. Eksempler på gjennomgripede problemstillinger er utfordringer knyttet til økende innsamling av elektroniske spor, tendenser til å lagre data i svært lang tid, rekkevidden av de registrertes samtykke og mangelfull tilgangskontroll. I sin utredning peker Personvernkommissjonen på betydningen av den teknologiske utviklingen. Departementet mener det bør utvikles gode teknologiske løsninger som kan medvirke til å redusere negative personvernkonsekvenser.

Som ledd i oppfølgingen av Personvernkommissjonens rapport bevilget departementet i meldingsåret midler til gjennomføring av særskilte prosjekter i regi av Datatilsynet. Det mest synlige av disse prosjektene har hittil vært opprettelsen av veiledningstjenesten og nettstedet *slettmeg.no*, som skal veilede og bistå publikum som opplever seg krenket ved tekst og bilder på Internett. Stadig flere opplever at de utsettes for krenkende atferd på nettet. Det er ikke alltid flere regler er best egnet til å håndtere denne type konflikter. Målet med prosjektet er derfor å etablere et lavterskeltilbud som kan veilede publikum i hvordan de for eksempel kan få fjernet eller gjort informasjonen utilgjengelig for andre.

Personvernundersøkelsene gjennomført i 2005 viste at det er gjennomgående liten kjennskap til og kunnskap om rettigheter og plikter i personvernregelverket blant norske borgere og virksomheter. Dette inntrykket bekreftes i Personvernkommissjonens rapport. I meldingsåret fikk Datatilsynet derfor også midler for å igangsette et arbeid for å bedre kjennskapet til og etterlevelsen av personopplysningslovens regler om informasjonssikkerhet og internkontroll, blant

annet gjennom bruk av personvernombudsordningen.

Personvern i det digitale samfunnet

Nye utfordringer oppstår som følge av en rask digital utvikling og stadig større bruk av digitale og sosiale medier. Eksempelvis er det i dag mer enn to millioner norske brukere på *Facebook*. Spørsmål om eierskap og tilgang til informasjon er viktig for de mange brukerne. Samtidig er jurisdiksjonsspørsmålet en kompliserende faktor. Bruk av sosiale medier på nett innebærer spredning av store mengder personopplysninger, samt en globalisering av de problemstillinger som oppstår i kjølvannet av digitaliseringen. Hvilket lands regler gjelder for bruk av opplysninger på nett når de er lagt ut av norske brukere på et amerikansk nettsted, men er tilgjengelige over praktisk talt hele verden? Og hvem skal føre tilsyn med at de reglene som gjelder, faktisk blir fulgt? Nye globale lagringsmetoder i form av blant annet *cloud computing* åpner enorme muligheter, men utfordrer også grensene for eierskap, bruk av og kontroll med informasjon.

I meldingsåret har spørsmålet om mulig implementering av EUs datalagringsdirektiv vært et tilbakevendende tema. Samlet gir spor fra mobil- og nettbruk, bruk av elektronisk billett i kollektivtrafikken, elektroniske bompasseringer og bruk av andre typer elektroniske betalingsmidler et svært detaljert bilde av borgernes bevegelser, atferd og preferanser. Det er viktig å sørge for at den enkelte i størst mulig grad sikres informasjon om og kontroll med bruken av disse elektroniske sporene.

Reduksjon av anonyme alternativer, i kombinasjon med at elektroniske spor i større grad registreres, medfører at personvernet utfordres.

Regelverksarbeid

På bakgrunn av at regelverket anvendes på en teknologi i rask utvikling, ble det ved vedtakelsen av personopplysningsloven i 2000, besluttet at det skulle foretas en etterkontroll av lovgivningen. Etterkontrollen var i løpet av meldingsåret på alminnelig høring, og både høringsnotatet og de eksterne utredningene foretatt av dr. juris Dag Wiese Schartum og førsteamanuensis dr. Lee Bygrave, pekte på behov for endringer i lovgivningen. Rapporten vedrørende spørsmål om bruk av fødselsnummer og biometri, bærer spesielt preg av at teknologien er under stadig utvikling og tydeliggjør behovet for et regelverk som tar høyde

for denne utviklingen. Det bør derfor være et mål at regelverk generelt er så teknologinøytralt som mulig. For tiden er både EUs personvernregelverk og vår nasjonale personopplysningslov, som bygger på EU-direktiv 95/46/EF, til revisjon. Ett av målene er å få et mer tidsmessig oppdatert regelverk som tar høyde for den teknologiske utviklingen. Samtidig er det nå 30 år siden OECDs personvernretningslinjer ble vedtatt, og også disse er satt under lupen med tanke på oppdatering.

Personvern reguleres imidlertid ikke bare i det sektorovergripende nasjonale og internasjonale personvernregelverket. I meldingsåret vedtok Stortinget blant annet ny politiregisterlov. Loven innebærer langt bedre regulering av politiets bruk av personopplysninger enn gammelt regelverk. Ikrafttredelse av regelverket forutsetter forskrifter som for tiden er under utarbeidelse. Når reglene trer i kraft, vil de innebære et bedret personvern for dem som registreres i politiets registre. I meldingsåret avga Metodekontrollutvalget sin rapport *Skjult informasjon – åpen kontroll*, inntatt i NOU 2009:15. Rapporten er nyttig i personvern-sammenheng ved at den gir en god oversikt over politiets bruk av skjulte, og personvern-inngripende, tvangsmidler. I meldingsåret ble også Medieansvarsutvalget nedsatt. Utvalgets mandat er å foreta en samlet vurdering av reglene om plassering av ansvar for ytringer, med sikte på å vurdere om det er grunnlag for et mer enhetlig system for plassering av ansvar. Utvalget skal herunder vurdere tiltak som kan sikre enkeltmenneskers personvern i møte med media. Også dette er et eksempel på at det foregår personvernrelatert arbeid av stor betydning for borgerne. Sektorreguleringen må spille sammen med det generelle personvernregelverket for å gi borgerne best mulig personvern.

2 Fornyings-, administrasjons- og kirkedepartementets merknader til Datatilsynets årsmelding for 2009

Helhetlige og tidlige personvern-vurderinger

Datatilsynet er bekymret for at personvernet svekkes som følge av mange enkeltstående tiltak, som går på bekostning av personvernet, og at personvernet tilsesettes som følge av marginale, ikkedokumenterte gevinster, eller av rene effektivitetshensyn. Tilsynet fokuserer på den samlede effekten av et stort antall nye personopplysnings-

behandlinger, mangelfull ansvars plassering, elektroniske spor, manglende sletting, større samhandling og færre anonyme alternativer. Departementet støtter tilsynet i at enkeltstående tiltak må ses i sammenheng med andre tiltak som får konsekvenser for personvernet. For å kunne foreta en reell forholdsmessighetsvurdering, vil en være nødt til å se på den samlede effekten av opptak/registrering og lagring av personopplysninger.

Datatilsynet peker videre på en tendens til at konsekvensen av innsamling og lagring av personopplysninger undervurderes, og at innskrenkninger i bruken av opplysningene og gode sikkerhetsløsninger vurderes som tilstrekkelig kompensasjon for lagringen. I likhet med tilsynet understreker departementet at innsamling og lagring av personopplysninger er et personverninngrep i seg selv. Ut fra Menneskerettsdomstolens praksis må forholdsmessighetsvurderingen foretas før innsamling og lagring av opplysninger finner sted, ikke først i tilknytning til spørsmål om bruken av opplysningene. Dette henger sammen med at personvern-vurderingene ikke kan foretas ut fra en forestilling om at lagringssystemene tilbyr total sikkerhet. Sikkerhetsrisiko knyttet til lagring av opplysninger vil alltid måtte være en del av vurderingen i forkant av en beslutning om å gjennomføre et tiltak som har konsekvenser for personvernet. Departementet ønsker i denne forbindelse å understreke betydningen av at vurderinger av personvernkonsekvenser foretas tidlig i en beslutningsprosess, noe også Personvernkommisjonen påpekte i NOU 2009:1 og som departementet selv peker på i sin veileder i vurdering av personvernkonsekvenser utgitt i 2008.

Teknologi og personvern

Teknologien setter i dag marginale grenser for lagringskapasitet, og det er ofte mer kostbart å slette opplysninger enn fortsatt å oppbevare dem. Til tross for stadig nye teknologiske løsninger, vil slettereglene i personopplysningsloven være avgjørende for hvor lenge opplysningene kan lagres; sletting skal skje når behandlingens formål er oppfylt. Dette ble i meldingsåret, som året før, påpekt i Datatilsynets årsmelding, og brudd på sletteplikten beskrives som den største og alvorligste enkeltutfordringen for personvernet. Når vi samtidig legger igjen store mengder elektroniske spor, og personopplysninger i økende grad utveksles mellom databaser, er resultatet at betydelige mengder opplysninger til enhver tid er lagret om hver av oss på svært mange steder uten at vi har kjennskap til det.

En ny lagringsmåte som har fått gjennomslag internasjonalt, er *cloud computing* der opplysningene ikke lagres ett definert sted, men derimot i den del av nettskyen der det til en hver tid er ledig kapasitet. Nettskyen kan enkelt beskrives som en rekke servere tilknyttet Internett. I denne nettskyen kan både virksomheter og private leie lagringskapasitet. Både økonomisk og kapasitetsmessig har *cloud computing* et stort potensial. Samtidig byr denne teknologien på mange utfordringer både teknisk og juridisk. Departementet vil følge utviklingen på området tett.

Datatilsynet peker på at datasystemer må bygges opp på en personvernvennlig måte. Det er ved utformingen av datasystemene at nivået for ivaretagelse av personvernet defineres. Tilsynet peker på at innebygde personverngarantier (*privacy by design*) er spesielt viktig når man har ambisiøse samordningsprosjekter som krever informasjonsflyt mellom flere parter. Departementet er enig i at det er viktig at sikre datasystemer er på plass før det iverksettes tiltak som får personvernkonsekvenser.

Velferd, forskning og helse

Datatilsynet har i stor grad vært engasjert i spørsmål vedrørende personvern og helse i meldingsåret. Det oppstår stadig nye utfordringer på dette området. Tilsynet har blant annet vært kritisk til enkelte sider av samhandlingsreformen, for eksempel forslag om tilgang til helseopplysninger på tvers av virksomhetsgrenser og etablering av fellesregistre i denne forbindelse. Tilsynet frykter det skjer en uthuling av taushetsplikten, og advarer sterkt mot at det åpnes for tilgang på tvers før tilstrekkelige interne sikkerhetsløsninger foreligger. Gode tekniske løsninger er avgjørende for å sikre at bare aktører med tjenstlig behov for opplysningene får tilgang. Datatilsynet viser til helseregisterlovens forarbeider, Ot.prp. nr. 5 (1999-2000), og peker på at forskriftsbestemmelser om særlige sikkerhetskrav for behandling av helseopplysninger må fastsettes i tett samarbeid med Datatilsynet. På dette grunnlag ønsker Datatilsynet å bli inkludert i arbeidet med forskrift om informasjonssikkerhet ved samhandling i helsesektoren.

Videre er tilsynet bekymret for en økning i antall personer som fremover vil kunne få direkte tilgang til pasientjournaler, samt en sentralisering av registrene hos Folkehelseinstituttet. Kombineret med nye unntak fra taushetsplikten, senest i forslag til ny helsepersonellov § 29 b om unntak

for formål som kvalitetssikring, administrasjon, planlegging eller styring, er Datatilsynet bekymret for utviklingen. Departementet er enig i at spredning av helseopplysninger kan være en utfordring for den nødvendige tilliten mellom pasient og helsearbeider. Fremover er det derfor viktig å legge til rette for å ivareta pasientenes tillit til helsetjenesten, slik at de ikke unnlater å oppsøke tjenestene i frykt for at helseopplysninger skal spres. Dette må ses i sammenheng med behovet for økt samhandling i helsetjenesten.

Lov om medisinsk og helsefaglig forskning som trådte i kraft 1. juli 2009, innebar store endringer for Datatilsynets arbeidsfelt. Loven innebærer at Datatilsynet ikke forhåndsgodkjenner medisinsk og helsefaglig forskning. De regionale komiteer for medisinsk og helsefaglig forskningsetikk innehar nå godkjenningskompetansen, og Datatilsynet uttrykker bekymring for at komiteenes tilknytning til forskningsmiljøene skal få innvirke på saksbehandlingen.

I løpet av meldingsåret ble det fremmet forslag om å etablere et sentralt register for hjerte- og karlidelser. Datatilsynet etterlyste en prinsipiell tilnærming til hjemmelsgrunnlaget for etableringen av slike registre. Etter tilsynets mening bør slike registre etableres med samtykke fra pasienten, alternativt må opplysningene være pseudonymiserte, eller på annen måte være underlagt et særlig vern. Datatilsynet ønsker større grad av selvbestemmelsesrett for de registrerte i stedet for et ensidig fokus på informasjonssikkerhet. Dette henger sammen med at personvern vurderingene må foretas i forbindelse med selve registreringen, som i seg selv er et inngrep i den personlige rettsfære.

Datatilsynet påpeker videre brudd på register- og personvernlovgivningen i to tilfeller hos Kreftregisteret, ett hos folkehelseinstituttet, ett i Colon Cancer bank samt ett hos NTNU i forbindelse med at pasientjournaler var på avveie. Manglene relaterte seg i stor grad til sviktende hjemmelsgrunnlag for behandlingene, og samtykke står sentralt i denne sammenheng. I alle sakene har det skjedd klare brudd på helseregisterloven. Departementet mener sakene sender signal om at Datatilsynet også i fremtiden bør arbeide for at personvern blir ivaretatt i helsesektoren og føre en tett dialog med helsemyndighetene. Departementet fremholder at det er mulig å ivareta personvern hensyn samtidig som man opprettholder et godt forskningsklima med mulighet for gode og viktige resultater.

Etterkontroll av personopplysningsloven

I løpet av meldingsåret var forslag til revisjon av personopplysningsloven på høring. Høringen besto av et høringsnotat fra Justisdepartementet samt professor Dag Wiese Schartum og førsteamanuensis Lee Bygraves «*Utredning av behov for endringer i personopplysningsloven*» og «*Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12*», samt Datatilsynets rapport fra 2005 om kameraovervåking. Datatilsynet gikk grundig inn i høringssaken og hadde omfattende merknader basert på erfaringer med det regelverket de er satt til å forvalte. Datatilsynet er, som tilsynsmyndighet og forvaltningsmyndighet, en svært sentral høringsinstans når det gjelder personvernlovgivningen.

For det første er deres erfaring at regelverket ikke er tilstrekkelig lett å forstå for aktører som må forholde seg til lovgivningen. Derfor ønsker tilsynet å få klarere fram at alle er bundet av regelverket, og de går inn for en viss omstrukturering av det. Tilsynet foreslår videre en tydeliggjøring av betydningen av behandlingsformål som avgrensningskriterium. Tilsynet ønsker også å styrke personvernet i møte med ytringsfrihet, slik at personvernet får større gjennomslagskraft utenfor ytringsfrihetens kjerneområde. Datatilsynet foreslår, som et tillegg til forslagene i høringssaken, at den behandlingsansvarlige pålegges varslingsplikt når en uautorisert utlevering av personopplysninger har funnet sted. Når det gjelder konsesjonsordningen, foreslår Datatilsynet at konsesjonsplikten opprettholdes som i dag, foruten at Datatilsynet gis adgang til å gi dispensasjon fra konsesjonsplikten. Datatilsynet la også vekt på at mindreåriges personvern må styrkes og at det er et særskilt behov for å avklare barns samtykkekompetanse. Datatilsynets erfaringer er av stor verdi for lovrevisjonen, og deres vurderinger vil være et nyttig verktøy i det videre lovrevisjonsarbeidet. Departementet har merket seg at de temaene Datatilsynet legger størst vekt på, langt på vei er sammenfallende med de temaene som får størst oppmerksomhet i internasjonale fora. Departementet fremhever i denne sammenheng betydningen av tilsynets deltakelse i internasjonale diskusjonsfora for vår nasjonale personvern-debatt.

Samferdsel

I løpet av meldingsåret har Datatilsynet ført tilsyn hos tre tilbydere av offentlig transport der det

sentrale temaet var elektronisk billettering. Det ble videre ført tilsyn hos Statens vegvesen for å kontrollere personvern ved strekningsvis automatisk kontroll (SATK). I tillegg gjennomførte etaten tilsyn hos to bompengeselskaper. Datatilsynet setter muligheten for anonym ferdsel høyt og mener det samles inn langt flere opplysninger enn nødvendig i samferdselssektoren. Departementet viser i denne forbindelse til at det er satt i gang et interdepartementalt arbeid der også Datatilsynet deltar, som har som mål å legge til rette for anonyme bompasseringer. Det er viktig å opprettholde prinsippet om at kun de opplysningene som er nødvendige for å oppnå formålet, skal lagres.

3 Fornyings-, administrasjons- og kirke departementets merknader til Personvernemndas årsmelding for 2009

Ny Personvernemnd ble oppnevnt i 2008, med funksjonstid fra 1. januar 2009. Advokat Eva I.E. Jarbekk, oppnevnt av Stortinget, etterfulgte professor Jon Bing som nemndas leder. Også flere av nemndas øvrige medlemmer og vararepresentanter var nye fra 2009. Det første funksjonsåret ble et arbeidskrevende år for nemnda, som fikk en betydelig økning i antall saker sammenlignet med tidligere år – 25 innkomne saker i 2009 mot seks i 2008. Den store saksmengden gjorde at nemnda ikke klarte å ferdigbehandle alle sakene i løpet av meldingsåret, og det gjensto ti saker til behandling ved utgangen av 2009. Nemnda mener den store økningen i antall saker kan ha sammenheng med Datatilsynets tilsynsobjekter, da enkelte bransjer/objekter i større grad enn andre ser seg tjent med å påklage Datatilsynets avgjørelser.

Til tross for den store saksmengden har Personvernemnda kun omgjort to av klagesakene og i de resterende ferdigbehandlede sakene opprettholdt Datatilsynets vedtak. Samsvar mellom Datatilsynets og Personvernemndas vurderinger gir Datatilsynet større faglig tyngde i deres fremtidige virksomhet. Mange av sakene har vært prinsipielle og av betydelig omfang. Etter departementets syn reflekterer både antall saker og deres kompleksitet at presset på personvernområdet øker i takt med samfunnets ønsker om å iverksette nye og inngripende tiltak.

Personvernemnda har kun myndighet til å avgjøre enkeltsaker, men møter i sin virksomhet en rekke vanskelige avveininger. Da de ikke selv kan reise rettspolitiske debatter, etterlyser de dette fra annet hold på flere områder. Et forhold

nemnda særskilt etterlyser, er forskriftsreguleringer framfor bruk av standardkonsesjoner og nevner i den forbindelse konsesjon for å drive kredittopplysningsvirksomhet. Departementet vil her vise til at personopplysningsforskriften vil bli gjennomgått når personopplysningsloven er revidert. I den forbindelse vil det kunne være aktuelt å vurdere det forholdet nemnda tar opp.

Blant sakene avgjort i 2009 trekker nemnda fram vedtakene om helseforskning, der de finner det bekymringsverdig at det later til å være en tendens til å forsøke å unngå varsling av forskningsobjekter og innhenting av samtykke. De viser til at det ligger en personverntrusel i den praksis som benyttes når regelverket neglisjeres med tro på at skaden enkelt kan repareres i ettertid. Tildeling av konsesjon i etterkant vil skape en uheldig presedens, og det er også tvilsomt om lovverket gir rom for en slik etterfølgende, reparerende konsesjon.

4 Administrasjon og ressurser

Datatilsynets budsjett og rammevilkår

Datatilsynet hadde i 2009 et disponibelt beløp på i overkant av kr. 29 millioner. I tillegg fikk Datatilsynet ekstrabevilgning for særskilte prosjekter på personvernområdet på til sammen kr. 5,1 mill. kroner. Sammenlignet med 2008 har budsjettet økt med ca. 1,5 mill. kroner i tillegg til de særskilte prosjektbevilgningene. De særskilte bevilgningene kom som en følge av problemstillinger påpekt av Personvernkommissjonen i NOU 2009:1, områder der departementet så behov for raskt å iverksette målrettede tiltak. Den generelle budsjettøkningen vil bidra til å styrke Datatilsynets rolle som personvernbeskytter, tilsyn og informasjonsyter.

Vesentlige deler av Datatilsynets budsjett går til å dekke lønnskostnader, som i alt omfatter 36 årsverk. Ti medarbeidere var i permisjon i løpet av hele eller deler av meldingsåret, og vikarer og ekstrahjelp måtte hentes inn som erstatning. Data-

tilsynet må som en landsomfattende virksomhet sette av deler av budsjettet til reisevirksomhet. Dette er utgifter som er nødvendige for å løse oppgaven som tilsynsmyndighet. Deler av kostnadene går også til å dekke internasjonal virksomhet. Datatilsynet deltar bl.a. i EUs artikkel 29-gruppe, som er EUs rådgivende organ i personvernspørsmål, samt enkelte av arbeidsgruppene knyttet til denne. Det finnes gode internasjonale fagmiljøer som fører diskusjoner om både nasjonale og globale problemstillinger. Å følge den internasjonale utviklingen er en forutsetning for å stå i spissen for et godt personvern på hjemmebane.

Personvernemndas budsjett og rammevilkår

Nemnda hadde i meldingsåret et budsjett på kr. 1,65 millioner. Totalt forbruk var på i underkant av kr 1,5 millioner. 12 nemndsmøter ble avholdt i løpet av meldingsåret. Naturlig nok har forbruket gått noe opp sammenlignet med 2008 i forbindelse med økningen i antall saker og møter.

Personvernemndas sekretariat består av en deltidsstilling. I løpet av meldingsåret ble sekretariatets kontor flyttet til Sandefjord. Nemnda er svært fornøyd med sekretariatsordningen, og flyttingen har ikke skapt praktiske problemer. Ny leder, nestleder og to nye medlemmer startet sin funksjonstid 1. januar 2009, etter at de forhenværende hadde avsluttet sin andre og siste mulige periode i 2008. Departementet vurderer Personvernemnda, med dens tekniske, medisinske, kommersielle og juridiske kompetanse, som godt egnet til å veie personvernensyn og andre viktige samfunnshensyn mot hverandre.

Fornyings-, og administrasjons- og kirke departementet

t i l r å r :

Tilråding fra Fornyings-, og administrasjons- og kirke departementet av 15. oktober 2010 om Datatilsynets og Personvernemndas årsmeldinger for 2009 blir sendt Stortinget.

Vedlegg 1

Datatilsynets årsmelding for 2009

Del I

1 Om Datatilsynet

Datatilsynet ble etablert 1. januar 1980 i samsvar med den daværende personregisterloven vedtatt i 1978.

Datatilsynet har til oppgave å beskytte den enkelte mot at personverninteressene krenkes gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvern hensyn som behovet for vern av personlig integritet og privatlivets fred. Datatilsynets virksomhet er regulert i Lov om behandling av personopplysninger av 14. april 2000 (personopplysningsloven) og Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) av 18. mai 2001.

Datatilsynet er et uavhengig forvaltningsorgan, administrativt underordnet Fornyings- og administrasjonsdepartementet. Uavhengigheten innebærer at departementet ikke kan gi instruks om, eller omgjøre Datatilsynets utøving av myndighet etter personopplysnings- eller helseregisterloven. Personvernemnda er klageinstans for Datatilsynets vedtak. Nemnda avgir sin egen årsmelding.

Datatilsynets oppgaver

Som en følge av at personopplysningsloven den 1. januar 2001 erstattet den tidligere personregisterloven, ble hovedtyngden av Datatilsynets arbeid flyttet fra forhåndskontroll til etterfølgende kontroll. Dette i form av tilsynsarbeid, informasjon og oppfølging av brudd på regelverket.

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 begrenses. Deltakelse i råd og utvalg er derfor en viktig del av Datatilsynets arbeid. Også som

høringsinstans i saker som kan ha en personvernmessig konsekvens har Datatilsynet innflytelse på samfunnsutviklingen.

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 kontrollerer Datatilsynet at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet. Datatilsynet bistår bransjeorganisasjoner med å utarbeide bransjevise adferdsnormer, og gir bransjer og enkeltvirksomheter råd om sikring av personopplysninger. Datatilsynet motiverer også til, og støtter virksomheter som på frivillig basis har oppnevnt et eget personvernombud.

Sist, men ikke minst, har Datatilsynet også en viktig ombudsrolle. 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. For å skape oppmerksomhet og interesse omkring personvernsspørsmål deltar Datatilsynet aktivt i den offentlige debatt og legger stor vekt på å praktisere merofentlighet.

2 Organisasjon og administrasjon

Datatilsynets budsjett og rammevilkår

Datatilsynets budsjett var i 2009 kr 29 020 000,-. I tillegg fikk Datatilsynet 4 948 000,- kroner for å etablere tre ulike prosjekter på personvernområdet. Prosjektene skal videreføres også i 2010 og 2011. Prosjektene retter seg mot personvern i skolen, personvern og informasjonssikkerhet i norske virksomheter (personvernombudsordningen) og etablering av en veiledningstjeneste som skal bistå publikum som opplever å få sitt personvern krenket på Internett.

Ca 75 prosent av det ordinære budsjettet dekket lønnskostnader, fordelt på 36 medarbeidere. 10 medarbeidere var ute i permisjon hele eller deler

av 2009, hvorav 7 i svangerskapspermisjon. Vikarer og ekstrahjelp ble tilsatt som erstatning for disse. To medarbeidere sluttet i virksomhetsåret.

Som tilsynsorgan skal Datatilsynet dekke hele landet, inklusive Svalbard, og gjennomføring av tilsyn medfører en del kostnader knyttet til reisevirksomhet. Dette gjelder også reisevirksomhet knyttet til Datatilsynets internasjonale engasjementet.

Organisasjon

Datatilsynet var i 2009 bemannet med 36 årsverk, som fordeler seg slik:

- Direktøren
- Juridisk avdeling: 16 medarbeidere. Fire av disse er jurister knyttet til Datatilsynets juridiske veiledningstjeneste, og betjener henvendelser per telefon og e-post ved siden av ordinær saksbehandling
- Tilsyns- og sikkerhetsavdelingen: 8 medarbeidere
- Administrasjonsavdelingen: 7 medarbeidere
- Informasjonsavdelingen: 4 medarbeidere

Datatilsynet vurderer kjønnssammensetningen fortløpende, og søker å ta hensyn til å rekruttere i forhold til denne om kvalifikasjonene ellers er like.

Datatilsynet har som mål å arbeide aktivt for at etaten til enhver tid gir kvinner og menn like arbeidsforhold og like muligheter til karriereutvikling og faglig utvikling. Gjennomsnittsalderen i Datatilsynet er for tiden 43 år for menn og 39 år for kvinner.

Gjennomsnittsalder totalt er 41år,

Datatilsynet ønsker å stimulere til et kulturelt og kompetansemessig mangfold i staben. Videre tilrettelegges det for en personalpolitikk som skal virke motiverende, og hindre utstøting av personer med nedsatt funksjonsevne. Datatilsynet er knyttet til avtalen om inkluderende arbeidsliv. Fokus har også i 2009 vært tiltak som forebygger belastningslidelser. Dette har vært tiltak knyttet til trening, ergonomisk veiledning og instruksjon om hensiktsmessig arbeidsteknikk.

3 Saksbehandling

Det ble journalført totalt 6 515 dokumenter i meldingsåret. Av disse var 3 305 innkomne og 2 945 utgående brev fra Datatilsynet. Resten var journalførte interne notater. Dette er omtrent på samme nivå som tidligere år.

Antallet nye saker som ble behandlet i tilsynet har gått ned i forhold til 2008. I 2009 ble det behandlet 1 553 saker hvor hovedvekten var ved juridisk avdeling. Nedgangen i antall skyldes at antallet henvendelser på e-post har økt betydelig. Spørsmål og svar av rent generell og veiledende karakter blir ikke journalført. E-posthenvendelser Datatilsynet må saksbehandle tas ut og journalføres og behandles på vanlig måte. Det er mye som tyder på at fordelingen, som den er i dag, gir et godt bilde av skillet mellom Datatilsynets publikumstjeneste og formelle saksbehandling. Veiledningstjenesten er bemannet med 4 årsverk, og har god responstid på henvendelser på telefon og e-post.

Konsesjoner

I meldingsåret ble det gitt 195 konsesjoner for behandling av personopplysninger. Av disse utgjorde bruk av personopplysninger i forskning godt over halvparten av søknadene. Helseforskningsloven trådte i kraft i 2009, og vi har merket at antallet konsesjonssøknader har avtatt. Datatilsynet har brukt en del tid og ressurser på kompetanseoverføring i anledning lovens ikrafttredelse. Antallet konsesjoner for banker, forsikringsselskaper samt kredittopplysningsvirksomheter er omtrent som tidligere år.

Meldeplikten

Meldeplikten innebærer at den som ønsker å sette i gang en behandling av personopplysninger skal orientere Datatilsynet senest 30 dager før behandlingen starter. Det er imidlertid en del unntak fra meldeplikten. Meldinger er gyldige i tre år, så blir de slettet fra databasen.

I 2009 kom det inn 3 778 nye meldinger om behandling av personopplysninger. Det var 800 flere enn i 2008. Totalt er det nå 9 292 meldinger i meldingsdatabasen, mot 8 640 året før. Det har med andre ord vært en økning i antallet nye meldinger. 3 126 meldinger ble i meldingsåret slettet fra databasen som utløpt på dato, mot 3 212 året før.

Høringer

Datatilsynet gav 162 høringsuttalelser i 2009, hvorav tilsynet hadde konkrete merknader til 87. En del av høringsuttalelsene var tidkrevende, blant annet høringen i forbindelse med etterkontroll av personopplysningsloven. Denne står nærmere omtalt i kapittel 9.

Klagesaker

I meldingsåret oversendte Datatilsynet 23 saker til Personvernemnda for videre klagebehandling. Det er en klar økning i forhold til året før hvor syv saker ble oversendt. Datatilsynet har i de sakene som er behandlet av nemnda fått medhold i langt de fleste. Datatilsynets erfaring er at de saker som blir oversendt til Personvernemnda ofte knytter seg til områder der lovgivningen er uklar, og hvor klager, så vel som Datatilsynet, ser seg tjent med å få en avgjørelse som klargjør rettstilstanden. En annen kategori saker er vedtak som oppleves som begrensende for den klagende part, men hvor han likevel velger å påklage, til tross for at rettstilstanden er relativt avklart.

Saksbehandling i tilknytning til internasjonale fora

Datatilsynet mottar en rekke forespørsler og spørreundersøkelser fra Artikkel 29-gruppen og de andre internasjonale fora tilsynet deltar i. I tillegg kommer en del henvendelser direkte fra de andre europeiske tilsynsmyndighetene. Det har i 2009, som i tidligere år, vært en del henvendelser av kartleggingskarakter der Datatilsynet mottar spørreskjemaer om ulike personvernemaer. Kartleggingen har ofte som mål å undersøke status fra hvert enkelt land for å se at alle har tilfredsstillende kontrollsystemer på områder der landene har likt regelsett. Andre henvendelser dreier seg om hvilken praksis det enkelte land har på nasjonalt nivå.

Les om Datatilsynets deltakelse i internasjonale fora i kapittel 5.

4 Deltakelse i offentlige råd og utvalg

Datatilsynet skal bidra til å fremme respekten for det enkelte samfunnsmedlems privatliv, særlig når det gjelder bruk av personopplysninger. Råd- og utvalgsarbeidet er et viktig middel for å nå dette målet.

I meldingsåret har Datatilsynet deltatt i følgende råd og utvalg:

E-valg – referansegruppe

Datatilsynet har deltatt med avdelingsdirektøren for juridisk avdeling i en departemental referansegruppe for vurdering og valg av fremtidig system for elektroniske valg. Referansegruppen har hatt

fire møter, hvor det siste i 2009 var en presentasjon av forskjellige alternativer for e-valg. E-valg er planlagt som forsøksordning for kommende kommune- og fylkestingsvalg.

Arbeidsgruppe for opprettelse av Offentlig elektronisk postjournal (OEP)

OEP er en felles, allmenn tilgjengelig internettbasert publiseringstjeneste for elektroniske postjournaler. Fornyingsdepartementet er ansvarlig for å lansere OEP. Direktoratet for forvaltning og IKT (Difi) har et forvalter- og administrasjonsansvar for tjenesten fra det øyeblikk tjenesten blir lansert.

Datatilsynet har i 2009 deltatt i den praktiske uttestingen av OEP. Løsningen skal etter planen lanseres i løpet av 2010.

Samarbeidsråd for helsesektoren

Rådet er opprettet av Sosial- og Helsedirektoratet med sikte på å koordinere arbeid med informasjonsteknologi i helsesektoren. Formålet med rådet er å styrke samarbeidet aktørene imellom, og med de sentrale myndigheter. Datatilsynet oppfatter rådet som et viktig forum, og deltar som observatør.

Bransjenorm for helsesektoren

Sosial- og Helsedirektoratet har i samarbeid med helsesektoren utviklet en bransjenorm for helsesektoren. Normen skal bidra til å harmonisere nivået i helsesektoren hva gjelder informasjonssikkerhet. Datatilsynet har bistått med råd og veiledning ved utforming av normen. Arbeidet med selve normen ble avsluttet september 2006, men det utvikles stadig tilhørende faktaark. En styringsgruppe, som Datatilsynet deltar i som observatør, har overtatt ansvaret for forvaltning av normen. Arbeidet består nå i å få en hensiktsmessig spredning og implementering av normen i sektoren. Dette skaper store utfordringer gitt sammensetningen av små, mellomstore og store aktører.

KIS – Koordineringsutvalget for informasjonssikkerhet

Utvalget består av representanter for sju departementer, Statsministerens kontor og ni direktorater. Opprettelsen av koordineringsutvalget er et ledd i gjennomføringen av Nasjonal strategi for informasjonssikkerhet. Arbeidet omfatter alminnelig IT-sikkerhet og spørsmål knyttet til rikets

sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Utvalget skal samordne videreutviklingen av IT-sikkerhetsregelverket, få frem felles standarder, normer, metoder og verktøy for IT-sikkerhet og sørge for samordning av tilsynspraksis. Utvalget skal også drøfte aktuelle risiko- og sårbarhetsspørsmål og bidra til koordinering av informasjonstiltak og beredskapsplanlegging. Mye av arbeidet i KIS delegeres til arbeidsgrupper. Datatilsynet har prioritert å være aktiv i disse arbeidsgruppene.

KOBI – begrepsapparat innen regulering av informasjonssikkerhet

Koordineringsutvalget for informasjonssikkerhet opprettet KOBI som en ny gruppe i 2006. Alle myndigheter som regulerer informasjonssikkerhet sitter i denne gruppen. Siktemålet er å lage en metode for klassifisering av informasjon med utgangspunkt i behovet for beskyttelse.

Koordineringsutvalget for E-forvaltning

Utvalget skal arbeide med samordning mellom forskjellige offentlige organer for å realisere IT-politisk plan. Møtene ledes av Fornyringsministeren. Arbeidet fokuserer på hvordan målene i planen kan realiseres, og hvordan de enkelte aktørene kan bidra.

NAFAL

NAFAL er et tilpasningsråd for sivil luftfart. Hovedtemaet i rådet er implementering av sikkerhetsløsninger på flyplasser. Innen denne tematikken reises en rekke spørsmål i forhold til personvern.

Internett- og abusegruppen

Gruppen er etablert av Post- og teletilsynet for at internettoperatører og andre interesserte parter skal kunne ha et forum for internettrelaterte spørsmål. I 2009 var følgende saker på agendaen:

- Bransjenorm mot spam
- IKT-trusselbildet
- Ulike tekniske forhold ved nettrafikk – blant annet IPv6 og status for knutepunktene for norsk internettrafikk (NIX og regionale IX-er.)

Ett møte ble avholdt i 2009.

5 Internasjonalt samarbeid

I likhet med deltakelse i norske offentlige råd og utvalg, er også deltakelse på internasjonale møter og arbeidsgrupper en viktig arena for å påvirke personvernutviklingen. EU er den viktigste premissleverandøren for fremtidige personvernrettslige normer og regler. Datatilsynet har derfor valgt å være deltaker i utvalgte arbeidsgrupper under artikkel 29-gruppen. De internasjonale møtene er også en arena for utveksling av synspunkter. Nedenfor er en oversikt over de internasjonale arbeidsgrupper og råd som Datatilsynet er representert i.

Artikkel 29-gruppen

Den norske personopplysningsloven reflekterer personvernprinsippene som er nedfelt i EU-direktivet om personvern. Datatilsynet deltar som observatør i arbeidsgruppen opprettet etter direktivets artikkel 29. Gruppen har som oppgave å drive frem koordinering og synkronisering av EU/EØS-landenes nasjonale personvernarbeid, med utgangspunkt i personverndirektiv 46/95. Gruppen har en rådgivende funksjon overfor Kommisjonen og står fritt til å tolke og konkretisere direktivets innhold. Datatilsynet deltar på møtene med direktøren og avdelingsdirektøren på juridisk avdeling. 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. Gjennom året har arbeidsgruppen blant annet sett på utfordringer med overføring av opplysninger om flypassasjerer til andre land. Datatilsynet stiller seg bak Artikkel 29-gruppens oppfatning om at de myndigheter som har saklig behov for denne type informasjon ikke bør få direkte tilgang til bookingsystemene hos flyselskaper og reisebyråer, men bør måtte etterspørre informasjonen når de har behov.

Mye av arbeidet i Artikkel 29-gruppen har dreid seg om overføring av personopplysninger mellom nasjonalstater. Binding Corporate Rules og Safe Harbour er to avtalesett i tillegg til EUs standardavtale om overføring av personopplysninger til tredjeland. Artikkel 29-gruppen følger utviklingen på området. I meldingsåret deltok avdelingsdirektøren for juridisk avdeling som en del av den europeiske delegasjonen på en konferanse om Safe Harbour i Washington DC.

I 2009 gjorde Artikkel 29-gruppen undersøkelser overfor søkemotorer (Google, Yahoo, Micro-

soft og IxQuick) på Internett, og så på sosiale nett-samfunn (blant annet Facebook og Myspace). En utfordring ved disse tjenestene er at mange av de store og ledende aktørene er etablert i land utenfor EU/EØS, særlig i USA. Tjenesten *Google Street View* ble behandlet spesielt. Dialogen førte til at bilder hvor personer er med skal redigeres slik at det ikke skal være mulig å identifisere enkeltpersoner.

Dette har direkte betydning for Datatilsynet da tilsynet ved sin deltagelse bedre kan vurdere hvordan det kan styrke personvernet for norske borgere overfor slike aktører. Det avgjørende punktet er hvor langt personopplysningsloven gjelder – spørsmålet om jurisdiksjon.

Artikkel 29-gruppen ferdigstilte dokumentet «*The Future of Privacy*» i meldingsåret. I dokumentet viser gruppen en del aktuelle utfordringer, og presenterer noen prinsipper som kan være med på å styrke personvernet, blant annet prinsippet om at nye systemer bygges med henblikk på personvern («*Privacy by design*»), og at systemer i sin grunnversjon skal gi et godt personvern («*Privacy by default*»). Som eksempel på det siste prinsippet vil et system som respekterer «privacy by default»-prinsippet ikke dele informasjon med andre før brukeren selv aktivt velger at det skal opptre slik. Datatilsynet har mange eksempler på at det motsatte er tilfellet – at brukeren selv i stedet må gå aktivt inn og gjøre noe for å begrense hva som deles med en større gruppe.

Technology Subgroup

Technology Subgroups møter holdes i Brussel, og Datatilsynet er representert med en saksbehandler. Gruppen arbeider med teknisk-relaterte spørsmål for Artikkel 29-gruppen. I 2009 har det vært avholdt tre møter. Følgende hovedsaker har vært under behandling eller blitt presentert i endelige rapporter i 2009:

- Behavioural advertising
- Google street view
- Letters to Search Engine Operators
- Questions for social networks
- Opinion e-Privacy Directive
- eCall
- Opinion on online social networking

Berlin-gruppen

Den internasjonale arbeidsgruppen for personvern innen telekommunikasjon, Berlin-gruppen, er primært nedsatt for å arbeide med tekniske

problemstillinger knyttet til telekommunikasjon, men behandler også andre tekniske problemstillinger. Blant de mest sentrale sakene i meldingsåret var:

- Bruk av «svarte bokser» i kjøretøy. Hvilken informasjon lagres og hvordan benyttes slike data?
- Antipiratvirksomhet i Europa
- Elektroniske bomssystemer
- Mobilitet og informasjonssikkerhet
- Internettfiltre
- Personvern i sosiale nettverk

En rekke andre tekniske problemstillinger var gjenstand for drøftelser i gruppen. Arbeidet i gruppen gir Datatilsynet viktige bidrag i sitt arbeid med tekniske problemstillinger.

Spring Conference

Hver vår avholdes et større «vår møte» der artikkel 29-gruppen inviterer tilsynsmyndigheter fra land som ikke er del av EU/EØS, som for eksempel Sveits. Møtet ble i meldingsåret arrangert i Edinburgh. Datatilsynet deltok med to personer.

Working Party on Police and Justice

Gruppen arbeider med spørsmål vedrørende politisamarbeid som faller inn under tredje søyle, det vil si utenfor det indre marked. Gruppen rapporterer til Spring Conference og eventuelle forslag og resolusjoner vedtas her. I 2008 og 2009 arbeidet gruppen blant annet med forhold knyttet til Lisboa-avtalen, samt spørsmål om behandling av personopplysninger i tilknytning til Cybercrime-konvensjonen. Datatilsynet er representert med en saksbehandler. Det er avholdt tre heldagsmøter i meldingsåret.

Joint Supervisory Authority

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengen-området, eller er straffedømt i et av medlemslandene. Møtene avholdes normalt i tilknytning til møtene i Working Party on Police and Justice i Brussel, og Datatilsynet er representert med to medlemmer i gruppen. I tillegg har en informasjonsmedarbeider bistått i arbeidet med å utvikle informasjonsmateriekknyttet til innføringen av SIS II.

Kontrollkommisjonen for Interpol

Kommisjonen skal overvåke anvendelsen av personvernlovgivning innen dette området, samt behandle forespørsler om innsyn i Interpols registre. Datatilsynet var i 2009 representert med en representant i kommisjonen.

Internasjonalt saksbehandlermøte

Dette er et internasjonalt samarbeidsforum for juridiske saksbehandlere. Det ble avholdt to møter, henholdsvis i Praha og på Kypros. Diskusjonene omhandlet blant annet kameraovervåking, kredittopplysningsvirksomhet, bruk av biometri i arbeidslivet og barn og ungdoms bruk av Internett. I forbindelse med temaet barn og ungdoms bruk av Internett, ble det norske Datatilsynets opplegg «*Du bestemmer*» trukket fram av det spanske tilsynet, etter vellykket gjennomføring i Spania. Datatilsynet var representert med to saksbehandlere på disse møtene.

Nordisk datatilsynsjefmøte

Dette er et møte for direktørene i de nordiske datatilsynene, og arrangeres annet hvert år. I 2009 var det arrangert i Sverige. Direktøren, avdelingsdirektøren for juridisk avdeling samt en seniorrådgiver fra juridisk avdeling deltok fra det norske Datatilsynet. På møtet var det enstemmig oppslutning om å rette en henvendelse til Nordisk råd om personvern i Norden.

Nordisk saksbehandlermøte

Dette er et årlig nordisk forum for saksbehandlere. Arrangementet ble i 2009 avholdt i Torshavn på Færøyene. Datatilsynet var representert med en fra ledelsen og to saksbehandlere. «*Du bestemmer*»-kampanjen ble redegjort for, og møtet hadde videre tema barn og unge. Et annet tema var personvern i arbeidslivet. Datatilsynet redegjorde for den norske e-postforskriften. Møtene er ellers et viktig forum for utveksling av erfaringer mellom de nordiske landene.

Nordisk teknologimøte

Det ble avholdt et møte i Stockholm hvor det var deltakere fra øvrige Datatilsyn i Norden. Blant de sentrale spørsmål som ble drøftet var:

- Status vedrørende FRA-loven og datalagringsdirektivet i de ulike landene
- Tekniske funn på kontroller

- e-billettering
- e-ID, elektroniske signaturer og nettbanker

6 Informasjonsvirksomheten

Personvernlovgivningen 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 med hensyn til sin behandling av personopplysninger. Datatilsynet er derfor avhengig av å oppnå synlighet i samfunnet og å skape oppmerksomhet og debatt omkring sentrale personvernspørsmål. Aktiv informasjonsvirksomhet er dermed et virkemiddel som vektlegges sterkt. Tilsynet har som en uttalt målsetting å kommunisere sine standpunkter på en tydelig måte som folk flest forstår, og å være offensiv og eksperimenterende i valg av virkemidler og kanaler. Dette skal imidlertid ikke gå på bekostning av Datatilsynets seriøsitet, etterrettelighet og integritet.

Mediekontakt og foredragsvirksomhet

Som et ledd i det å kunne ha høy beredskap med hensyn til å respondere på henvendelser fra mediene er mange medarbeidere blitt rustet til å kunne gi uttalelser innen egne saksområder, skrive debattinnlegg med videre. Sett i forhold til organisasjonens størrelse og administrative ressurser må Datatilsynet kunne sies å være en meget synlig aktør i samfunnsdebatten.

I løpet av meldingsåret har Datatilsynet besvart om lag 1 300 henvendelser fra mediene. Dette førte til over 5 700 registrerte medieoppslag i 2009 hvor Datatilsynet var nevnt. Det temaet som fikk fått størst medieomtale i 2009 var det omstridte datalagringsdirektivet. Andre saker omfattet av stor interesse var identitetstyveri, fildeling, skattelister og ulike søketjenester på Internett.

Det ble utarbeidet 16 egenproduserte artikler, kronikker og debattinnlegg til bruk i medier utenfor Datatilsynet. I mai publiserte Datatilsynet sin første melding på mikrobloggingstjenesten Twitter, og det ble lagt ut 135 meldinger i løpet av året. Ved årsskiftet hadde Datatilsynet ca 1 000 'followers' på tjenesten.

Det er blitt holdt 110 foredrag ut over Datatilsynets egne kurs og seminarer overfor personvernombudene. Dette er betydelig færre enn i året før, men er resultat av en nødvendig og helt bevisst prioritering fra Datatilsynets side.

Tabell 1.1

Antall foredrag	
2005	92
2006	157
2007	140
2008	162
2009	110

Tabell 1.2

Besvarte telefon- og eposthenvendelser		
	Telefon	E-post
2006	8 125	2 711
2007	7 300	2 673
2008	7 070	3 054
2009	6 952	4 401

Publikumsveiledning

Den kanskje viktigste delen av kommunikasjonsarbeidet er den direkte kontakten med enkeltpersoner og representanter for virksomheter som på eget initiativ tar kontakt for å søke råd og veiledning. De aller fleste slike henvendelser besvares av en juridisk veiledningstjeneste, bestående av fire jurister.

Veiledningstjenesten besvarte 6 952 telefonhenvendelser i meldingsåret, en liten nedgang sett i forhold til 2008. Årsaken til nedgangen skyldes nok i hovedsak at antallet henvendelser om direkte markedsføring over tid har gått markant ned. Fra 1. juni overtok også Forbrukerombudet ansvaret for reservasjon mot direkte markedsføring. Henvendelser om dette temaet håndteres dermed ikke lengre av Datatilsynet.

Samtidig som antallet telefonhenvendelser har gått ned, har antallet henvendelser pr e-post hatt en ganske betydelig økning i 2009. Samlet sett har dermed antallet publikumshenvendelser øket i forhold til året før.

Tilgjengelighet og svartid vurderes gjennomgående fortsatt å være fullt ut tilfredsstillende både når det gjelder telefon- og e-posthenvendelsene.

Hva handler henvendelsene om?

Tabellen nedenfor viser telefonhenvendelsene besvart av den juridiske veiledningstjenesten. Henvendelsene er fordelt på tema, og hvorvidt innringer opptrer som (eller på vegne av) plikt- eller rettighetshavere.

Tabell 1.3

2009	Plikt	Rett	Total	Prosent
Annet	311	937	1248	18 %
Arbeidsgivers kontroll/innsyn	411	420	831	12 %
Biometri	16	39	55	1 %
Fødselsnummer	86	533	619	9 %
Helse, forskning	160	116	276	4 %
Internasjonalt (overføring utland)	86	32	118	2 %
Internett (publisering mv)	106	507	613	9 %
Internkontroll/info.sikkerhet	204	112	316	5 %
Kameraovervåking	402	378	780	11 %
Kredittopplysning	66	247	313	5 %
Kunderregister/Medlemsregister	186	172	358	5 %
Lokalisering, sensortechnologi	35	49	84	1 %
Lydopptak	32	78	110	2 %

Tabell 1.3

2009	Plikt	Rett	Total	Prosent
Melding/Konsesjon (rutiner)	495	76	571	8 %
Offentlige registre	102	158	260	4 %
Reservasjon/DM	33	254	287	4 %
Skoles kontroll/innsyn	70	43	113	2 %
Sum	2801	4151	6952	≈100 %

Det ble ved årsskiftet gjort endringer i kategoriseringen av tema. Dette må tas hensyn til ved bruk av materialet til sammenlikninger med tidligere år. Videre er det slik at også Tilsyns- og sikkerhetsavdelingen besvarer mange henvendelser om internkontroll, informasjonssikkerhet og tekniske spørsmål, som ikke kommer med i statistikken.

Arbeidsgivers bruk av GPS-lokalisering i forbindelse med såkalt flåtestyring og bruk av elektronisk kjørebok synes å være et tema med økende aktualitet.

Undervisningsopplegget «Du bestemmer»:

Undervisningsopplegget «Du bestemmer» er utviklet i samarbeid med Teknologirådet og Utdanningsdirektoratet og handler om hvordan barn og unge kan ta kontroll over egne personopplysninger, og respektere andres integritet. Første modul av undervisningsopplegget, rettet mot aldersgruppen 14-17 år, ble lansert januar 2007.

Inspirert av svært gode tilbakemeldinger på undervisningsopplegget, og stor etterspørsel etter et lignende opplegg rettet mot de noe yngre elevene ble det i april 2009 lansert et tilpasset undervisningsopplegg rettet mot elever i alderen 9-13 år. Overfor denne målgruppen har temaet digital mobbing fått en noe større plass enn i det opprinnelige undervisningsopplegget.

I forbindelse med lanseringen av materialet ble det etablert en ny webløsning. Både tekstmaterialet og alle filmene tilhørende prosjektet er gjort lettere tilgjengelig enn tidligere. Dette er nå tilgjengelig både på bokmål, nynorsk, samisk og engelsk.

Tidlig i 2009 ble materialet distribuert til personvernmyndighetene i Europa og verden for øvrig, med oppfordring om å ta dette i bruk uten å måtte betale for rettigheter mv. Responsen har vært overveldende. Brosjyrene har blitt oversatt til bruk i Tyskland og Østerrike og her har de også dubbet filmene. I Spania har alt materiale blitt oversatt til spansk og baskisk, og en kata-

lansk versjon er på trappene. Også i Makedonia og Slovenia har materialet blitt oversatt og tatt i bruk. Ellers har både Belgia, Storbritannia, Sveits, Isle of Man, Tyrkia og Litauen vist interesse for å ta i bruk undervisningsmaterialet.

Teknologirådet, Utdanningsdirektoratet og Datatilsynet fortsetter samarbeidet om Du bestemmer, og planlegger utvikling av nye elementer til kampanjen, som vil bli iverksatt i 2010.

Selvtest mot identitetstyveri

Mye tyder på at identitetstyveri vil være et økende problem i Norge. Datatilsynet bidrar derfor aktivt i det såkalte «ID-tyveriprogrammet» som prosjekteres av Norsk senter for informasjonssikring, NorSIS. Som et bidrag til programmets arbeid tok Datatilsynet initiativ til å utvikle og finansiere en «selvtest» for at publikum selv skal finne ut hvor utsatt han/hun er for identitetstyveri. Testen ble lansert i juni 2009 og ved årsskiftet har testen blitt tatt av nær 28 000 personer. Selvtesten er nå også blitt oversatt til engelsk og gjøres fritt disponibel for andre lands personvernmyndigheter. Mange land har allerede meldt sin interesse. Blant annet har New Zealand tatt initiativ til å spre en tilpasset versjon av selvtesten i det sør-østlige Asia.

Kommuneprosjektet – Informasjonssikkerhet og internkontroll

Målet med «kommuneprosjektet» er å bedre kommunenes etterlevelse av personvernlovgivningen. Virkemidlene er tilsyn, opplæring og annen informasjonsvirksomhet.

Etter å ha oppdatert og gjort veilederen om internkontroll innholdsmessig mer tilgjengelig ble den i november distribuert til samtlige kommuner med oppfordring om å ta denne i bruk. I samarbeid med foreningen Kommunal Informasjonssikkerhet (KINS) og NorSIS utvikles et gratis dagsseminar som i løpet av våren 2010 skal tilbys på syv ulike steder i landet. Senere vil samt-

lige kommuner bli bedt om å rapportere hvor langt de er kommet i arbeidet med å etablere et dokumentert internkontrollsystem for sin behandling av personopplysninger.

Veiledningstjenesten Slettmeg.no

I forbindelse med revidert nasjonalbudsjett ble Datatilsynet i 2009 tildelt ekstra prosjektmidler til etablering av en veiledningstjeneste som skal bistå personer som opplever sitt personvern krenket på Internett, eller som av andre grunner ønsker å få slettet eller rettet personopplysninger på nettet. Bakgrunnen var anbefalinger i Personvernkommisjonens rapport NOU 2009:1 «Individ og integritet».

Rådgivningstjenesten planlegges lansert i mars 2010 og lokaliseres i Datatilsynets lokaler. Tjenesten rettes mot hele befolkningen, voksne så vel som unge. Tjenesten betjenes av to medarbeidere som skal gi publikum bistand via telefon, e-post og chat.

I 2009 har det blitt jobbet med å utvikle et navn, en profil og en egen nettside for tjenesten. Nettsiden vil få domenenavnet Slettmeg.no som også blir navnet på tjenesten. På nettsiden vil publikum finne guider og praktiske råd for hvordan de selv kan gå frem når man opplever seg krenket via Internett.

Slettmeg.no skal ikke utøve saksbehandling og fatte formelle vedtak. Tjenesten skal for eksempel ikke ha myndighet til å pålegge noen å slette eller rette krenkende opplysninger fra Internett. Utøvelse av eventuelle sanksjoner overlates til tilsynsmyndigheter, politi, domstoler og andre. Fokus for slettmeg.no er rådgivning, hjelp til selvhjelp og tett kontakt med de forskjellige nettjenestene.

Slettmeg.no er i første omgang et forsøksprosjekt over to år.

Personvernombod

I løpet av 2009 har det vore ei jamn tilstrøyming av nye personvernombod, utan den store rekrutteringsinnsatsen frå tilsynet si side. Ved utgangen av året er ein oppe i 151 ombod, ein auke på 26 ombod. Samstundes har ei verksemd avslutta ordninga, grunna vanskar med å skaffe personar til å ta på seg rolla. For første gang har også Datatilsynet avgjort å oppheve vedtaket om ordninga med ei verksemd, fordi det har vore umogleg å kome i kontakt med verksemda. Talet på verksemdar med ombod er også i vekst, og det er ved utgan-

Tabell 1.4

	Antall ombod
2007	95
2008	124
2009	151

gen av 2009 over 300 verksemdar som har personvernombod.

Datatilsynet arrangerte for første gang eit todagarskurs i informasjonstryggleik og internkontroll for vidarekomne. Ut i frå evalueringane må dette seiast å vere eit særskilt vellukka kurs, som det vil vere aktuelt å arrangere fleire gonger. I løpet av 3. tertial er det også arrangert opplæringskurs for nye ombod og innføringskurs i internkontroll og informasjonstryggleik. I løpet av året er det halde åtte kurs for omboda, med gjennomsnittleg 20-30 deltakarar på kvart kurs.

Personvernombodsordninga har også fått ekstra tilrettelagde midlar for 2009 og dei to komande åra, som vil føre til auka satsing på rekruttering, marknadsføring og tilrettelegging av ordninga. I samband med dette har det også vore tilsett ein prosjektleiar for ordninga.

7 Tilsyns- og sikkerhetsarbeid

I kontrollvirksomheten ble det varslet eller fattet 391 vedtak fordelt på 168 kontrollobjekter. Hele 117 av funnene ble karakterisert som alvorlige ut fra tilsynets egne vurderinger. Det ble funnet avvik som enten medførte varsel om vedtak, vedtak eller påpekning av plikt hos i underkant av 90 prosent av objektene. Dersom kontrollene mot kameraovervåking trekkes ut av utvalget, er tallet rundt 80 prosent.

Andelen virksomheter som får formalisert reaksjon har dessverre økt de senere årene. I et normalår regner tilsynet at rundt 60 prosent av besøkte virksomheter får en eller annen form for reaksjon. Noe av økningen er antakelig forklart ved at tilsynet har fått bredere erfaring, og tilsynsteamene har blitt mer profesjonelle i å isolere avvik. Det må imidlertid presiseres at utvalget av potensielle kontrollobjekter er noe skjevt, siden etaten praktiserer risikobasert kontrollvirksomhet. Det innebærer at sektorer hvor sannsynlighet for funn er høy, prioriteres.

7.1 Kort om sektorer som ble kontrollert

E-billettering og bomsystemer griper inn i personvernet på grunn av omfattende lagring av transaksjoner. Kontrollene avdekket en tiltagende tendens til å lagre detaljerte data i større omfang og over lengre tid enn hva regelverket, etter tilsynets oppfatning, gir rom for.

Kontrollene i finanssektoren tok sikte på å kartlegge praksis med å sette driftsoppgaver bort til virksomheter lokalisert utenfor EØS-sonen, i det aktuelle tilfellet Ukraina. Kontrollene søkte også å etablere forvaltningspraksis på området.

Kameraovervåking er et synlig tegn på overvåkingen i samfunnet. Tidligere kontrollvirksomhet har avdekket stor forskjell i overvåkingstrykket i ulike norske byer. Tilsvarende ble bekreftet i rapporteringsårets kontroller. I sentrale handlegater varierer andelen overvåkede butikker fra i underkant av 20 prosent til rundt 50 prosent.

Datatilsynet har over tid konstatert store utfordringer med å opprettholde tilfredstillende personvern innen forskning, spesielt i medisinsk forskning. Personvernet kommer ofte i konflikt med forskers ønske om lett tilgang til forskningsmateriale. De to kontrollene som ble avvirket peker i retning av manglende respekt for de rettigheter den registrerte er gitt fra lovgivers side.

Innen justissektoren så tilsynet på automatisk trafikk kontroll. Utviklingen i retning av strekningsvise systemer innebærer en mer inngripende tilnærming til bilistene, siden alle passerende fotografes. Hvem som er ansvarlig for slike anlegg og hvilke hjemler som anføres byr også på utfordringer.

Kontrollene mot kommunesektoren ble gjennomført i ett fylkesmannsembete. Det konstateres store variasjoner i etterlevelse av regelverket. De vanligste manglene dreier seg om manglende internkontroll og dokumentert informasjonssikkerhet.

Tilsynet har fulgt opp tidligere aktiviteter mot utdanningssektoren. Det ble fokusert på administrative systemer. Tidligere har elektroniske læringsplattformer, kameraovervåking i skolehverdagen og elevenes bruk datamaskin i opplæringsøyemed vært underlagt kontroller.

Datatilsynet kontrollerte også behandling av personopplysninger innenfor netthandel, med spesiell vekt på auksjonssider. I tillegg ble det foretatt kontroll med sosiale nettsamfunn, hvor opptjening av poeng eller gevinster var en viktig faktor.

Det ble gjennomført kontroll mot et mindre antall biblioteker. Tilsynet konstaterte at det stort sett var en ryddig håndtering av personopplysning

ger blant de kontrollerte. Samtidig avdekket tilsynet en praksis med innhenting av fødselsnummer for nasjonale lånekort som vil følges opp.

I kontrollene mot tannhelsetjenesten avdekket tilsynet mangler ved virksomhetenes egenkontroll, tilgangsstyring og informasjonssikkerhet. I ettertid har det vært oppfølgende dialog med Tannlegeforeningen.

Offentlig forvaltning er tradisjonelt utfordrende kontrollobjekter. Det skyldes ikke minst at det trer inn annet lovverk som i mange tilfeller overstyrer mange av rettighetene i personopplysningsloven. Tilsynet erfarer at forvaltningen har en tendens til å strekke egne hjemler langt, i noen tilfeller langt utover hva det finnes støtte for i lovverket. Datatilsynet har derfor utfordret en del forvaltningsorganer på dette punktet.

Datatilsynet gjennomføre noen kontroller hos private statistikkbyråer. Det ble rapportert om relativt ryddige forhold hos de besøkte virksomhetene. I noen grad ble det påvist manglende databehandleravtale der deler av behandlingen var satt bort, men hovedinntrykket er likevel tilfredstillende.

Kontrollene innen telekommunikasjon avdekket en del mangler, blant annet manglende konsesjon eller brudd på sentrale vilkår i konsesjonen, samt mangler når det gjelder internkontroll.

7.2 Styring av og mål med kontrollvirksomheten

Kontrollvirksomheten styres gjennom halvårslige tilsynsplaner. Dette gir god dynamikk og setter etaten i stand til å justere de operative valgene til foreliggende situasjon. Datatilsynet gjennomfører i likhet med de fleste tilsynsorganer risikobaserte kontroller. Det innebærer at innsatsen rettes inn mot områder hvor sannsynlighet for regelverksbrudd anses som høy og/eller at konsekvensene ved brudd er mest alvorlige.

Det overordnede målet med Datatilsynets kontrollvirksomhet er i henhold til personopplysningsloven å bidra til etterlevelse av lovregler om behandling av personopplysninger.

Målet med den operative kontrollvirksomheten er:

- Å skaffe kunnskap om trusler mot personvernet innen ulike typer bransjer.
- Å bruke erfaringer operativt til å sette fokus på personvern i ulike sektorer.
- Å kunne identifisere om visse grupper mennesker er spesielt utsatt for krenkelse av personvernet.
- Å overvåke den teknologiske utviklingen og hvilke trusler det innebærer for den enkelte.

- Å bruke erfaringer fra operativt tilsyn til å kommunisere med samfunnet for øvrig.
- Gjennom vedtak å sørge for at regelverksbrudd stanses.

Personopplysningslovens regler om internkontroll er basis for kontrollmetodikken, ved at det gjennomføres systemrettet tilsyn. Det innebærer vektlegging av systemrevisjon av dokumentasjon kombinert med verifikasjon av praksis.

7.3 Nøkkeltall

Datatilsynets kontrollvirksomhet omfatter aktiviteter mot i alt 168 virksomheter. Tallet er en økning fra forrige år hvor tilsvarende tall var 141. Økningen omfatter imidlertid rundt 25 kontroller hvor funn ikke ble fulgt opp med videre saksbehandling, men avgrenset til påpekning av plikt.

I vårsesjonen ble det avvirket kontroll mot 77 virksomheter. Av disse var 73 stedlige kontroller, mens fire ble gjennomført som kontroll av virksomhetens nettside og en ble avlyst som følge av at behandlingen ble avsluttet etter at virksomheten mottok varsel om kontroll.

I høstens sesjon ble det avvirket kontroll mot 91 virksomheter, samtlige var stedlige kontroller. To planlagte kontroller ble avlyst av hensyn til uforutsette forhold. Følgende bransjer (eller temaområder) var underlagt kontroll i rapporteringsåret: Datatilsynet brukte en alternativ kontrollmetode i vårens sesjon, såkalt nettbasert kontroll. Metoden har vært anvendt før i begrenset omfang og kan kun brukes der temaet for kontrollen er snevret til enkel faktainnhenting. Kontrollene følger samme prosedyre som øvrige kontroller, med unntak av forutgående varsel og fremmøte hos virksomhetene. I enkelte tilfeller har det vist seg vanskelig å komme i kontakt med nettbaserte virksomheter for å få gjennomført en effektiv kontroll.

7.4 Bruk av formelle reaksjoner

Datatilsynets praksis ved kontroll er å bruke formelle reaksjoner ved regelverksbrudd. Alternativt kunne tilsynet benyttet en mykere variant ved å veilede virksomhetene til bedre etterlevelse. Det finnes andre tilsynsmyndigheter har dette som praksis og har høstet gode erfaringer med denne metoden. Imidlertid vil dette ofte være sektormyndigheter som har jevnlig kontakt med samme tilsynsobjekt, og de har gjerne vesentlig større mannskap og faste etablerte kanaler til bransjeaktørene. Datatilsynet er ofte inne i en sektor i en

Tabell 1.5

Bransje/Sektor	Antall
Arbeidsliv	6
Barnevern – offentlig	5
Barnevern – privat	5
Bibliotek	3
E-billettering og bomssystemer	5
Finanssektoren	2
Kameraovervåking	90
Forsikring	1
Forskning	2
Helse	1
Justissektoren	1
Kommune	6
Kundesystemer	2
Netthandel	4
Nettsamfunn – elektronisk kommunikasjon	4
Offentlig forvaltning	5
Statistikkbyrå	4
Tannhelse	7
Telekommunikasjon	4
Utdanning	11
Sum	168

kort periode. Et formelt vedtak stiller strenge krav til kvalitet i saksbehandlingen og gir kontrollobjektene rettigheter de avskjæres fra om vedtaksliknende formuleringer kommuniseres på andre måter. Et vedtak krever at funn må dokumenteres. Disse må videre vurderes opp mot regelverkets bestemmelser og den berørte virksomhet må høres før tilsynet fatter sin beslutning.

7.5 Generelt fra kontrollvirksomheten

Det avdekkes mange brudd på regelverkets krav. Alvorlighetsgraden varierer, men gjennomgående er det for lite kjennskap til og respekt for de rettsregler som er fastsatt i personopplysningsloven. En generell beskrivelse av situasjonen er at

- virksomhetene ikke har gjort seg tilstrekkelig kjent med regelverket (kjennskap)
- de i altfor liten grad har avklart hvem som må gjøre hva (ansvar)
- de har mangelfull oversikt over hvilke personopplysninger som behandles og har ikke reflektert over formål eller behandlingsgrunnlag
- de har mangelfull systematikk i tilnærmingen til regelverket (internkontroll)
- de ikke sørger for en god nok sikring av personopplysningene (informasjonssikkerhet)
- de ikke følger sentrale plikter i regelverket, som informasjonsplikten og slettebestemmelsene

Ovennevnte finner tilsynet i større eller mindre grad hos et flertall av virksomhetene. Tallmaterialet viser ikke noen skjevfordeling mellom store, mellomstore og små virksomheter.

Kjennskap til regelverket

Personopplysningsloven er i noe større grad kjent hos virksomhetene i meldingsåret enn i tidligere år. Samtidig «konkurrerer» denne lovens plikter mot andre rettslige plikter som påhviler virksomhetene. Ledelsens bevissthet og motivasjon til å håndtere pliktene er avgjørende for hvor sterk fokus virksomheten legger i etterlevelse.

Datatilsynet driver kontrollvirksomhet innen et meget bredt spekter av virksomheter. På den ene siden av skalaen finner man de store finansaktørene, med ressurssterke organisasjoner med egen juridisk og teknisk kompetanse. I den andre enden av skalaen finner man virksomheter som drives «fra gutterommet». Disse har en forretningsidé som kan realiseres med begrensede økonomiske ressurser som følge av nettets utallige muligheter. Slike virksomheter drives ofte i en grenseflate mellom hobby og næringsvirksomhet, ofte med gründeren selv som eneste aktive. Virksomheten kan likevel ha flere titalls tusen brukere eller kunder.

De store konsernene er tilsynsteknisk de enkleste å håndtere. Pålegg fra offentlige myndigheter følges opp. I noen få tilfeller prøves saken for klageinstans, men de retter seg etter de avgjørelser som blir tatt. Virksomheter som driver i den andre enden av skalaen er langt mer krevende å arbeide med for en tilsynsmyndighet. De kan være vanskelige å få tak i, det er uklart hvem som egentlig er ansvarlig, de har lite kunnskap om regelverkets eksistens og de baserer virksomheten på produkter eller konsepter andre har laget.

I tillegg finnes tannlegekontor, små kommuner, butikker og barneverninstusjoner. De står ofte uten egen juridisk eller teknisk kompetanse, og mangler kanskje også økonomi til å kjøpe slik bistand. Å drive kjernevirksomheten på en økonomisk forsvarlig måte innen rammen av regelverket kan by på utfordringer for enkelte virksomheter. Små og mellomstore virksomheter har ofte lite tid til annet enn kjernevirksomheten. Etterlevelse av regelverk er noe de må ta etter evne, etter at pasienter, kunder eller brukere er håndtert. Ovenfor denne gruppen er bransjeforeningene meget viktige som støttespillere.

Den marginalt økende kunnskap om regelverket fører ikke automatisk til etterlevelse. Virksomheten må gjennom en rekke faser som alle byr på nye utfordringer; forstå omfanget, beslutningsprosessen, gjennomføring og opprettholdelse. Det krever vedvarende fokus fra ledelsens side, hvilket ofte ikke er til stede. Etterlevelse av regelverk handler til syvende og sist om bedriftskultur. Der som ledelsen ikke fokuserer på viktigheten av å følge regelverket og interne ressurspersoner som kan drive prosessen, er det vanskelig å få god kultur i praksis.

Internkontroll og informasjonssikkerhet

Internkontroll har vist seg å by på mange utfordringer for virksomhetene. De har manglende forståelse av hvordan kravet skal ivaretas, langt mindre etablere et tilfredsstillende system som fungerer i virksomheten. Internkontroll er et organisatorisk styringsredskap som effektivt skal foredle og tilpasse regelverkets krav til den aktuelle virksomhet.

Det er mange brudd på bestemmelsene om internkontroll. Når Datatilsynet fatter vedtak i underliggende plikter, som informasjonsplikt, innsyn, retting og sletting, er det ofte fordi virksomheten ikke har en systematisk tilnærming til regelverket, slik loven krever.

Situasjonen synes å være marginalt bedre for informasjonssikkerhet. De fleste virksomheter forstår at bruk av informasjonsteknologi krever en systematisk tilnærming. De er dessuten redd for at virksomheten kan bli kompromittert som følge av dårlig sikkerhet. Historier om virus, dataangrep og systemkollaps har åpenbart nådd de aller fleste. Derfor vil de fleste enten i egen regi, eller ved innleid kompetanse sørge for en form for systematisk sikkerhetsarbeid. Det er likevel et langt stykke frem til å oppfylle regelverkets krav. Ofte kan fokuset virksomheten legger til grunn være et helt annet enn regelverket krever. Virk-

somheten kan for eksempel være svært opptatt av tilgjengelighet til personopplysningene, men helt neglisjere tilstrekkelig konfidensialitet til samme opplysninger.

Det alvorligste avviket som går igjen går på manglende vurderinger om hvorvidt sikkerheten er tilfredsstillende ivaretatt. Virksomhetene har plikt til å definere akseptabel risiko for egen virksomhet. De må også gjennom risikovurderinger sørge for at de ligger innenfor disse rammene.

Viktige forutsetninger

Det er en del basale forutsetninger som må være på plass for at behandlingen av personopplysninger kan anses å være trygg. Etter tilsynets vurdering bør minst følgende forutsetninger være oppfylt:

1. Noen må ta et ansvar for å forvalte opplysningene korrekt.
2. De ansatte vet hvilke retningslinjer som gjelder for behandlingen og følger disse.
3. Det må være satt i verk systematiske tiltak for å behandle opplysningene på en god måte og at dette kan dokumenteres.
4. Eventuelt misbruk eller brudd på forventet sikkerhet må bli oppdaget og håndtert.

Dersom disse fire forutsetningene ikke er oppfylt, synes det rimelig å hevde at forutsetningene for en trygg forvaltning av opplysningene ikke er på plass. Mangel på en eller flere komponenter øker sannsynligheten for at ting går galt. Hvor store konsekvenser et eventuelt sikkerhetsbrudd får er avgjørende for den totale risiko.

Datatilsynets kontroller har gjennom flere år avdekket at mange virksomheter, både i privat og offentlig sektor, ikke ivaretar de ovennevnte grunnleggende forutsetningene. Det er videre sterke korrelasjoner ute og går. Om en av komponentene mangler, er det stor sannsynlighet for at flere mangler¹.

Sikkerhetsbrudd

Etter Datatilsynets vurdering er det fare for alvorlige sikkerhetsbrudd hos mange virksomheter, både i privat og offentlig sektor. Når og hvor dette eventuelt skjer er vanskelig å forutsi. Manglende sikkerhet er en faktor, men det må også foreligge

en utløsende årsak. Det kan være utro tjenere eller eksterne som skaffer seg urettmessig tilgang til opplysninger.

I Norge finnes det svært mangelfull oversikt over sikkerhetsbrudd. Det er gjennomgående lite tilrettelagte løsninger for å rapportere slike hendelser, og virksomhetene vil ofte vegre seg for slik rapportering av hensyn til sitt rykte.

Personopplysningsforskriften har siden år 2001 hatt plikt til å rapportere sikkerhetsbrudd. Rapporteringen synes å være meget begrenset. I løpet av meldingsåret kom det inn 51 saker. En tilsvarende rapporteringsplikt er tatt inn i Kredittilsynets IKT-forskrift. Datatilsynet har tatt initiativ for en koordinering av de to pliktene.

Del II

8 Temaer og tendenser i 2009

En viktig del av Datatilsynets mandat er å identifisere farer for personvernet, og gi råd om hvordan farene kan unngås eller begrenses.

Datatilsynet vil peke på noen utviklingstrekk med stor påvirkningskraft for personverntilstanden i Norge. Analysene er begrunnet i erfaringer fra tilsyn og saksbehandling, fra høringsarbeidet, deltakelse i forskjellige arbeids- og styringsgrupper nasjonalt og internasjonalt, samt saker som Datatilsynet er blitt oppmerksom på gjennom tips eller medieomtale. Beskrivelsen av tendensene bygger på grundigere omtaler andre steder i årsmeldingen.

Datatilsynets mandat er å se til at vernet av opplysninger om privatpersoner ikke svekkes, at opplysninger om vedkommendes private forhold ikke samles, spres eller brukes uten at det finnes forståelige, avveide lovhjemler, eller at vedkommende har gitt sitt frivillige, uttrykkelige og informerte samtykke. Personvernet skal verken settes til side for å løse mindre presserende problemer, eller problemer som like gjerne kan løses på annen måte. Inngrep må være forholdsmessige.

8.1 Personvernet svekkes på flere områder

Personvern ble i en rekke lovforslag i meldingsåret identifisert som en hindring for å kunne oppnå et godt mål. Datatilsynet er bekymret for at personverngarantier ønskes svekket for å oppnå marginale, ikke-dokumenterte gevinster, eller av rene effektivitetshensyn. Personvern er i sitt fundament en garanti for individet. Garantivilkårene innebærer blant annet at en del grunnleggende

¹ Dette er realitet i en overvekt av kontrollrapporter hvor det er påvist brudd på personopplysningslovens § 13 om informasjonssikkerhet. Det er sjeldent tilsynet kun påpeker et enkelt brudd på nevnte bestemmelse, men ofte et knippe bestemmelser i tilhørende forskrift.

krav må være oppfylt før man kan behandle opplysninger om enkeltmennesker. Behandlingen må være rimelig og forholdsmessig. Det må finnes forutsigbare, forståelige lovhjemler eller foreligge et informert, frivillig samtykke. Personen må settes i stand til å kunne forutsi om og hvordan han er omfattet av tiltaket.

Dersom personvernet blir sett som en hindring som helst bør ryddes av veien, vil det i praksis bety at denne garantien med tiden vil smuldre bort.

8.1.1 Bagatellisering av lagring av personopplysninger

Datatilsynet observerer en tendens til at personvernutfordrende *innsamling og lagring* av personopplysninger bagatelliseres. Spesielt har dette vært tydelig i debatten rundt datalagringsdirektivet, og i argumentasjonen rundt en samling og sammenslåing av norske helseregistre. (Les mer i avsnittene om henholdsvis justissaker og helsesaker). Bagatelliseringen av personvernrisikoen kommer samtidig med forsikringer om at opplysningene bare skal brukes i helt særskilte tilfeller eller under strenge forutsetninger. Det forespeiles en meget høy grad av sikkerhet hvor misbruk tilnærmet er utenkelig.

Datatilsynet vil understreke at innsamling og lagring av personopplysninger er personverntruede *i seg selv*, en tolkning som også er fremhevet av Menneskerettsdomstolen.

Kravet til en grundig avveining mellom de mulige fordelene ved å kreve lagring og ulempene for privatlivet må derfor gjelde fra det øyeblikk personopplysningene samles inn. Det er ikke nok å ta denne vurderingen når opplysningene på et senere tidspunkt eventuelt blir tatt i bruk.

Makt og misbruksfare

Det vil alltid være fare for misbruk av personopplysninger som finnes lagret et eller annet sted. Opplysningene er ikke bare nyttige for den som samler inn, men kan ha nytteverdi for en rekke andre aktører også. En tro på at opplysningene vil kunne underlegges total sikkerhet er en utopi.

Den som har mye informasjon om enkeltpersonen har i tillegg skaffet seg en maktposisjon ovenfor den registrerte.

Man kan ikke *fjerne* personvernulempene ved innsamling av data ved å innføre sikkerhetstiltak, man kan bare i enkelte tilfeller gjøre noen av ulempene mindre. I noen sammenhenger, men langt i fra alltid, vil det være nok til å gjøre tiltaket

Tabell 1.6

Status	Fordeling ¹
Behandlingsansvaret er uavklart, virksomheten har i liten grad forhold seg til regelverket	Ca. 40 %
Behandlingsansvaret er avklart, men i manglende grad ført til tilstrekkelig etterlevelse regelverket	Ca. 30 %
Behandlingsansvaret er godt avklart og virksomheten har iverksatt en tilfredsstillende etterlevelse	Ca. 30 %

¹ Fordelingen er basert på et grovt overslag og bygger på en overordnet gjennomgang av kontrollrapporter for 2009.

akseptabelt. Det er viktig å skille mellom tilfellene der ulike reparerende tiltak *kan* gi akseptabelt personvern, og der risikoen for personvernulempene blir uakseptabelt stor.

8.1.2 Mangelfull ansvars plassering utfordrer personvernet

I mange av meldingsårets kontrollrapporter fremgår at behandlingsansvar ikke er avklart. Tabell 1.6 under gir en grov illustrasjon av fordelingen: Stadfesting av behandlingsansvar er meget viktig for å få god etterlevelse. Dersom den ansvarlige ikke er kjent med sitt ansvar, er det overhengende fare for at ingen foretar seg noe, i hvert fall ikke på en systematisk måte.

Datatilsynet konstaterer at det eksisterer stor usikkerhet i virksomhetene om plassering av behandlingsansvar. Dette er spesielt fremtredende i forvaltningen, hvor informasjon deles på tvers, på en mer eller mindre systematisk måte.

8.1.3 Diffuse krav til lagring i skattelovgivning og bokføringsregelverket utfordrer personvernet

Behandlingsansvarlige argumenterer for omfattende lagring av personopplysninger under henvisning til krav i annen lovgivning, særlig regnskapslovgivningen og skattemyndighetenes krav til å sjekke opplysningene. Tilsynet verken ønsker eller kan pålegge sletting i de tilfeller hvor annen særregulering krever fortsatt oppbevaring. Likevel ser Datatilsynet at en tydeligere angivelse av

hvilke opplysninger som er nødvendige å lagre er vesentlig for å oppnå bedre personvern i Norge.

Det er problematisk når behandlingsansvarlige henviser til eksempelvis bokføringsloven som grunnlag for at selv den minste lille detalj må oppbevares i tre år og seks måneder, eller i ti år. Når absolutt alle detaljer som angår transaksjonen blir tatt vare på, vil det også bety langtidslagring av personlig informasjon. Datatilsynet stiller spørsmål ved samfunnsnyttene i at detaljerte opplysninger rundt trivialiteter som et enkelt pizzakjøp eller en tilfeldig bomplassering skal lagres i flere år.

Uklarhetene i lagringskrav har Datatilsynet påpekt ved flere anledninger, både i tilsvaret til konkrete høringsforslag og på eget initiativ, til skattemyndighetene og til relevante departementer.

8.1.4 Mengden elektroniske spor øker

Teknologi gjør hverdagen lettere for den enkelte. Teknologien kan samtidig introdusere nye utfordringer for personvernet. I de senere årene har kombinasjon av forflytning, sensorsystemer og lagring representert en økende utfordring. Sensorsystemer kan være alt fra GPS og radiofrekvensbrikker (RFID), til elektroniske billetter og strekkoder og deres tilhørende avlesersystemer. Avlesning av posisjon, retning, tidspunkt og andre karakteristika knyttes til personer og lagres. I mange tilfeller for diffuse formål.

Et godt eksempel er introduksjon av flåtestyring, en metode som blant annet brukes for å sikre effektiv utnyttelse av en virksomhets bilflåte, for eksempel ved å finne en ledig bil som befinner seg i nærheten av oppdraget, ikke en som er langt unna. Teknologien kan imidlertid også brukes til å føre elektroniske kjørebøker som overtar for arbeidstakers plikter til å føre manuell logg over bruk av tjenestebil. Systemene, som ofte introduseres som en forenkling, drar med seg nye problemstillinger knyttet til personvernet.

Til forskjell fra flåtestyring, som sier noe om hvor kjøretøyet befinner seg på et gitt tidspunkt, lagrer kjørebøkene informasjon om hvor kjøretøyet har vært. Det representerer en vesensforskjell. Kombinert med mangel på sletting av informasjon, vil denne teknologien kunne innebære et voksende problem i arbeidslivet. I kontrollene Datatilsynet har gjennomført på området, påberopes det grunnlag for lagring i inntil 10 år av hensyn til skattemyndighetene. Datatilsynet er i tvil om lagringen er nødvendig etter skattelovgivningen. Arbeidsgivers økte kunnskap om arbeidstakers posisjon til enhver tid innebærer en maktforstyving i arbeidstakers disfavør.

Bruk av biometri har ofte forenkling som mål. Brukeren trenger verken passord, kort eller andre elementer, men kan benytte finger eller iris til å autentisere seg i ulike sammenhenger. Dette oppleves enkelt og effektivt, uten at man tenker videre over hvilke andre problemstillinger bruken kan introdusere. I mange tilfeller registreres det mengder av overskuddsinformasjon, rett og slett fordi systemene innbyr til det.

8.1.5 Anonyme alternativer forsvinner

Datatilsynet har gjennom flere årsmeldinger påpekt tendensen til at de anonyme alternativene er under særlig press. Bomringer og kollektivtrafikk er områder Datatilsynet har fulgt spesielt med på i flere år.

Løsninger der personlige, elektroniske brikker erstatter ihendehaverbevis som klippekort, dagsbilletter eller kontanter, medfører en betydelig trussel for personvernet dersom fundamentale personvern hensyn ikke bygges inn i billetterings-systemene.

Datatilsynet mener det bør være mulig å lage de elektroniske løsningene på en slik måte at man ikke knytter elektronisk billett eller brikke til én bestemt person. I praksis ser tilsynet likevel at viljen til å lage personvernvennlige løsninger er liten. Offentlige og private virksomheter ønsker i stor grad å kunne følge den enkelte personen i sine systemer, for blant annet å kunne trekke ut data av høy kvalitet til bruk i planleggingsarbeidet.

8.1.6 Samhandling gir personvernutfordringer

Økt samhandling mellom databaser og økt utnyttelse av offentlige data har vært et uttalt politisk mål i Norge. Datatilsynet savner en mer bevisst holdning til personvernssidene av samhandling.

I helsesektoren har det i meldingsåret vært flere forslag som utfordrer personvernet, spesielt samhandlingsreformens forutsetninger om tilgang til helseopplysninger på tvers av virksomhetsgrenser, og et forslag om samordning av forskningsrettede helseregistre.

Datatilsynet er bekymret for at ønsket om samhandling innen helsesektoren medfører stadig forslag om uthuling av helsepersonells taushetsplikt. Datatilsynet vil minne om at vissheten om at helseopplysninger blir formidlet videre fra legen, kan gjøre at flere vil kvie seg for kontakt med helsevesenet. Les mer om denne problemstillingen i kapitlet *Velferd, forskning og helse*.

I justissektoren fortsatte utviklingen i retning av økt sammenkobling av databaser mellom lan-

dene, der ulike europeiske politimyndigheter gis anledning til å søke i norske databaser, mens norske myndigheter kan søke i andre europeiske. Se for eksempel avsnittet om Prüm-avtalen i kapitlet *Justis- og utlendingsfeltet*.

Sammenkobling av databaser og mer «flyt» av data er problematisk for personvernet av flere årsaker:

- Mengden opplysninger som finnes om den enkelte kan bli ute av proporsjoner i forhold til alvorligheten av problemet man ønsker å løse.
- Faren for at opplysningene kan bli tatt i bruk til andre, nye formål øker. Den registrerte mister oversikten over egne personopplysninger, og informasjon til den registrerte blir vanskeligere å gjennomføre, siden det også for den behandlingsansvarlige blir vanskelig å forutsi hvor opplysningene kan komme til å vandre. I praksis velger man ofte bort å informere borgeren.
- Kvaliteten til opplysningene blir et problem: Det er ikke gitt at opplysninger samlet inn i en sammenheng er gode nok i en annen sammenheng.
- Misbruksfaren øker jo videre distribuert opplysningene er.
- Ansvar for opplysningene, samt det å ha tilstrekkelig sikkerhet, blir vanskeligere når opplysningene «flyter» i og mellom datasystemer.
- Muligheten til feilretting blir vanskelig når opplysningene utveksles. Feil kan forplante seg.

8.1.7 *Diffuse formål og manglende behandlingsgrunnlag svekker personverngarantier*

Behandling av personopplysninger forutsetter klart definerte formål og gyldig behandlingsgrunnlag. Datatilsynet avdekker dessverre mange avvik knyttet til disse forutsetningene. Virksomhetene er i varierende grad bevisst formålet og hvilke avgrensninger det gir for bruk av opplysningene.

Formål og behandlingsgrunnlag utgjør kjernen i personopplysningsloven. Formålet skaper rammer for selve behandlingen og gir mer eller mindre direkte anvisning om hvilke personopplysninger det er saklig grunn for å behandle. Formålet avgrenser også behandlingsansvarliges frihet til å benytte opplysningene i andre sammenhenger og til andre formål. Behandlingsgrunnlaget bidrar til å sikre den registrertes rettigheter. Lovens hovedregel er at den registrerte skal gi sitt frivillige, uttrykkelige og informerte samtykke. Alternativt kan behandlingen ha hjemmel i lov.

Manglende behandlingsgrunnlag er blant de mest vanlige avvikene som avdekkes i Datatilsynets kontroller. I forvaltningen er behandlingen i mange tilfeller basert på tvilsomt hjemmelsgrunnlag, gjerne ved at eksisterende hjemler er strukket uforholdsmessig langt. Hos private virksomheter er det gjerne mangler knyttet til samtykke. Det kan være gitt mangelfull informasjon, samtykke kan være i strid med krav til frivillighet eller det er ikke gitt uttrykkelig.

Samtykke er spesielt utfordrende for virksomheter i en monopolistisk situasjon. I privat sektor kan det være bomselskaper, offentlig kommunikasjon eller dominerende markedsaktører, som i en del tilfeller ikke tilbyr personvernvennlige alternativer. Den registrerte står dermed uten reelle valgmuligheter, utover å avvise tilbudet fra monopolisten.

8.1.8 *Manglende sletting gir press mot personvernet*

Datatilsynet har over tid fremholdt at brudd på sletteplikten er den største og alvorligste enkeltutfordringen for personvernet. Regelverkets utgangspunkt stiller krav til sletting når formålet med behandlingen er oppfylt. Det som i praksis skjer, er at virksomheten enten unnlater å slette eller definerer nye formål. Det synes å eksistere en form for eierskap til opplysninger generert i egen virksomhet, hvilket også påvirker holdningene til sletteplikten.

Kostnadene ved oppbevaring av opplysninger er fortsatt fallende, derfor vil virksomhetene sjelden sette i gang sletting av bedriftsøkonomiske årsaker. Tvert imot møter Datatilsynet en rekke argumenter for vedvarende lagring, som plikter etter regnskapslovgiving og skattelovgivning. Personopplysningsloven er kanskje den eneste reelle faktor som trekker i retning av en restriktiv slettepraksis.

Forbrukerhensyn brukes også som argument for videre lagring. I mange tilfeller hevder virksomheten at det er en ulempe for den registrerte om regelverkets slettekrav skal legges til grunn. Den registrerte kan, i følge disse virksomhetene, få innskrenket sin klageadgang eller miste andre naturlige rettigheter.

Datatilsynet opplever i mange tilfeller at sletting overhodet ikke har vært et tema i virksomheten. Dersom diskusjonen har vært oppe, er det sjelden på bakgrunn av hensynet til den registrertes personvern.

Datatilsynet kjemper en stadig tyngre kamp om tilfredsstillende slettepraksis. Mange vil ha

lang lagringstid. Heller ikke de registrerte synes å være spesielt opptatt av problematikken, med mindre de har opplevd krenkelser som følge av praksisen. Mange synes ikke helt å gripe essensen i hvorfor sletting er viktig. Det tradisjonelle argumentet om at; *for den som ikke har noe å skjule bør ikke vedvarende lagring av informasjon være et problem* – står fortsatt sterkt. Nordmenn flest har meget høy tillit til virksomhetenes behandling og stiller sjelden kritiske spørsmål.

8.1.9 Mangelfulle utredninger av lov- og forskriftsforslag gir personvernkonsekvenser

Datatilsynet har i flere årsmeldinger påpekt manglende personvernutredning før nye lov- og forskriftsforslag sendes ut på høring. Det er alvorlig når utredningsinstruksen ikke følges på dette området. Man kan ikke la presentasjonen og vurderingen av personvernkonsekvenser være opp til høringsinstansene alene. Premissene for vurderingen må ligge i utkastet, først da vil man kunne få brede, gode høringsprosesser med tilstrekkelig fokus på personvern.

Fornyings- og administrasjonsdepartementet har utviklet en nyttig veileder i vurdering av personvernkonsekvenser av lov- og forskriftsforslag. Datatilsynet anbefaler denne veilederen til alle som har befattning med høringsforslag.

Inngripende tiltak bør revideres jevnlig

Datatilsynet etterlyste i årsmeldingen for 2008 fokus på revisjon og evaluering av personverninn-gripende tiltak som allerede er innført. Dette ønsket er fortsatt like aktuelt, også etter at Metodekontrollutvalget leverte sin rapport i meldingsåret (NOU 2009:15). I rapporten til utvalget ble ulike inngripende metoder for etterforskning for politi og PST gjennomgått og evaluert. Ett av metodekontrollutvalgets viktigste funn var imidlertid reelle mangler på mulighetene til å foreta en tilstrekkelig evaluering på området. Datatilsynet vil understreke betydningen av at man følger opp Metodekontrollutvalgets funn også når det gjelder tilrettelegging av etterfølgende evaluering. Slik tilrettelegging må innebære at man definerer formål og parametre for måling, og bygger disse inn i regelverket, før man tillater de integritetsutfordrende metodene.

8.1.10 Bygg inn personverngarantier i datasystemer fra starten av

Godt personvern og informasjonssikkerhet krever innsats og finansiering. Mange systemer, der man ikke har vist noe behov for å lagre detaljer om enkeltmennesker, blir designet slik at man i praksis lagrer det meste om den enkelte i svært lang tid. Innebygde personverngarantier er spesielt viktig når man har ambisiøse samordningsprosjekter som krever informasjonsflyt mellom flere parter.

I meldingsåret ble det tydelig at det nå etterspørres nye, store og ambisiøse dataprojekter i sektorer med spesielt høye krav til personvern, taushetsplikt og konfidensialitet. Et eksempel er fremkommet gjennom debatten om NAV. Det er åpenbart behov for et omfattende datasystem for å kunne gjennomføre intensjonene i NAV-reformen.

Stortinget forutsetter omlegginger i helseforetakenes journalsystemer for å kunne gjennomføre samhandlingsreformen. Store endringer må gjøres før det er forsvarlig å kunne hente journalinformasjon på tvers av virksomhetsgrenser.

I tillegg har det også vært tydelig vist, både i meldingsåret og i foregående år, at politiets datasystemer har en rekke svakheter og trenger oppgradering.

Med den historiske kunnskap man har om NAVs, politiets og helsevesenets ulike systemer, bør man være klar over at det ikke er gjort i en håndvending å endre disse.

Datatilsynet er opptatt av at systemene designes på en personvernvennlig måte fra starten av, i stedet for at man velger uklare strategier for så å kompensere for manglende personvern i etterkant. Tilsynet konstaterer at problemstillingen strekker seg over fem ulike akser:

- For mange gis tilgang til for mange opplysninger.
- Det gis for stor informasjonsdybde, ofte langt ut over tjenestelig behov.
- Det legges ikke begrensninger på tiden medarbeiderne har tilgang til opplysningene.
- Det gis tilgang til for mange personer, ofte langt utover tjenestelig behov.
- Kontrollmekanismene, som for eksempel rutiner i tilknytning kontroll av logger, er mangelfulle.

9 Nærmere om utvalgte saksfelter

9.1 Justissektoren og utlendingsfeltet

9.1.1 Datalagringsdirektivet

2009 har i stor grad vært preget av debatten om datalagringsdirektivet. Datatilsynet understreker at direktivet representerer et brudd med dagens regime for registrering og lagring av kommunikasjonsopplysninger. Direktivet går på tvers av sentrale rettslige prinsipper, friheter og menneskerettigheter. En implementering av direktivet i norsk rett medfører at store mengder data om norske borgeres kommunikasjon og bevegelser blir registrert og oppbevart i lengre tid. Et av de sentrale spørsmålene er om Stortinget skal benytte reservasjonsretten i EØS-avtalen, mot innføring av direktivet i norsk lovgivning.

Motstanderne av direktivet er mange, noe som ikke minst har vist seg på ulike sosiale nettverksplattformer og blogger på Internett. Tilhengerne av en innføring av direktivet finnes i første rekke blant de myndigheter som skal etterforske og oppklare straffbare forhold. Etter Datatilsynets oppfatning har debatten delvis vært preget av manglende kunnskaper om hva selve direktivbestemmelsene innebærer, og hva direktivets formål er. Direktivet ble innført i kjølvannet av terrorangrepene i Madrid og London, og målsetningen var at man skulle få et effektivt middel til beskyttelse mot organisert kriminalitet og terror. Likevel har debatten i liten grad dreiet seg om direktivets nøkkelbegrep «*serious crime*», eller «*grov kriminalitet*» som det heter i den danske direktivteksten. Ved flere anledninger har tilhengerne tatt til orde for at direktivet er et viktig verktøy for oppklaring av mindre alvorlige forbrytelser.

I debatten rundt datalagringsdirektivet fremkommer det påstander om at personvernet ikke vil bli berørt ved datalagring fordi man vil sette klare og strenge forutsetninger for videre bruk av opplysningene. Høringsutkastet til norsk implementering av datalagringsdirektivet trekker frem at opplysningene ikke vil bli sett nærmere på av politiet med mindre det foreligger konkret mistanke, samt at en domstol har godkjent uthentingen av opplysningene.

Personvernbeskyttelsen i vestlig rettstradisjon skal imidlertid ikke utelukkende verge en mot etterfølgende bruk av innsamlede opplysninger, for eksempel til konkret overvåking. Det er ikke uproblematisk for personvernet å «notere ned alt» om hvilke kontakter man har og hvor man er når man kommuniserer i tilfelle man skulle trenge det

senere. Staten må eventuelt kunne godtgjøre at selve «nednoteringen», innsamlingen og lagringen av informasjonen, er forholdsmessig og nødvendig.

En planmessig lagring av opplysninger i tilfelle de skal vise seg nødvendige i en senere etterforskning kan komme til å utfordre uskyldspresumpsjonen, et viktig grunnpremiss i norsk rettssystem.

Datatilsynet advarer mot innføring av datalagringsdirektivet i norsk rett.

9.1.2 Prüm-avtalen – «Schengen III»

I slutten av november i meldingsåret meddelte Justis- og politidepartementet at Norge hadde undertegnet den såkalte Prüm-avtalen om et intensivert grenseoverskridende politisamarbeid i Europa. Avtalen innebærer blant annet at politimyndighetene i de ulike avtalelandene skal kunne dra nytte av ulike europeiske databaser som inneholder personopplysninger, i forbindelse med etterforskning av straffbare forhold. Avtalen gir dermed norsk politi tilgang til ulike registre over DNA-analyser og fingeravtrykk samt ulike kjøretøyregistre i samtlige av EUs medlemsland. I tillegg legges det til rette for utveksling av informasjon mellom avtalepartene i forbindelse med store arrangementer med grenseoverskridende dimensjoner.

Justisminister Storberget har i ulike avisintervjuer fremhevet at avtalen vil være et effektivt middel til bekjempelse og oppklaring av straffbare forhold, som for eksempel villainnbrudd. I tillegg til at det nasjonale DNA-registeret er utvidet til også å inneholde opplysninger innhentet i forbindelse med etterforskning av «hverdagskriminalitet», borger dette i følge Storberget for at flere år gamle forhold kan få en oppklaring. Som eksempel trekker Storberget i VG 30. november i meldingsåret frem at uløste saker om overfallsvoldtekter kan bli oppklart etter at DNA-prøver er innhentet i forbindelse med overtredelser av veitrafikklovgivningen.

Avtaleinngåelsen innebærer imidlertid ikke bare fordeler for mennesker i Norge. Datatilsynet mener at lavere terskler for innhenting av DNA-prøver og fingeravtrykk, i kombinasjon med at myndigheter i nesten 30 land gis søketilgang i disse opplysningene, også fører med seg utfordringer for personvernet. Det burde være tilstrekkelig å vise til Storbergets trafikkover tredelseseksempel gjengitt over, samtidig som man husker at avtalen også forutsetter at opplysninger om norske borgere skal utleveres til myndigheter i andre land.

Selv om det finnes enkelte mekanismer i selve avtaleverket som skal ivareta individets rettigheter, ser Datatilsynet at personvernkonsekvensene av en implementering av avtaleverket bør utredes nærmere før avtalen trer i kraft.

9.1.3 Lisboa-traktaten

Innføringen av Lisboa-traktaten fører med seg en rekke endringer i EUs traktatsfundament. Blant annet skal det innføres et felleseuropeisk regelverk som omfatter behandling av personopplysninger innenfor EUs tredje pilar, det vil si området for justis- og politisamarbeid.

Datatilsynet vil følge med på forslag som dukker opp som følge av disse endringene.

9.1.4 Den svenske FRA-loven

Den svenske loven om signalspaning trådte i kraft 1. desember 2009. Loven omtales ofte som FRA-loven, ettersom det er Försvarets radioanstalt i Sverige som foretar signalspaningen. Signalspaningen omfatter all kommunikasjon som krysser den svenske territorialgrensen. Dette fører til at en stor del av norsk datatrafikk berøres, idet vesentlige deler av denne datakommunikasjonen går via Sverige. FRA-loven gir de svenske myndighetene anledning til å avlytte og samle inn selve innholdet i kommunikasjonen.

Initiativet har avstedkommet sterk kritikk i Sverige. Blant annet kunne man i september 2009 lese et innlegg i Dagens Nyheter, undertegnet av en rekke størrelser innenfor svensk akademisk, som konkluderte på følgende vis: «FRA:s avlysning av civil kommunikasjon medfør kartlegging av vældigt många helt oskyldiga medborgare på individnivå» og at massiv kartlegging av uskyldige er uakseptabelt.

Datatilsynet gjennomførte i 2009 en utredning om FRA-loven på oppdrag fra Fornyings- og administrasjonsdepartementet. Datatilsynet mener FRA-loven i ytterste konsekvens kan ha en nedkjølende effekt på ytringsfriheten til Norges befolkning. Muligheten for å bli overvåket kan medføre en usikkerhet som kan gjøre at enkelte vegrer seg for å kommunisere og innhente informasjon. I samhandling med hverandre tilpasser mennesker innhold og form etter kontekst og samtalepartner. En utenforstående og potensiell «medlytter» endrer forutsetningene for samhandlingen, også selv om samtalepartene «ikke har noe å skjule».

En del norske teletilbydere har morselskap i Sverige. Noen av disse bruker svensk infrastrukt

turen, også for norsk innenlandstrafikk. Datatilsynet påpekte i utredningen om FRA-loven at departementene burde vurdere å kreve at bruk av den svenske infrastrukturen opphører for innenlandstrafikk.

9.1.5 Politiregisterloven

Datatilsynet har siden 2003 etterlyst progresjon i arbeidet med ny politiregisterlovgiving, og er tilfreds med at det endelige utkastet i 2009 ble oversendt Stortinget (Ot. Prp 108 (2008-2009)).

Loven gir svært generelle bestemmelser som fremmer sentrale personverngarantier. Loven skal imidlertid ledsages av et omfattende forskriftsverk, og Datatilsynet mener det først er når forskriftene er laget at det kan bli tydelig om loven faktisk leder til bedret personvern innen politisektoren eller ikke. Datatilsynet vil følge nøye med på området.

Datatilsynet mener at loven i for stor grad gjør unntak fra grunnleggende personverngarantier, som rett til innsyn og informasjon, for politiets sikkerhetstjeneste (PST). Mest bekymringsfullt er det at det er opp til PST selv å vurdere hvorvidt de svært skjønsmessige unntakene kommer til anvendelse. Datatilsynet mener at denne tilliten bør ledsages av skjerpet kontroll med tjenesten, og etterlyser konkrete tiltak for å styrke kontrollarbeidet ved Stortingets EOS-utvalg.

9.1.6 Endringer i straffegjennomføringsloven etter Datatilsynets kontroll med kriminalomsorgen

I 2007 gjennomførte Datatilsynet kontroll med kriminalomsorgens behandling av personopplysninger. Kontrollen avdekket store mangler ved etterlevelsen av personopplysningslovens krav, herunder uklare ansvars- og myndighetsforhold og dårlig informasjonssikkerhet. Datatilsynet fant også grunn til å stille spørsmål ved om *Kriminalomsorgens sentrale forvaltnings* behandling av personopplysninger hadde tilfredsstillende rettslig grunnlag, og anbefalte at straffegjennomføringsloven ble endret.

Datatilsynet er svært tilfreds med at regjeringen, som en direkte konsekvens av kontrollen, har lagt frem forslag om endringer i straffegjennomføringsloven for å avklare ansvarsforhold og styrke det rettslige grunnlaget for behandling av personopplysninger i kriminalomsorgen. Datatilsynet stiller seg i det vesentlige positivt til de foreslåtte endringene.

9.1.7 Lovregulering av offentlige undersøkelseskommisjoners virksomhet

Regjeringen har lagt frem forslag om å lovregulere virksomheten til offentlige undersøkelseskommisjoner som etableres i forbindelse med hendelser av stor samfunnsmessig betydning, for eksempel en ulykke eller korrupsjon.

Datatilsynet mener at offentlige undersøkelser som hovedregel bør gjennomføres av etablerte forvaltningsorganer. Tilsynet er allikevel tilfreds med at det søkes etablert rettssikkerhetsgarantier i form av blant annet rett til informasjon og kontradiksjon for de personer som underlegges en offentlig undersøkelse.

Tilsynet mener imidlertid at det foreslåtte regelverket ikke fullt ut gir det vernet som personverndirektivet krever. Blant annet peker tilsynet på at den personkretsen som gis rettigheter etter loven er snevrere enn det personverndirektivet krever. Datatilsynet mener derfor at utkastet må harmoniseres med direktivet før regelverket eventuelt vedtas.

9.1.8 Omfattende endringer i utlendingsregelverket

I rapporteringsåret har det vært fremmet til sammen fem forslag om endringer i utlendingslov og -forskrift. Tilsynet mener at lovprosessen har vært fragmentarisk, og at det derfor har vært vanskelig underveis å få et helhetlig bilde av rettsutviklingen på området.

Datatilsynet reagerer generelt på at utlendingsforvaltningen blir stadig mer nærgående overfor enkeltpersoner, og viser spesielt til at nye regler vedrørende familiegjennomføring i sin ytterste konsekvens nødvendiggjør en kartlegging av når og hvor et enkelt barn har blitt unnfanget. Tilsynet mener at en slik utvikling skaper en stadig større ubalanse i forholdet mellom enkeltpersoner og offentlig myndighet.

Datatilsynet reagerer også på at ansatte ved asylmottak og omsorgssentre pålegges meldeplikt til utlendingsforvaltningen om forhold som er av betydning for de vedtak som skal treffes der. Tilsynet mener at departementet ikke har tatt hensyn til at asylmottak og omsorgssentre er å anse som midlertidige hjem, og savner at bestemmelsene er vurdert i forhold til EMK artikkel 8. Tilsynet stiller også spørsmål ved om de personer som pålegges meldeplikt har slik kompetanse som er nødvendig for å sikre tilfredsstillende kvalitet på de opplysningene som skal gis.

9.2 Tele og internett

9.2.1 Fildeling – avslag på søknad om konsesjon

Simonsen Advokatfirma søkte i 2006 Datatilsynet om konsesjon til å behandle personopplysninger som et ledd i bekjempelsen av ulovlig spredning av opphavsrettighetsbeskyttede åndsverk på Internett – ofte omtalt som ulovlig fildeling. Datatilsynet innvilget søknaden i november samme år, med en tidsbegrenset gyldighet på ett år. Konsesjon ble fornyet én gang. Konsesjonen har så langt gitt advokatfirmaet tillatelse til å samle inn og registrere IP-adresser som er observert i aktivitet på ulike fildelingsnettverk. Firmaets målsetning med denne informasjonsinnhenting har vært å danne bevisgrunnlag for straffeforfølgelse og erstatningssøksmål, rettet mot enkeltindivider mistenkt for brudd på åndsverklovens bestemmelser. En IP-adresse vil ikke nødvendigvis være egnet til å avsløre den enkelte fildelers identitet direkte, men via kobling med opplysninger fra internettleverandørene, vil det være mulig å indirekte identifisere den enkelte fildeler. Ettersom disse personopplysningene er beskyttet av det norske regelverket om elektronisk kommunikasjon, må det foreligge en rettslig kjennelse før informasjonen kan utleveres.

Advokatfirmaets søknad om ytterligere forlengelser, ble avslått ved Datatilsynets vedtak i juni 2009. Advokatfirmaet har klaget avslaget, og saken er oversendt til Personvernemnda for endelig avgjørelse.

9.2.2 Fødselsdato og andre tilleggsopplysninger på nummeropplysningstjenester

I 2009 har Datatilsynet hatt flere større saker der nummeropplysningstjenester på Internett har vakt stor forargelse hos publikum. Felles for disse er at det tilbys flere personopplysninger enn det som tradisjonelt har blitt ansett å være nummeropplysning, for eksempel fødselsdato. Tilbyderne bruker også opplysningene på nye måter, for eksempel gjennom sammenstillinger med andre opplysninger. Problematikken ble tatt opp av Datatilsynet i forbindelse med et tilsyn mot Lindorff Match AS allerede i april 2008.

Datatilsynet mottok i første kvartal 2009 en rekke henvendelser vedrørende publisering av fødselsdato og -år på nettsiden www.finnfirma.no. Datatilsynet kom frem til at det ville være i strid med personopplysningsloven å publisere både fødselsdato og -år, men at publisering av enten det

ene eller det andre ikke ville være i strid med en interesseavveining etter personopplysningsloven. Virksomheten innrettet seg etter dette, og Datatilsynet avsluttet saken.

I juni 2009 begynte *www.telefonkatalogen.no* (Eniro) å publisere fødselsår og -måned i tillegg til de tradisjonelle kontaktopplysningene som navn, adresse og telefonnummer. Datatilsynet mottok i den forbindelse mange hundre henvendelser på telefon, e-post og brev. Publikum opplevde publiseringen som et overtramp mot personvernet, og uttrykte at publiseringen gjorde det for enkelt å finne frem til hele fødselsdatoen, da fødselsåret ligger åpent på skatteliste. Etter kort tid valgte Eniro selv å fjerne informasjon om fødselsdato fra telefonkatalogens nettsider, og Datatilsynet avsluttet derved saken.

I september 2009 mottok tilsynet en rekke klager på nettstedet *www.iam.no*. Nettstedet er en tjeneste med kontaktinformasjon, men publiserte en rekke tilleggsopplysninger om de registrerte. Det gjaldt publisering av opplysninger om fødselsdato, stjerne-tegn, treff på vedkommendes navn på Google, samt opplysninger om hvilke roller de hadde i næringslivet. Tilsynet mottok mange klager fra publikum, som opplevde at en samlet publisering av så mange opplysninger var krenkende. Mange reagert i tillegg på at opplysningene var feilaktige, og omhandlet mindreårige og personer med hemmelige adresser og telefonnumre.

I løpet av vinteren foretok *Iam* en rekke endringer på nettsiden, blant annet ble fødselsdato erstattet med alder, og det ble publisert en reservasjonsløsning.

Iam-saken er ved årsskiftet snart ferdig behandlet i Datatilsynet. Under saksbehandlingen har tilsynet mottatt en redegjørelse fra de ansvarlige bak *www.iam.no*, samt en nærmere avklaring fra Post- og Teletilsynet av e-komforskriftens anvendelse på nummeropplysning med tilleggstjenester. Datatilsynet har sendt varsel om vedtak til *Iam*, og bedt de ansvarlige om å foreta utbedringer. Videre har tilsynet mottatt bekreftelse på at *Iam* vil etterkomme de varslede påleggene. Saken ventes ferdigbehandlet i februar 2010.

9.3 Barn og unge – rett til blanke ark

Dagens barn og unge får registrert og lagret opplysninger om seg selv i langt større grad enn det som var tenkelig få tiår tilbake. Allerede ved fødselen begynner det offentlige registrering av opplysninger om barnas helse, deres evner og oppførsel. Gjennom et normalt livsløp vil den totale informasjonsmengden om hver av disse bli

enorm. Konsekvensene for deres personvern er nærmest uoverskuelige.

Personvernutfordringene for barn og unge ligger blant annet i å sikre at opplysninger fra oppveksten ikke blir «bagasje» som barnet må ha med seg resten av livet. Dette gjelder særlig for opplysninger av sensitiv karakter, eller fra vanskelige perioder i livet. Datatilsynet mener at barn og unge i oppvekstfasen må kunne tillates å gjøre feil og dumheter, uten at dette skal hefte ved dem i all fremtid.

9.3.1 Mindreåriges samtykkekompetanse – etterkontroll av personopplysningsloven

Datatilsynet har i forbindelse med etterkontrollen av personopplysningsloven uttalt at det er behov for et styrket vern av mindreåriges personvern. Dagens personopplysningslov inneholder ikke en særlig regulering av mindreåriges personvern.

I Barneombudets supplerende rapport til FNs komité for barns rettigheter 2009, har ombudet uttrykt bekymring for at dagens lovgivning ikke i tilstrekkelig grad sørger for vern av barns privatliv. Ombudet påpeker at dagens regelverk forutsetter at foreldre tar gode valg for sine barn, og at det ikke tas høyde for at barn kan ha behov for vern mot foreldres eksponering av sine barn. Dette gjelder for eksempel i tilfeller hvor foreldre legger ut sensitiv informasjon i barnefordelings- og barnevernssaker på Internett, uten at informasjonen er tilstrekkelig anonymisert. Barneombudet har bedt komiteen om å anbefale Norge å ta nødvendige skritt for å sikre barn et godt rettslig vern av deres privatliv.

Datatilsynet foreslår en ny bestemmelse om barns rettigheter etter loven med en henvisning til hvilke bestemmelser som er relevante. Det bør blant annet reguleres at barns samtykkekompetanse skal avhenge av barnets alder. Samtykkekompetansen må samsvare med barnelovens og barnekonvensjonens system, hvor barnet gis gradvis større selvbestemmelsesrett på bekostning av foreldrenes samtykkekompetanse.

9.3.2 Spesielt om bruk og misbruk av opplysninger om egne barn

Datatilsynet har fått henvendelser om tilfeller hvor foreldre publiserer opplysninger om barna sine på Internett, ofte for å skape sympati for egen barnevern- eller barnefordelingssak. Opplysningene som publiseres i den forbindelse er ofte svært sensitive, og i mange tilfeller unntatt fra offentlighet, slik for eksempel sakkyndigvurderinger kan være.

Det finnes begrensninger i foreldres rett til å bestemme over egne barn. Dersom foreldre ikke sørger for nødvendig behandling av alvorlig sykdom eller skade, kan fylkesnemnda vedta at barnet allikevel skal ha behandling, jf. barnevernloven § 4-10. Bestemmelsen gjelder fysisk helbred, men tilsynet vil presisere at barnet i tillegg har krav på psykisk helbred og integritet. Datatilsynet mener derfor at noen også må kunne overprøve foreldrenes beslutning om å publisere opplysninger om sine barn på Internett. I disse sakene kan det hevdes at foreldrenes publisering har et opinionsdannende formål, og derved er beskyttet av ytringsfrihetsvernet. Det medfører at publiseringen faller utenfor Datatilsynets kompetanseområde, i henhold til personopplysningslovens § 7.

Barnekonvensjonens artikkel 16 understreker imidlertid at barn har en selvstendig rett til privatliv. Det taler for at foreldrenes ytringsfrihet om forhold som angår barnet er begrenset. Videre pålegger Barnekonvensjonens artikkel 3 de nasjonale myndigheter, herunder Datatilsynet, å la barnets beste være et grunnleggende hensyn ved all myndighetsutøvelse. Dette taler for at en publisering som foreldrene gjennomfører, og som krenker barnets personvern, ikke er beskyttet av ytringsfrihetsvernet, selv når formålet er opinionsdannende.

Hvilken kompetanse Datatilsynet har i disse sakene har ennå ikke blitt satt på spissen i praksis. Tilsynet ønsker allikevel at lovgiver klargjør hvilken kompetanse tilsynet har til å pålegge sletting i disse tilfellene.

Datatilsynet har arbeidet lenge med denne problemstillingen, og ser et akutt behov for tiltak på området. Tilsynet betviler imidlertid at den planlagte hjelpetjenesten, Slettmeg.no, uten myndighet til å fatte vedtak og ilegge sanksjoner, vil kunne bidra til å løse de alvorligste sakene hvor barn eksponeres av sine foreldre. Tilsynet har erfart at det i slike saker er nødvendig med vedtakskompetanse. Det må anses å være urealistisk å forvente at et barn på eget initiativ vil begjære sletting av informasjon om seg selv, når det er foreldrene som har lagt den ut. Et alternativ er å gi barnevernet en tydelig handlingsplikt når foreldre grovt krenker barnas personvern.

9.3.3 *Føresette sin tilgang på It's learning i skulen*

Læringsplattformer i skulen blir meir og meir vanleg, allereie frå barneskulen. Samstundes manglar

konkrete reglar for foreldre og føresette sin rett til innsyn i barna sine kontoar på desse plattformene. Barn har rett på privatliv og personvern, og Personvernkommissjonen skriv i si utgreiing at «på same måte som vaksne har krav på personvern på arbeidsplassen, har barn og unge krav på privatliv i skolen». Datatilsynet kom i 2009 med ei prinsipiell uttaling om dette.

Mange bruksområde

Eit av hovudproblema med plattformene er at dei har eit vell av kommunikasjonsmoglegheiter. I tillegg til at foreldre kan få tilgang til timeplanar, informasjonsbrev frå skulen og anna nyttig informasjon, kan elevane også chatte, sende e-post og diskutere med andre elevar og lærarar. Dette er kommunikasjon som foreldra vanlegvis ikkje har tilgang til. Datatilsynet stiller seg difor kritisk til at foreldra kan få slik informasjon, berre fordi innføring av dei elektroniske systema gjer det mogleg.

Ifølgje barneloven er barn ned i 7-årsalderen gjeve rett til sjølvbestemming i saker av personleg karakter. Datatilsynet meiner difor at dei delane av læringsplattformene som omfattar personleg kommunikasjon med andre, ikkje skal vere tilgjengelege for foreldra. Kva opplysingar foreldra kan få innsyn i må vurderast opp mot til dømes opplæringslova, samt kva opplysingar det vil vere naturleg å ha i samband med oppfølging av barnet.

Datatilsynet meiner at det må gjerast ei heilskapleg vurdering av kva for informasjon som kan seiast å tilhøyre barnet si private sfære. I ei slik vurdering vil eleven sin alder og funksjonane i plattformene vere naturlege faktorar som må diskutertast.

Foreldrekontoar

Datatilsynet legg også vekt på at foreldre og føresette i utgangspunktet vil kunne utøve innsynsrett på vegne av barna. Difor meiner Datatilsynet at den beste løysinga truleg vil vere å gje foreldra eigne kontoar slik at dei kan halde seg oppdatert på relevant informasjon. På denne måten vil det framleis vere eleven sjølv som bestemmer over passord og brukarnamn. Det er betre enn at elevane opplever «frivillig tvang», når dei må gje foreldra tilgang til alt eller ingenting. Datatilsynet tilrår også at ei slik ordning blir praktisert allereie frå skulestart, slik at kommunikasjonen mellom heim og skule blir ryddig.

9.3.4 *Elevlisten er et offentlig dokument*

Flere kommuner har kontaktet Datatilsynet med spørsmål om blant annet problemstillinger knyttet til friskoler sitt ønske om å kontakte elever i ungdomsskoletrinnet med informasjon om skoletilbud. På bakgrunn av dette tok Datatilsynet i 2007 opp spørsmålet med Justis- og politidepartementet. Datatilsynet oppfordret samtidig departementet til å forskriftsfeste et unntak fra offentlighet for elevlister i grunnskolen.

Den nye offentleglova med forskrift trådte i kraft fra 1. januar 2009, uten at det er gjort unntak for elevlister. I brev fra Justisdepartementet den 18. juni 2009 har departementet senere også stadfestet at elevlister er offentlig dokument, omfattet av hovedregelen om innsynsrett etter offentleglova. Dersom elevlistene bare inneholder informasjon om navn, adresse, telefonnummer og eventuelt fødselsnummer, er i utgangspunktet ingen deler av elevlisten unntatt fra innsyn etter offentleglova, sier Justisdepartementet i sin vurdering.

Taushetsplikten vil likevel gjelde dersom noen av elevene har hemmelig telefonnummer eller adresse, eller dersom adressen røper et forhold som må sies å være personlig, for eksempel at vedkommende bor på en barnevernsinstitusjon.

Skolene er ansvarlige

Datatilsynet oppfordrer skolene til å vurdere behovet for elevlister og utøve stor varsomhet med hensyn til utlevering av slike lister og andre opplysninger om elever i skolen. Det er viktig å vurdere risikoen for at opplysningene kan komme på avveier. En kan ikke se bort fra at utlevering av elevlister kan føre til uønsket bruk av personopplysninger om barn helt ned til seksårsalderen.

Kommunen bør samtidig vurdere selve innholdet i elevlistene. Etter Datatilsynets oppfatning må skolene for eksempel unngå å ha fødselsnummer i elevlistene. Slike lister bør heller ikke publiseres på Internett.

9.3.5 *Skadebegrensning for barn som har fått seksualiserende bilder av seg publisert på nett*

I forbindelse med at den såkalte Faremo-rapporten ble sendt på høring fra Justisdepartementet i mars 2007 viste Datatilsynet til sine erfaringer med at barn og unge støter på uforholdsmessig store problemer dersom bilde- eller filmmaterialet er lagt ut om dem på nettet. Materiale som de i ettertid ønsker fjernet. Når det gjelder bilder som

kan karakteriseres som barnepornografi, risikerer barn og unge også straffeforfølgelse dersom de selv forsøker å finne igjen bildene for å få dem fjernet.

Datatilsynet bad derfor departementet om å ta inn følgende forslag til tiltak:

«Kripos må tillegges ansvar for å bistå barn og unge med å fjerne publiserte bilder/filmer av seg selv».

Begrunnelsen for dette er at man med filterteknologien mot barneporno og straffebestemmelser (straffeloven § 204a) gjør det straffbart å søke etter barnepornografi selv om man har til formål å avdekke brudd på straffeloven. Dette gjør at man blir avhengig av politiets bistand for å søke etter og fjerne filmer eller bilder for å begrense skaden for barnet.

9.3.6 *Elevar sitt personvern i skulen – skuleprosjektet*

Datatilsynet fekk i 2009 tildelt ekstra midlar for å styrke personvernet i skulen frå Fornyings-, administrasjons- og kyrkjedepartementet (FAD). Prosjektet skal kartlegge og vidare utarbeide rettleingsmateriell om korleis eleven sitt personvern blir ivareteke i skulen.

Det er behov for både meir kunnskap om personverntilstanden i skulen, samt meir tilrettelagt informasjonsmateriell. Rettleingsmaterialet blir spesielt viktig, for det handlar ikkje berre om å sette ein standard, men også om å gje den nødvendige hjelpa som skal til for å gjere det riktig. Elevane er i ei formande fase i livet, der tankar om eigen integritet og fridom blir utvikla. Skulen bidreg ikkje berre med kunnskap, men også med haldningar og verdiar. Skulen er ein viktig normformidlar og utøvar av eksempelets makt. Det vil vere negativt om elevar gjennom erfaringar frå skulen får inntrykk av at dårleg personvern både er normalt og akseptabelt.

Prosjektet skal berre ta føre seg elevar i grunnskulen sitt personvern, ikkje personvernet til lærarar og andre tilsette. Prosjektet skil seg også klart frå Datatilsynet sitt undervisningsopplegg for skulane, «Du bestemmer». Medan «Du bestemmer» handlar om å bevisstgjere born og unge om eige personvern, skal dette prosjektet handle om skulen si ivaretaking av elevane sitt personvern.

Fleire emne er relevante for prosjektet personvern i skulen, og dette må vurderast opp mot prioriteringar og behov. Så langt er det klart at emne

om elektroniske læringsplattformer får prioritet. Kameraovervaking og overvaking av elevane sine pc-ar er også døme på emne som må bli behandla. Prosjektet er planlagt gjennomført i løpet av ein toårsperiode, og vil då vare fram til 2011.

9.4 Arbeidsliv

9.4.1 *E-postforskriften og innsyn i arbeidstakers e-postkasse*

Nye bestemmelser om innsyn i arbeidstakers e-postkasse trådte i kraft 1. mars 2009. Bestemmelsene er tatt inn i personopplysningsforskriftens kapittel 9.

Forskriften regulerer arbeidsgivers adgang til å gjøre innsyn i arbeidstakers e-postkasse, herunder vilkår for, og prosedyrer ved, innsyn. Bestemmelsene omfatter også arbeidstakers personlige område og andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten. Reglene gjelder så langt de passer også for universiteters og høyskoleers innsyn i studenters e-postkasse, og for organisasjoners og foreningers innsyn i frivilliges og tillitsvalgtes e-postkasse.

Bestemmelsene er preseptoriske, noe som innebærer at det ikke er adgang til å fastsette instruks, eller inngå avtale om arbeidsgivers innsyn, som fraviker bestemmelsene til ugunst for arbeidstaker. Forskriftsreguleringen er i hovedsak en kodifisering av Datatilsynets praksis på området.

Datatilsynet har merket en betydelig økning i antall saker som omhandler arbeidsgivers innsyn i e-post. Det har videre vært en merkbar tilvekst av telefoniske henvendelser om temaet. Økningen i saker, særlig i siste halvdel av 2009, kan tyde på at regelverket er blitt bedre kjent og mer tilgjengelig etter reguleringen. Et annet trekk er at det har blitt enklere for Datatilsynet å behandle sakene når vilkår for innsyn og prosedyrer for slikt innsyn er klarere regulert.

Saksbehandlingen viser at det fortsatt er mange som ikke kjenner til, eller ikke etterlever, bestemmelsene i personopplysningsforskriften. Videre erfarer Datatilsynet at atskillige arbeidsgivere mangler rutiner for avslutning av e-postkasse ved endt arbeidsforhold. Ofte er det mangler i informasjonen arbeidstaker får i forbindelse med gjennomføring av innsyn, og mangler ved prosedyrene for innsyn.

9.4.2 *Springsteknologi*

Datatilsynet har i 2009 foretatt flere kontroller mot virksomheters bruk av springsteknologi i arbeidslivet, og da særlig GPS-løsninger i virksomhetens egne kjøretøy. Bakgrunnen for kontrollene er de mange henvendelser tilsynet har mottatt fra både ansatte og arbeidsgivere. Henvendelsene til Datatilsynet skyldes dels en økende bruk av slike enheter i arbeidslivet, og dels fordi aktørene i arbeidslivet enten finner regelverket uklart eller at det hersker en del usikkerhet rundt hvilke regler som regulerer bruken av springsteknologi.

Datatilsynet har på bakgrunn av henvendelsene, samt de nevnte kontrollene, sett et stort behov for klarere retningslinjer på området. Datatilsynet vil derfor utarbeide retningslinjer for i hvilken grad det er adgang til å benytte GPS-løsninger i virksomhetens kjøretøy i tråd med personopplysningsloven.

Retningslinjene vil se nærmere på to formål som ofte brukes til å begrunne overvåking av virksomhetens biler, nemlig flåtestyring og dokumentasjon for virksomhetskjøring (elektronisk kjørebok).

Vurderingen av om GPS-løsninger i virksomhetens egne kjøretøy er lovlig eller ikke, vil ikke kunne avgjøres på bakgrunn av personopplysningsloven alene. Forholdet vil også berøre øvrig lovgivning, som skatteloven og arbeidsmiljøloven. Datatilsynet er i dialog med ansvarlige myndigheter for å få avklart spørsmålene.

9.4.3 *Internkontrollprosjekt mot tillitsvalgte*

På bakgrunn av en sak som berørte manglende systemer for internkontroll i en arbeidstakerorganisasjon, har Datatilsynet satt i gang et prosjekt med særlig fokus på dette. Det har vist seg at behandlingen av personopplysninger i fagforeninger på lokalt nivå, og da særlig på tillitsvalgnivå, medfører store utfordringer. Årsaken til dette er blant annet hyppig utskifting av tillitsvalgte, sviktende tilretteleggelse fra organisasjonen sentralt, manglende kompetanse hos den enkelte, samt et regelverk som ikke uten videre er tilgjengelig for personer uten erfaring på feltet.

Interessen og engasjementet for prosjektet har vært stor blant fagforeningene, og et systematisk arbeid for å prøve å få behandlingen av personopplysninger i tråd med personopplysningsloven har stått på agendaen til organisasjonene. Det har blitt avholdt flere møter med samtlige av de største fagforeningene. I tillegg har tilsynet gitt og mottatt skriftlige innspill, samt holdt foredrag for

deler av tillitsvalgtapparatet. Arbeidet har i flere av organisasjonene kommet langt, og Datatilsynet vil følge prosessen videre.

Datatilsynet vil i løpet av 2010 utarbeide en veiledende oversikt over hvilke rutiner som minimum må innarbeides på tillitsvalgnivå, for å sikre at behandlingen av opplysninger også på lokalt nivå skjer med tilfredsstillende sikkerhet. Tilsynet vil videre stille opp på foredrag/opplæring av tillitsvalgte i regi av den enkelte forening.

9.5 Etterkontroll av personopplysningsloven

Dagens personopplysningslov trådte i kraft 1. januar 2001. Da loven ble utarbeidet tok Justis- og politidepartementet til orde for at det burde foretas en etterkontroll av regelverket etter en femårsperiode. Dette ble tiltrådt av Justiskomiteen. For å følge opp dette ga Justisdepartementet og Moderniseringsdepartementet professor dr. juris Dag Wiese Schartum og førsteamanuensis dr. juris Lee Bygrave i oppdrag å utrede ulike problemstillinger på dette området. I henholdsvis 2006 og 2008 ble rapportene «Utredning av behov for endringer i personopplysningsloven» og «Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12» forelagt Justisdepartementet. Videre skrev Datatilsynet i 2005 en rapport om kameraovervåking og bestemmelsene som regulerer denne formen for behandling av personopplysninger.

I meldingssåret ble disse rapportene sammen med Justisdepartementets høringsnotat sendt ut på høring.

Lovrevisjonen ga Datatilsynet anledning til å komme med innspill om hvordan regelverket tilsynet er satt til å forvalte, fungerer i praksis, samt komme med forslag til endringer som vil kunne styrke personvernet eller gjøre regelverket bedre tilpasset dagens virkelighet. Arbeidet med høringsuttalelsen fikk derfor høy prioritet, og involverte mange av tilsynets medarbeidere. Den uensartede behandlingen de ulike delene av loven var gitt i underlagsmaterialet til høringen, gjorde det vanskelig å danne seg en samlet oversikt over forslag til endringer av regelverket og resonnementene som lå til grunn for forslagene. Videre bar deler av utredningene preg av å være teoretiske avhandlinger, lite egnet som bidrag til å løse de problemstillinger som personvernet står overfor i praksis.

Lovens oppbygning

Datatilsynet har erfart at helt sentrale poenger i loven ikke blir fanget opp av de som forsøker å gjøre seg kjent med regelverket, eksempelvis hvem som er forpliktet av lovens krav og hvilke hensyn loven skal ivareta. Tilsynet har derfor foreslått en endring av formålsbestemmelsen for å presisere at loven gjelder alle og enhver som behandler personopplysninger. Tilsynet deler også Justisdepartementets oppfatning om at den pedagogiske oppbygningen av loven kan forbedres på enkelte områder, for eksempel bør grunnkravene til behandling av personopplysninger fremkomme tidligere og klarere enn det som er tilfellet i dagens regelverk.

Avdøde personer

Tilsynet har også tatt til orde for at avdøde personer skal gis et styrket vern, i hvert fall i en viss tid etter personens død. Hensynet til vedkommendes ettermæle og de pårørende tilsier dette. Personopplysningsloven slik den er i dag beskytter ikke avdøde personer, noe som i ulike sammenhenger gir uheldige utslag.

Kravet om et definert og saklig formål

Erfaring fra Datatilsynets kontrollarbeid og ulike henvendelser fra publikum og virksomheter vitner om mangelfull kunnskap om regelverket som beskytter personvernet. Det gjelder for eksempel vekten på *formålet ved behandlingen* – det faktum at formålet legger streng begrensning på hva opplysningene senere kan benyttes til. I mange tilfeller samles det inn opplysninger om personer uten at formålet er klart definert på forhånd. Datatilsynet foreslår derfor at dette tydeliggjøres og defineres som en av legaldefinisjonene.

Ytringsfrihet og personvern

Avveiningen mellom ytringsfrihet og hensynet til den enkeltes personvern kan by på utfordringer, og det er vanskelig å trekke opp klare retningslinjer for når personvernehensyn bør veie tyngst. I henhold til dagens lovgivning er det kun et fåtall av lovens bestemmelser som kommer til anvendelse på behandling av personopplysninger som skal tjene kunstneriske, litterære eller journalistiske, herunder opinionsdannende formål, jf. lovens § 7. Etter Datatilsynets vurdering har unntaket fått et for vidt nedslagsfelt. Dagens regulering og praktiseringen av den har ikke tatt høyde

for Internettets utbredelse og mulighetene Internett gir til å publisere personopplysninger for allmennheten. Tilsynet anbefaler å fjerne uttrykket opini-
onsdannende formål for å begrense unntakets nedslagsfelt og på den måte styrke personvernet når man er utenfor ytringsfrihetens kjerneområde.

Informasjonsplikt

Informasjonsplikten er grunnleggende for personvernet. Dagens bestemmelser gir ikke den behandlingsansvarlige noen plikt til å informere den registrerte om at personopplysninger er kommet på avveie. Datatilsynet foreslår derfor at det pålegges en uttrykkelig varslingsplikt for den behandlingsansvarlige når en uautorisert utlevering av personopplysninger har funnet sted.

Konsesjon og meldeplikt

I rapportene som ligger til grunn for høringen tas det til orde for at omfanget av konsesjonsplikten for behandling av personopplysninger skal reduseres. Argumentene for forslaget var at dagens ordning er for omfattende og fører til en lite hensiktsmessig bruk av tilsynets ressurser. Datatilsynet foreslår i høringen en alternativ løsning som innebærer at konsesjonsplikten opprettholdes som i dag, men at tilsynet gis en adgang til å gi dispensasjon. Datatilsynet bevarer på denne måten muligheten for forhåndskontroll, samtidig som behandling av opplysninger som ikke representerer noen reell fare for personvernet kan unntas fra konsesjonsbehandling. Forslaget fra tilsynet gjør endringer i bestemmelsene om meldeplikt mindre påkrevet.

Kameraovervåking

Datatilsynet erfarer at overvåkingstrykket er økende, og mener det er behov for en moderat innstramning av lovens krav. Datatilsynet påpeker også problemstillingen med lydopptak i tilknytning til kameraovervåking. Lyd- og bildeopptak sammen gir muligheter til et større inngrep i personvernet.

Mindreåriges personvern

Personopplysningsloven inneholder ingen særlige bestemmelser om barn og unges personvern. Datatilsynet uttalte seg også om dette i høringsuttalelsen, jf kapittel 9.3 *Barn og unge*.

9.6 ID-kort og e-signaturer

9.6.1 Ny kravspesifikasjon for PKI i offentlig sektor

Direktoratet for forvaltning og IKT (Difi) sendte i meldingsåret ut forslag til ny kravspesifikasjon for PKI i offentlig sektor. PKI står for Public Key Infrastructure, og er en løsning for administrasjon, utsendelse og bruk av digitalt sertifikat over datanett. Dette gjør det mulig for brukerne å autentisere seg, identifisere seg eller kryptere meldinger over Internett. Datatilsynet påpekte flere mangler ved utredningen.

Datatilsynet ønsker en klarere anvendelse av prinsippene bak PKI. Blant annet ligger det kvalitetssikringsmekanismer i teknologien, og disse er ikke tatt med i tilstrekkelig grad. Kravspesifikasjonen bør legge opp til bruk av PKI hver gang en handling krever identifisering, for eksempel om en ber om tilgang til beskyttelsesverdige personopplysninger om seg selv. I høringsuttalelsen stilte Datatilsynet spørsmål om høringsforslaget i tilstrekkelig grad tar hensyn til kravene i lov om elektronisk signatur.

Datatilsynet reagerer blant annet på bruk av sentralisert lagring for bruk av PKI via tredjeparter, som for eksempel nettbanker. En slik sentralisert lagring åpner for stor risiko.

Det er positivt at den nye spesifikasjonen har fått på plass løsninger både for privat og virksomhetsrelatert bruk. Tilsynet savner likevel profesjonssertifikater egnet til å kunne verifisere en persons profesjon.

10 Kameraovervåking

I årsmeldinga for 2008 fekk kameraovervåking ein del omtale, overordna trendar blei skildra og det blei gitt nokre perspektiv på utviklinga på feltet. I denne årsmeldinga blir derfor berre to forhold som har peikt seg ut i 2009 nemnt.

Kameraovervåking ser ut til å vere eit interessant tema for mange. Temaet blir ofte dekt i pressa. Også i 2009 har det vore mange spørsmål frå publikum til Datatilsynet om kameraovervåking.

Ein stor del av spørsmåla kjem frå verksemder og personar som ønskjer å nytte kamerovervåking og som søker råd om kva som er akseptabelt og kva reglar som gjeld. Fleire spørsmål kjem dessutan frå publikum som reagerer negativt på eit konkret tilfelle av overvåking, til dømes på arbeidsplassen, overvåking i det offentlege rommet eller naboen si kameraovervåking. I mange saker blir det yttra ønskje om at Datatilsynet kjem på kontroll.

Statistikk over svar per telefon og e-post av Datatilsynets juridiske rettleiingsteneste, syner at om lag 10 prosent av alle spørsmål til denne tenesta handlar om kameraovervaking. I den ordinære saksbehandlinga er prosentdelen litt lågare. Blir kontroll og høyringssaker haldne utanfor, er om lag 4 prosent av alle nye saker i 2009 om kameraovervaking.

Kartlegginga av kameraovervaking i Noregs største byar er no avslutta. I løpet av året vart Tromsø, Bergen og Oslo kontrollert, og tidlegare har ein sett på overvaksingsgrada i Trondheim og Kristiansand. Det syner seg at det er stor variasjon i grada av overvaking, der nærare halvparten av dei kontrollerte verksemdene i Oslo nytta seg av kameraovervaking, gjorde berre 18 prosent det same i Trondheim. Det er heller ikkje noko spesifikt mønster når det gjeld typen butikkar eller verksemdar som har overvaking. Mange av verksemdene med varer av høg verdi, som gullsmedar, våpenforrentingar og sportsbutikkar hadde ikkje overvaking, medan nesten alle kioskar hadde det.

Det er viktig å understreke at myten om at alle har kameraovervaking syner seg å ikkje stemme. Årsaka til at Oslo skil seg markant ut er truleg resultat av høgt innbyggjartal, mange kjedeverksemdar med felles regelverk, samt tettleiken av verksemdar og butikkar. Verksemdene si oppleving av tryggleik vil også spele inn.

Alle tilsyna er gjennomført i tilnærma samanliknbare gater i dei ulike byane. I Oslo valde ein, i tillegg til å kontrollere Karl Johans gate, også å gjere ei synfaring i to gater for å sjå på skilnader mellom aust og vest i byen. Dette var ein meir uformell kontroll der det ikkje vart fatta vedtak. I Smalgangen (aust) hadde 41 prosent av verksemdene overvaking, medan tilsvarande tal for Bogstadveien (vest) var 28 prosent. I Smalgangen var det også meir utprega fasadeovervaking enn på vestkanten. Talet på kamera vart også undersøkt i dei to gatene, og tilsynet stiller seg mellom anna kritisk til at mange av restaurantane og serveringsstadene overvaka gjestene sine. I Smalgangen hadde ein restaurant til dømes åtte kamera som overvaka både gjester og tilsette. Dei fleste vil forvente ein viss diskresjon på slike stader, samt å ha høve til å sitte uforstyrra over lenger tid.

Kontrollane har også undersøkt om verksemdene overheld melde- og varslingsplikta, altså om dei sender melding til Datatilsynet, og om overvakinga er godt skilta i lokala. Resultatet av desse undersøkingane har vore nedslåande i alle byane. I Tromsø braut 90 prosent eitt eller begge krava, i Bergen braut 83 prosent regelverket og i Oslo var talet 81 prosent. Datatilsynet har forståing for at

næringsdrivande ynskjer å sikre verdiane i butikkane, men det må skje i tråd med regelverket. I tillegg er eit poeng med å varsle om kameraovervaking å hindre at tjuveri skjer, og det tilsynet er difor overraska over at så mange ikkje overheld varslingsplikta på ein god måte.

Sjølv som etterleving av regelverket har vore nokså dårleg, er det grunn til optimisme. På bakgrunn av kontrollane ser tilsynet at fleire av dei store butikkjedene som har vorte kontrollerte i fleire av byane, har innført betre rutinar både for varsling og melding av kameraovervaking.

Samarbeid med NELFO

I 2009 har Norsk Teknologi og bransjeforeininga NELFO laga ein bransjespesifikasjon. Formålet er å definere kva kompetanse installasjonsbedriftene må ha, og slik sikre at kameraovervaksingsanlegg har rett teknisk kvalitet innanfor gjeldande regelverk. Ei viktig side her er kunnskap om personvern og regelverket knytt til dette emnet.

Bransjespesifikasjonane har bransjen sjølv utvikla. Datatilsynet har, som ein sjølvstendig part, kome med råd knytt til personvernet. Det er lagt ned mykje arbeid med å lage bransjespesifikasjonen og kursopplegg, også frå Datatilsynet si side.

Personvern og regelverk har fått stor plass i kursopplegget som er utvikla. Datatilsynet har, i alle fall i startfasa, sagt seg villig til å stille med sitt personell for undervisning om personopplysningsloven og personvern i samband med kameraovervaking. Første kurs vart halde i november 2009 og fekk særse gode tilbakemeldingar frå deltakarane, og det er planlagt nytt kurs på nyåret.

Det er kunden, og ikkje installatørar eller leverandørar av kameraovervaking, som har ansvaret for at personvernregelverket blir følgt. Samstundes vurderer Datatilsynet det slik at installasjonsbedriftene har ei nøkkelrolle når det gjeld å betre ivaretakinga av personvernet. Auka kunnskap og større ansvarskjensle hjå installasjonsbedriftene vil bety mykje. Nettopp difor er bransjeforeininga sitt eige initiativ både viktig og gledeleg. At bransjeforeininga har laga ein bransjenorm er eit viktig steg, men ikkje nok i seg sjølv; installasjonsbedriftene må følge opp. Venteleg gjer dei det, men ved utløpet av meldingsåret har det gått for kort tid til at dette er avklara.

10.1 Samferdsel

10.1.1 Tilsyn – elektronisk billettering

Våren 2009 gjennomførte Datatilsynet tre tilsyn hos tilbydere av offentlig transport. Det sentrale

temaet for tilsynene var behandlingen av personopplysninger i forbindelse med elektroniske billettering – det vil si elektroniske reisekort.

For Datatilsynet er det sentralt at man også i fremtiden kan ferdes fritt i samfunnet uten å måtte legge igjen elektroniske spor om hvor man har vært og når reisen fant sted. Etter tilsynets vurdering er dette en forutsetning for reell fri ferdsel og ivaretagelse av privatlivets fred.

Det er viktig for personvernet til de reisende at det er mulig å benytte ordinære offentlige transporttilbud uten at det blir registrert informasjon om den enkeltes bevegelser. Når det gjelder de personlige elektroniske billettene er det et sentralt poeng at det ikke lagres flere opplysninger enn strengt tatt nødvendig, og at de personopplysninger som behandles slettes så raskt som mulig. Tilsynet har derfor pålagt selskapene å slette identifiserbare reiseopplysninger umiddelbart etter at reisen er betalt.

Når det gjelder periodebilletter, eksempelvis et månedskort, har Datatilsynet konkludert med at opplysninger om den første stemplingen skal slettes senest tretti dager etter at gyldighetsperioden for billetten er utløpt. Opplysninger om de enkelte reiser som finner sted innefor billettens gyldighetsperiode skal ikke kunne knyttes til den enkelte reisende. Opplysninger som eventuelt må registreres skal være anonyme. Tilsynet er av den oppfatning at virksomhetens behov for å foreta en avregning av billettinntektene seg i mellom, samt deres behov for å tilpasse rutetilbudet etter etterspørselen, vil kunne ivaretas ved behandling av anonyme opplysninger.

10.1.2 Tilsyn – strekningsvis automatisk kontroll (SATK)

Datatilsynet gjennomførte også et tilsyn hos Statens vegvesen for å kontrollere ivaretagelsen av personvernet i forbindelse med såkalt strekningsvis automatisk trafikkontroll (SATK). Dette tiltaket går ut på å beregne gjennomsnittshastigheten til passerende kjøretøy ved å måle hastigheten ved to punkter. Alle passerende kjøretøy blir fotografert i begge punkter, ikke bare de som holdt for høy fart, slik tilfellet er ved ordinær ATK. Altså blir også lovlydige sjåfører fotografert.

På kontrolltidspunktet var det ikke klart hvem som er behandlingsansvarlig for tiltaket, politiet eller Statens vegvesen. Først i ettertid ble det bekreftet at Statens vegvesen er behandlingsansvarlig. Under tilsynet kunne det heller ikke vises til et rettslig grunnlag for behandling av personopplysninger i forbindelse med SATK. Datatilsynet har bedt Statens vegvesen om å redegjøre for

dette. Etter tilsynets vurdering krever SATK hjemmel i lov. Uten gyldig behandlingsgrunnlag er tiltaket ulovlig.

Statens vegvesen ble også bedt om å vurdere en mer personvernvennlig løsning hvor kun sjåfører som bryter fartsgrensen blir avbildet. En slik løsning er benyttet i Sveits. Det er også sentralt for Datatilsynet at de som ferdes på norske veier på en tydelig måte blir gjort oppmerksomme på hvor strekningene der målingene finner sted begynner, og hvor de slutter, samt varsles der og da dersom de er målt i for høy hastighet.

10.1.3 Kontrollar av bomselskap

Datatilsynet har i løpet av våren 2009 kontrollert behandling av personopplysningar hjå to bomselskap. Kontrollane synta at kundane får for dårleg informasjon om handtering av personopplysningar, og at sletterutinane er mangelfulle.

I kontrollane såg tilsynet nærare på selskapa E18 Vestfold AS og Fjellinjen. Temaet for kontrollen var passeringsopplysningar, det vil seie informasjon om passerande køyrety, bomstasjonen som er passert og tidspunkt for passeringa.

Dårleg informasjon til kundane

Felles for begge desse kontrollane var at kundane ikkje får god nok informasjon. Kva data ein samlar inn i samband med passering, kor lenge passeringssdata eller bilete blir lagra, kvar og kor tid bileta blir tekne – blir det ikkje opplyst om.

Selskapa lagrar passeringssdata i 12 månadar for kundar som betaler på førehand. Datatilsynet meiner dette er for lenge, sidan det ikkje føreligg noko tilfredsstillande føremål for å lagre desse opplysningane så lenge.

Datatilsynet såg også at ein samla inn fleire personopplysningar enn nødvendig, mellom anna var kamera feilaktig stilt inn slik at ein kunne sjå både førar og passasjer.

Datatilsynet kritiserte sikringa av brukarprofilane til 40 000 kundar av bomselskapet E18 Vestfold AS. Tryggleiken ved pålogging til profilen på nett var ikkje bra nok, og mange av kundane kan difor ha ein ubeskytta profil på Internett med passeringssdata og andre personopplysningar. Den same problematikken gjeld også for Fjellinjen, sjølv om 180 000 av dei 600 000 kundane her kan ha sikra sin nettpofil.

Datatilsynet meiner det er overhengande fare for at uvedkomande kan gjennomføre urettmessig overvaking av køyretypasseringar.

10.2 Velferd, forskning og helse

10.2.1 *Utfordrende personvern i samhandlingsreformen*

I meldingsåret gav Datatilsynet en kritisk høringsuttalelse til forslag fra Helse- og omsorgsdepartementet om endringer i helseregisterloven og helsepersonelloven i forbindelse med samhandlingsreformen. I reformen ligger blant annet et ønske om å åpne for tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av liknende felles registre for ulike virksomheter.

Datatilsynet peker spesielt på faren for uthuling av taushetsplikten, og viser til allerede kjente mangler ved informasjonssikkerheten ved flere av landets helseforetak. Etter Datatilsynets oppfatning vil personvernet kunne bli sterkt svekket om man åpner for tilgang mellom helseforetakene før forholdene internt ved hvert enkelt helseforetak er tilfredsstillende.

Stortinget vedtok lovendringene i juni 2009, etter å ha kommet med enkelte justeringer. Blant annet ble det opprinnelige forslaget om at pasientene bare skulle ha reservasjonsrett for tilgang til helseopplysninger på tvers av virksomheter endret til et krav om aktivt samtykke. Pasientene fikk også en klar, lovfestet rett til innsyn i journallogg.

Både Helse- og omsorgsdepartement og Stortinget forutsetter at det skal foreligge en forhånds-vurdering av om opplysninger i journal kan deles med annet helsepersonell. I utgangspunktet tenker departement og Stortinget at denne vurderingen skal foretas ved registreringen av opplysningene. Det er også klart forutsatt fra Stortingets side at før tilgang på tvers kan finne sted, må journalene først være strukturert på en slik måte at det kun gis tilgang til nødvendige helseopplysninger.

Dette innebærer at det må gjøres store tilpasninger i de elektroniske pasientjournalene før de vedtatte lovendringene kan utnyttes. Problemene rundt intern og ekstern tilgangsstyring er mulige å løse, men det vil kreve betydelige ressurser. Datatilsynet er bekymret for at en presset økonomisk situasjon i helsetjenesten kan medføre at dette arbeidet får lav prioritet.

Datatilsynet vil kreve at ingen åpner sine journalsystemer for ekstern tilgang før informasjonssikkerheten er tilfredsstillende ivarettatt.

Ønske om samarbeid om forskrift

Et utkast til en forskrift om informasjonssikkerhet ved samhandling i helsesektoren ble utarbeidet av

departementet i forbindelse med høringen til lovendringene. Datatilsynet fant det sterkt beklagelig at forslaget til forskrift ikke i nevneverdig grad stiller andre eller strengere krav enn det som allerede følger av gjeldende regelverk.

Datatilsynet, som faginstans, har som hovedoppgave å stille både overordnede og konkretiserende krav til sikring av konfidensialitet, integritet og tilgjengelighet. Forarbeidene til helseregisterloven fastslår at særlige sikkerhetskrav for behandling av helseopplysninger i forskrift må fastsettes i tett samarbeid med Datatilsynet (Ot.prp. nr. 5 (1999-2000) side 195). Datatilsynet har på bakgrunn av dette anmodet departementet om samarbeid omkring utarbeidelse av sikkerhetsforskriften. Et slikt samarbeid pågår ikke når denne årsmeldingen utarbeides.

Vil man hjemle en vid tilgang til pasientjournaler for NAV, politi og forsikringsselskaper?

Den foreslåtte forskriften legger opp til en stor utvidelse av personkretsen som kan få direkte tilgang til pasientjournaler. Den eneste skranken som settes for andre formål enn medisinsk behandling, er taushetsplikten. Dette innebærer at man åpner for at enhver som kan kreve å få utlevert opplysninger fra pasientjournaler, også skal kunne få direkte tilgang til journalen.

En slik utvidelse av adgangen til å kunne «forsyne seg selv» i journalsystemene vil være alvorlig for personverntilstanden i Norge. Forslaget fremstår både som dårlig begrunnet og mangelfullt utredet.

Lovfestet rett til innsyn i journallogg

De vedtatte endringene lovfester en rett for pasienten til innsyn i loggen over personer som har lest deres journal (journallogg). Datatilsynet er positivt til endringen, men har likevel påpekt at journalloggen for de fleste vil gi liten informasjon.

Etter Datatilsynets mening bør retten til innsyn utvides med at den behandlingsansvarlige får plikt til å bistå og veilede pasienten med å forstå loggens innhold. Uten veiledning kan innsynsretten bli illusorisk.

10.2.2 *Forslag til nytt unntak fra helsepersonells taushetsplikt*

Helse- og omsorgsdepartementet har i meldingsåret foreslått en ny bestemmelse i helsepersonelloven § 29 b til å gi dispensasjon fra taushetsplik-

ten når formålet er kvalitetssikring, administrasjon, planlegging eller styring av helsetjenesten.

Datatilsynet er bekymret over at det stadig lovhjemles nye unntak fra helsepersonellens taushetsplikt, og særlig denne foreslåtte dispensasjonshjemmelen. Den vil gi departementet en svært vid fullmakt, som på sikt kan medføre en betydelig uthuling av helsepersonellens taushetsplikt. Dette medfører at pasientene står i fare for å miste kontrollen med sine helseopplysninger.

Forslaget må ses i sammenheng med ovennevnte lovendringer i helseregisterloven og helsepersonelloven, og åpner opp for at en utvidet personkrets kan gis direkte tilgang til pasientjournaler for en rekke nye formål uten pasientenes samtykke.

Unntakene fra taushetsplikten har etter hvert blitt mange uten at betydningen av dette har vært utredet. Datatilsynet understreker viktigheten av å holde oversikten over hvilken betydning det har for personvernet og tilliten mellom helsepersonell og pasient at det stadig vedtas nye unntak fra taushetsplikten. Datatilsynet vil i denne sammenheng spesielt peke på at formålet med taushetsplikten også er å sikre at personer ikke unnlater å oppsøke helsetjenesten i frykt for informasjonflyt.

10.2.3 *Åstedsundersøkelser ved plutselig og uventet småbarnsdød*

Regjeringen besluttet i 2008 å opprette et tilbud om dødsstedsundersøkelser ved plutselig og uventet barnedød. Undersøkelsene skal være frivillig for foreldrene, og blir å anse som en del av helsehjelpen til det døde barnet.

Datatilsynet mener at undersøkelsene lett får preg av å være politietterforskning. Det vises til at det er et uttalt formål å avdekke tilfeller av mishandling og annen omsorgssvikt fra foreldrene, og at undersøkelsene også skal gjennomføres av personer med politifaglig realkompetanse. Tilsynet frykter derfor at ordningen i enkelttilfeller innebærer en faktisk omgåelse av straffeprosesslovens krav om skjellig grunn til mistanke for at en politietterforskning skal iverksettes.

Regjeringen har i inneværende år besluttet at Folkehelseinstituttet skal iverksette og administrere ordningen, som en del av helsetjenesten. Den behandling av personopplysninger som finner sted vil etter dette reguleres av pasientrettighetsloven og helsepersonelloven, og faller i hovedsak utenfor Datatilsynets ansvarsområde.

Datatilsynet har i brev til departementet bemerket at helselovgivningen ikke er utarbeidet med tanke på denne type undersøkelser, og at

ordningen derfor uansett ikke bør innføres uten en forutgående lovbehandling. Tilsynet mener at regjeringen ikke har tatt tilstrekkelig hensyn til at foreldrenes menneskerettigheter brytes dersom en undersøkelse skjer uten gyldig samtykke, og peker på at det å hente inn samtykke fra foreldrene byr på store utfordringer – også etter helselovgivningen.

10.2.4 *Sentrale helseregistre bør ikke samles*

I forbindelse med Datatilsynets kontroll med Kreftregisteret høsten 2009, og alvorlige funn som ble avdekket i den forbindelse, er det av helsemyndighetene reist spørsmål om kreftregistrene bør overføres til Folkehelseinstituttet.

Datatilsynet er tilfreds med at Helse- og omsorgsdepartementet ønsker å sikre bedre etterlevelse av helseregisterlovgivningen for fremtiden, men mener dette må gjøres på andre måter enn å legge ansvaret for alle de sentrale helseregistrene hos en enkelt behandlingsansvarlig.

Dersom de sentrale helseregistrene samles hos en virksomhet utfordres den grunnleggende forutsetningen om at de sentrale helseregistrene skal holdes adskilt. Tilsynet frykter at man i realiteten går et langt skritt i retning av å opprette ett altomfattende, sentralt helseregister.

Det er betenkelig å legge ansvaret for en så omfattende samling av helseopplysninger til en virksomhet som for eksempel Folkehelseinstituttet, som selv er en betydelig bruker av de data som forvaltes. Blanding av rollene som ansvarlig forvalter og aktiv bruker av opplysningene gir rom for internt misbruk som nærmest er umulig for tilsynsmyndighetene å avdekke.

10.2.5 *Lov om medisinsk og helsefaglig forskning*

Lov om medisinsk og helsefaglig forskning trådte i kraft 1.juli 2009, og skulle bidra til å gjøre det enklere for forskeren å få oversikt over prosess og plikter. Ikrafttredelsen av loven har fått store konsekvenser for Datatilsynets arbeidsoppgaver. Dette fordi Datatilsynet ikke lenger forhåndsgodkjenner medisinsk og helsefaglig forskning.

Datatilsynet har både før og etter vedtakelsen av loven uttalt at den er uklar, både i seg selv, og når det gjelder forholdet til omkringliggende regelverk. Vanskelighetene gjelder blant annet fastsetting av lovens saklige virkeområde, hvilke krav som skal stilles til sikring av opplysningene (informasjonssikkerhet), og avklaring av de invol-

verte offentlige myndighetsorganers ansvarssområder.

Datatilsynet vil også påpeke at det er en vesentlig mangel ved helseforskningsloven at den ikke inneholder egne bestemmelser om informasjonsplikt. Informasjonsplikten er nedfelt både i personopplysningsloven og helseregisterloven, og gjelder supplerende, siden dette ikke er spesielt regulert i helseforskningsloven. Det ser imidlertid ut til at mange forskere ikke får med seg at de har en plikt til å informere. Forskningsdeltakerens rett til innsyn etter helseforskningsloven er illusorisk hvis de ikke informeres om at det blir forsket på dem.

Datatilsynet frykter at helseforskningsloven vil svekke forskningsdeltakernes personvern, selv om det er uttrykkelig fastsatt av lovgiver at loven ikke skal medføre vesentlig materielle endringer. Det at godkjenningskompetanse er overført fra Helsedirektoratet og Datatilsynet til de etiske forskningskomiteene kan i seg selv føre til en endret praksis. Komiteene er i langt større grad enn direktoratet og Datatilsynet knyttet til forskningsmiljøene.

Datatilsynet er spesielt bekymret for en endret praksis når det gjelder kravet til samtykke, og informasjonsplikten når prosjektet ikke er basert på samtykke. Datatilsynet frykter også at informasjonssikkerheten i praksis ikke vil bli ivaretatt tilfredsstillende. Det er også fare for at det etableres helseregistre etter helseforskningsloven, som etter helseregistersloven §§ 7 og 8 skulle vært forskriftsregulert. Det har neppe vært lovgivers intensjon at det er større adgang til å opprette forskningsregistre etter helseforskningsloven enn etter helseregisterloven.

Datatilsynet vil i fremtiden aktivt benytte seg av sin tilsynskompetanse til å følge utviklingen på helseforskningsområdet.

10.2.6 *Forslag om etablering av et personidentifiserbart nasjonalt register over hjerte- og karlidelser*

Det har i meldingsåret blitt fremmet forslag fra Helse- og omsorgsdepartementet om å etablere et sentralt register for hjerte- og karlidelser. Registeret er foreslått å være direkte identifiserbart og obligatorisk. Dette innebærer at registeret vil inneholde direkte identifiserende opplysninger, samt at det ikke skal innhentes samtykke fra den enkelte pasient før registrering. Det skal heller ikke være mulig å reservere seg mot å bli registrert.

Hjerte- og karregisteret er bare ett av flere sentrale registre forskningsmiljøet jobber med å forskriftshjemle, og vil fort danne en «mal» for lignende registre for andre sykdomsgrupper. Datatilsynet understreker derfor betydningen av å ha en prinsipiell tilnærming til hjemmelsgrunnlaget for etablering av slike registre.

Datatilsynet fremhever at sentrale helseregistre som hovedregel bør etableres med samtykke fra pasienten. Dette gjelder etter tilsynets vurdering spesielt når opplysningene i registeret skal være direkte identifiserbare. Registere som ikke baseres på samtykke må derfor være pseudonymiserte, eller på annen måte være underlagt et særlig vern.

Etter Datatilsynets vurdering innebærer etablering av et direkte personidentifiserbart hjerte- og karregister en stor trussel for personvernet. Datatilsynet kan ikke se at det foreligger andre hensyn enn rene hensiktsmessighetsbetraktninger bak departementets forslag om at registeret skal være identifiserbart.

Tilsynet er av den oppfatning at både helsemyndighetene og forskningsmiljøet mangler kunnskap om hva pseudonymisering av helseregistrene faktisk medfører av kostnader og begrensninger for forskningen. Det er i høringsnotatet fra departementet et ensidig fokus på hvilke negative konsekvenser pseudonymisering kan få, uten at disse er skikkelig utredet eller dokumentert.

Datatilsynet savner også at departementet foretar en prinsipiell vurdering av å gi de samtykkekompetente en adgang til å samtykke til behandlingen. Datatilsynet vil i den sammenheng fremheve at all erfaring tilsier at det generelt er svært stor vilje blant pasienter til å delta i forskning og kvalitetssikring når det gjelder sykdommer og lidelser som man selv er rammet av. Tilsynet savner også at departementet belyser alternative måter å gi pasientene kontroll over egne opplysninger på, herunder reservasjonsmulighet.

Datatilsynet har i sin høringsuttalelse bemerket at departementet ikke synes å ville akseptere hva personvern innebærer. Departementet virker ensidig opptatt av informasjonssikkerhet, og overser personvernets mest grunnleggende prinsipp – nemlig selvbestemmelsesretten.

10.2.7 *Personvernetrusler innen helseforskning – fire konkrete eksempler*

Alvorlige funn hos Kreftregisteret

I et møte mellom Kreftregisteret og Datatilsynet høsten 2008 fremkom det at Kreftregisteret selv

tvilte på om praksisen med å registrere opplysninger om friske kvinner som har deltatt i mamмоgrafiprogrammet var lovlig.

Datatilsynet vurderte saken, og fant at Kreftregisteret siden 2002 har behandlet opplysninger om ca 600 000 kvinner, uten å hente inn samtykke fra kvinnene i tråd med kreftregisterforskriftens krav. I mars 2009 fattet Datatilsynet vedtak om at Kreftregisteret enten måtte hente inn samtykke fra kvinnene, eller slette opplysningene om dem. Kreftregisteret klaget på vedtaket, som ble oversendt Personvernemnda. Nemnda fastholdt tilsynets vedtak, men forlenget fristen til å oppfylle pålegget.

I oktober 2009 gjennomførte Datatilsynet en stedlig kontroll hos Kreftregisteret. I den foreløpige rapporten konkluderes det med at Kreftregisteret også mangler rettslig grunnlag i form av samtykke fra de registrerte i undersøkelsesprogrammet vedrørende livmorhalskreft. Tilsynet har varslet et vedtak om at også opplysninger i dette registeret må slettes, med mindre det hentes inn samtykke. Dette gjelder opplysninger om ca 1,6 millioner kvinner.

Kontrollen avdekket også at Kreftregisteret ikke sletter opplysninger, slik de plikter i henhold til kreftregisterforskriften, men oppbevarer sikkerhetskopier på ubestemt tid. Endelig ble det avdekket at det ikke var etablert tilfredsstillende informasjonssikkerhet, slik at det er fare for omfattende utilsiktede utleveringer av direkte identifiserbare helseopplysninger. Det er heller ikke etablert rutiner for å avdekke om slike utleveringer finner sted.

Tvillingundersøkelsen

Datatilsynet ga avslag på søknad om konsesjon i forbindelse med Folkehelseinstituttets (FHIs) forskningsprosjekt *Tvillingundersøkelsen*. *Følger av personlighetsforstyrrelser: En populasjonsbasert studie av unge voksne*. Prosjektet var godkjent av Regional etisk komité (REK).

Etter tilsynets oppfatning ville forskningsprosjektet innebære en sammenstilling av et stort omfang av data, hvor store deler var av sensitiv karakter. Sammenstillingen vil si mye om hver enkelt registrert.

Tidligere konsesjon ble gitt under forutsetning at det ble innhentet samtykke fra de registrerte. Datatilsynet påpekte da at kobling med andre registre krever egen konsesjon. Samtykkeerklæringene i den opprinnelige konsesjonen omfattet ikke den omsøkte koblingen. Etter Datatilsynets vurdering forutsetter derfor behandlin-

gen at det blir innhentet nye samtykkeerklæringer fra de registrerte. Det at FHI skal orientere deltakerne gjennom sin informasjonsstrategi for Tvillingundersøkelsen, kan ikke avhjelpe personvertrusselen som utvidelsen av prosjektet utgjør for de registrerte.

Datatilsynet vurderte heller ikke at utvalget var så stort at det vil være uforholdsmessig vanskelig å be om nytt samtykke. Det forhold at frafallet kan bli høyere, kunne etter tilsynets oppfatning ikke tillegges avgjørende vekt, vurdert opp mot personvertrusselen som undersøkelsen utgjør. Datatilsynet la stor vekt på prinsippet om at den enkelte har råderett over opplysninger om seg selv og at de kan ta aktiv stilling til eventuell deltakelse i forskningsprosjektet.

Personvernemnda kom til samme resultat som Datatilsynet, og opprettholdt tilsynets vedtak. Prosjektet får ikke konsesjon uten at deltakerne samtykker til de nye undersøkelsene.

Systematiske brudd på regelverket i CoCa-banken

Datatilsynet mottok i februar 2009 en søknad om konsesjon til forskningsprosjektet Colon Cancer bank (CoCa-banken). Det fremgår av søknadspapirene at materialet allerede har vært brukt i lang tid uten godkjennelser, og at det søkes om å oppbevare datamaterialet på ubestemt tid til forskning.

Ved bruk av helseopplysninger og biologisk materiale har det frem til 1. juli 2009 vært påkrevd med konsesjon fra Datatilsynet (en forhåndsgodkjenning av prosjektet), dispensasjon fra taushetsplikt fra Helsedirektoratet (med mindre det foreligger et gyldig samtykke fra pasienten), en tilråding av prosjektet fra regional etisk komité (REK), samt melding om etablering av forskningsbiobank til Helsedirektoratet. Samtlige av disse punktene mangler i prosjektet CoCa-banken, med unntak av en periode på 1980-tallet hvor det forelå nødvendige tillatelser.

Det biologiske materialet består primært av svulstprøver fra tarmkreftpasienter, i tillegg til vevsprøver, blodprøver, serum og DNA. I tillegg inneholder CoCa-banken journaldata, opplysninger fra Kreftregisteret og Dødsårsaksregisteret, spørreskjema, samt analyser av det biologiske materialet. Materialet har i perioden 1982-2008 blitt brukt av minst 12 doktorgradsstipendiater, og er i bruk i minst 7 pågående doktorgradsprosjekter.

Datatilsynet nektet konsesjon, og kom med svært tydelig kritikk til driften av forskningsprosjektet. Ved avgjørelsen ble det lagt vekt på at det

ble behandlet helseopplysninger uten behandlingsgrunnlag og nødvendig konsesjon i et lenger tidsrom, at forskergruppen vanskelig kan sies å være i god tro med hensyn til krav oppstilt i helseregisterloven, manglende rutiner for innhenting og registrering av helseopplysninger i forskningsbiobank, samt mangelfull oppfølging i forhold til samtlige offentlige instanser.

Avslaget ble påklaget til Personvernemnda, som var enig i Datatilsynets vurdering.

Personvernemnda skrev i sitt vedtak:

«Systematisk neglisjering av gjeldende regelverk vil skade tilliten til forskningen på sikt. En tildeling av konsesjon i etterhånd i et tilfelle som dette, ville skapt en uheldig presedens; en presedens som ville undergrave befolkningens tillit til forskning og bidra til å svekke personvernreglenes stilling.»

Da konsesjonssøknaden var avslått etter behandling både i Datatilsynet og Personvernemnda, varslet Datatilsynet om vedtak om sletting av personopplysninger med tilknytning til forskningsbiobanken.

Mot slutten av meldingsåret klagde forskeren på Datatilsynets varslede vedtak om sletting. Regional etisk komité (REK) sendte et støtteskriv til personvernemnda, der komiteen tok til orde for å bevare det ulovlig innsamlede forskningsmaterialet. Saken er ved utgangen av 2009 ikke ferdigbehandlet i Personvernemnda.

Pasientjournaler på avveie – brukt til forskning på NTNU

I forbindelse med at NTNU søkte Helsedirektoratet om dispensasjon fra taushetsplikten til bruk av pasientjournaler i forbindelse med forskning, fremkom det at opplysningene allerede var innhentet og brukt i ulike sammenhenger over flere år. Direktoratet oversendte saken til Datatilsynet våren 2009, til orientering og mulig oppfølging.

Datatilsynet gjennomførte en stedlig kontroll ved NTNU i september 2009. Tilsynet mener å ha avdekket at pasientjournaler fra ca 20 fastlegekontorer, med opplysninger fra mer enn 110 000 pasienter, i sin helhet er stilt til disposisjon ved forskningsmiljøet på Norsk senter for elektroniske pasientjournaler ved NTNU.

Opplysningene er der blitt behandlet i strid med helseregisterloven, herunder krav om rettslig grunnlag og konsesjon. Tilsynet har sendt NTNU et varsel om at universitetet pålegges å

bedre sitt internkontrollsystem, for å unngå at lignende tilfeller oppstår i fremtiden.

Tilsynet mener at opplysningene har tilflytt NTNU gjennom brudd på helsepersonells taushetsplikt. Journalene er utlevert fra helsepersonell, uten at det er dokumentert samtykke fra pasientene eller gitt dispensasjon fra taushetsplikten. Tilsynet har derfor også oversendt saken til Helsetilsynet for en mulig oppfølging overfor helsepersonellet.

Saken var ikke ferdigbehandlet ved utgangen av 2009.

10.2.8 Omsorgsteknologi

Datatilsynet mottar en økende mengde henvendelser vedrørende såkalt «omsorgsteknologi», og media har også i 2009 hatt fokus på dette temaet. Dette gjelder særlig innen eldreomsorgen.

Det er mange positive konsekvenser av den nye teknologien. Den kan gi økt trygghet og selvstendighet, og mulighet til å bo lenger i eget hjem. Den kan gi trygghet og mobilitet utenfor boligen, og kan forlenge muligheten for aktiv deltakelse i samfunnslivet. Kroppssensorer kan gi mulighet for hjemmebasert behandling og medisinerings eller automatisk tilkalling ved akutt hjelp. Helse-tjenesten kan gi bedre og mer målrettet omsorg til de som trenger det mest. Teknologien innebærer imidlertid en betydelig økning i registrering av personopplysninger, og den kan i praksis brukes til overvåking av enkeltpersoner.

Datatilsynet ser utfordringer i forhold til personopplysningsloven krav om at det må foreligge gyldig behandlingsgrunnlag. Hovedregelen er at behandling av personopplysninger skal baseres på samtykke. En særlig problemstilling er vurderingen av dementes samtykkekompetanse. Det må foretas en konkret vurdering i hvert enkelt tilfelle. Etter pasientrettighetsloven er det for eksempel ikke tillatt å bruke sporingsteknologi overfor personer uten samtykkekompetanse som motsetter seg dette. Dersom det ikke kan innhentes samtykke til bruk av teknologien, må det foreligge annet behandlingsgrunnlag i samsvar med kravene i personopplysningslovens §§ 8 og 9.

Datatilsynet ser at bruken av slik omsorgsteknologi bør reguleres i lov, tilsvarende måten det er løst på i Danmark. Dette er spilt inn til Helsedirektoratet, og vil også fremheves i fremtiden.

Datatilsynet deltar i en referansegruppe nedsett av Helsedirektoratet, som har til formål å utarbeide en veileder for bruk av sporingsteknologi overfor demente og andre med kognitiv svikt.

10.2.9 Informasjonsplikt ved NAVs etterkontroller

Datatilsynet har pålagt NAV å etablere rutiner for å informere den registrerte, når det hentes inn pasientjournaler i forbindelse med etterkontroll av utbetalte ytelser.

Arbeids- og velferdsdirektoratet påklaget vedtaket. Direktoratet viste til at innhenting er hjemlet i folketrygdloven, og at personopplysningsloven gjør unntak fra informasjonsplikten ved lovhjemlede behandlinger.

Tilsynet har lagt avgjørende vekt på at informasjon er en grunnleggende rettighet, og at innhenting av pasientjournaler er et inngripende tiltak. Det må derfor stilles strenge krav til den aktuelle lovhjemmelen, for at personopplysningslovens unntak kommer til anvendelse.

Tilsynet mener at folketrygdlovens hjemmel er svært vid, og derfor har begrenset informasjonsverdi. Loven angir et handlingsrom som er så stort at det ikke er mulig for enkeltpersoner å forutse hvilke handlinger som faktisk gjennomføres, det vil si hvorvidt det hentes inn pasientjournaler, når det eventuelt skjer, og fra hvem de hentes inn.

Saken ligger ved utgangen av 2009 til behandling i Personvernemnda.

10.2.10 Automatisert frikortordning

Helse- og omsorgsdepartementet sendte i 2009 ut forslag til automatisering av frikortordningen til andre høringsrunde. Departementet har tatt til følge flere av innsigelsene Datatilsynet hadde i første høringsrunde, men forslaget har fortsatt flere aspekter hvor personvernet kan komme uheldig ut. Blant annet er departementet i tvil om det skal være mulig å reservere seg mot ordningen. I forslaget fra departementet kommer det frem at en slik reservasjonsmulighet vil kunne undergrave ordningen og gjøre den mindre kostnadseffektiv. Datatilsynet mener en slik reservasjonsmulighet må være på plass i tjenesten. Tilsynet minner om at dette ikke er en ordning begrunnet i rasjonalisering, men en tjeneste ment å hjelpe borgere som selv ikke makter å holde kontroll over hva de har rett på å få tilbakebetalt via frikortordningen.

10.2.11 Utval – personar med psykisk lidning som har teke liv

Helse- og omsorgsdepartementet foreslo i 2009 å oppnemne eit utval som skal undersøkje mogleg

svikt i system og forløp, knytt til personar med kjend psykisk lidning som har teke liv dei siste fem åra. Regjeringa vil pålegge alle å forklare seg for utvalet, også helsepersonell og andre som elles er bundne av lovbestemt teieplikt.

Forslaget medfører store inngrep i rettane til dei personane som blir omfatta.

Datatilsynet saknar mellom anna at departementet problematiserer forholdet til Grunnloven si § 97, som set forbod mot å gje lover tilbakeverkande kraft. Datatilsynet viser til at det å vedta ei svekking av teieplikta, for opplysningar som alle- reie er gitt, kan vere i strid med grunnleggjande rettstryggingsgarantiar, som borgarane sine krav til likebehandling og retten til å vite korleis prosessane vert gjennomførte.

10.2.12 Tilsyn: barnevern

Datatilsynet gjennomførte i meldingsåret kontroll hos offentlige barnevernsetater. Det viste seg ved kontrollene at barn som har bodd ved barnevernsinstitusjon kan letes frem i det sentrale datasystemet ODA i lang tid etter at de er flyttet ut. I tillegg påpeker Datatilsynet at det mangler rutiner for sletting når opplysninger lagres på server og hjemmeområde, samt at de rutinene som fins for tilbakeføring av papirbaserte opplysninger ikke er kjent i etaten.

Barnehjemsbarn er en spesielt utsatt gruppe, og det er derfor svært uheldig at systemet i dag svikter når det gjelder å ivareta barnas personvern. Barne- og familiedepartementet og Bufetat opplyser i et tilsvaret at det jobbes med å bedre tilgangsstyringen i barnevernets fag- og rapporteringssystem, ODA. Etter planen skal det i løpet av første halvår 2010 komme på plass en løsning som kun gir tilgang til opplysninger om utflyttede barn i en avgrenset periode etter at de har flyttet ut.

10.3 Økonomi

10.3.1 Endring av bokføringsregelverket – manglende vurdering av personvernkonsekvenser

Datatilsynets erfaring fra tilsyn og saksbehandling tilsier at behandlingsansvarlige i stor grad argumenterer for utvidet lagring av personopplysninger under henvisning til krav i annen lovgivning. Tilsynet verken ønsker eller kan pålegge sletting i de tilfeller hvor annen særregulering krever fortsatt oppbevaring, men finner det til tider problematisk at behandlingsansvarlige henviser til eksempelvis bokføringsloven som grunnlag for at ingen personopplysninger kan slettes.

Et annet problem i denne forbindelsen er at det ofte fremstår som uklart både for behandlingsansvarlige og Datatilsynet hvilke personopplysninger som faktisk kreves lagret i medhold av regnskapslovgivningen.

I delrapport II fra Bokføringsstandardstyret angående endringer i bokføringsregelverket fremgikk det at relevante personvernproblemstillinger ville berøres i delrapport III. I denne forbindelse skulle personvernspørsmål knyttet til hvilke personopplysninger som faktisk kreves lagret behandles.

Verken begrepet personvern eller personopplysning er nevnt en eneste gang i delrapport III, som ble sendt på høring i juni 2009. Datatilsynet uttalte i sin høringsuttalelse at den manglende behandling av forslagenes personvernkonsekvenser er svært beklagelig. I den forbindelse vises det til at Datatilsynet i januar 2009 henvendte seg til Fornyings- og administrasjonsdepartementet med tanke på midler til å opprette et prosjekt for å kartlegge hvor grensen går mellom personopplysningslovens bestemmelser om sletting og bestemmelser om lagring i regnskapsloven, bokføringsloven, ligningsloven og annet tilstøtende regelverk. Dette prosjektet ble utsatt i påvente av delrapport III fra Bokføringsstandardstyret.

Etter Datatilsynets vurdering er det av stor betydning for den enkeltes personvern at grensdragningen mellom de to regelsettene gjennomgås og at det klargjøres hvilke personopplysninger som faktisk er relevante å innhente og lagre

etter regnskapsregelverket, og hvor lenge det faktisk er relevant å lagre disse opplysningene. Datatilsynet vil derfor på ny henvende seg til relevante departementer med tanke på en ny utredning hvor personvernkonsekvensene av regelverket også vurderes.

10.3.2 Overføring av saker om reservasjonsregistret til Forbrukerombudet

Den 1. juni 2009 overtok Forbrukerombudet alle saker som omhandler reservasjon mot direkte markedsføring. Målet er at overføringen skal føre til et enklere regelverk og en mer ensartet forvaltningspraksis.

Reservasjonsreglene er overført fra personopplysningslovens § 26 til den nye markedsføringsloven. Datatilsynet behandler etter dette ikke lenger saker om eksempelvis manglende vask mot reservasjonsregistret.

Ifølge Forbrukerombudet har 1,7 millioner nordmenn så langt reservert seg mot telefonsalg, men mange blir likevel oppringt av telefonselgere. I samsvar med det nye lovverket blir reservasjonsordningen bedre utviklet, blant annet ved at det blir mulig å legge inn telefonnummer i reservasjonsregisteret. Videre må de som driver med telefonsalg sjekke registeret oftere enn tidligere. Det nye regelverket åpner også for at Forbrukerombudet kan ilegge overtredelsesgebyr.

Vedlegg 2

Personvernemndas årsmelding for 2009

1 Sammendrag

Dette er Personvernemndas niende årsmelding. I løpet av året er det kommet 25 klager, hvorav 15 er ferdigbehandlet i 2009. Datatilsynets vedtak er omgjort i to av de 15 sakene (PVN-2009-5 og PVN-2009-15).

Saksmengden har vært svært mye høyere enn tidligere år. Det er aldri tidligere kommet inn så mange saker. Personvernemnda finner det vanskelig å vurdere årsaken til økningen. Det ser ut til at klagenes innhold henger sammen med hvilke sektorer Datatilsynet gjennomfører tilsyn hos.

Flere av sakene har vært komplekse og prinsipielle. Fire av de største sakene, PVN-2009-11 (Nasjonalbiblioteket), PVN-2009-14 (Altinn), PVN-2009-16 (Drosjeløyve Oslo kommune) og PVN-2009-18 (Fildeling Simonsen) har nemnda arbeidet med i flere nemndmøter, uten at nemnda er kommet frem til noe vedtak i løpet av 2009.

Personvernemnda kan bare ta stilling i konkrete saker, men ser at det på flere områder er behov for en sektorovergripende rettspolitisk debatt.

2 Innledning

Personvernemnda er opprettet med hjemmel i lov om behandling av personopplysninger (2000:31). Loven trådte i kraft 1.1.2001. Personvernemnda er et klageorgan for vedtak fattet av Datatilsynet etter personopplysningsloven, helse-registerloven (2001:24) og helseforskningsloven (2008:44).

Personvernemnda er et uavhengig forvaltningsorgan administrativt underlagt Kongen og Fornyings- og administrasjonsdepartementet (FAD).

Personvernemndas arbeid reguleres av personopplysningsloven, forskrifter til denne, samt en instruks som departementet har utarbeidet. Forvaltningsloven og offentlighetsloven kommer også til anvendelse som for forvaltningen for øvrig.

Selv om departementet 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 Medlemmer

Personvernemnda har syv medlemmer som blir oppnevnt for fire år med adgang til gjenoppnevning for ytterligere fire år. Personvernemndas leder og nestleder oppnevnes av Stortinget, mens de øvrige medlemmer oppnevnes av Kongen. Første gangs oppnevning skjedde i 2001. I desember 2008 ble det oppnevnt ny leder og nestleder, samt to nye medlemmer, som startet sin funksjonstid 1.1.2009. Leder gjennom de første åtte år, Jon Bing, gikk av ved årsskiftet. Det samme gjorde nestleder Gro Hillestad Thune, medlem Siv Bergit Pedersen og medlem Hanne I Bjurstrøm, samt deres personlige vararepresentanter.

Personvernemnda besto i 2009 av følgende personer:

Eva I E Jarbekk, leder
Arve Føyen, nestleder
Tom Bolstad
Leikny Øgrim
Jostein Halgunset
Ørnulf Rasmussen
Ann Rudinow Sætnan

I tillegg har alle medlemmene personlige vararepresentanter:

Olav Torvund (vara for leder)
Ingvild Hanssen-Bauer (vara for nestleder)
Gry Nergård
Lars Erik Fjørtoft
Svein Erik Ekeid
Michal Wiik Johansen
Gisle Hannemyr

4 Andre organisatoriske forhold

Sekretariatet til Personvernemnda består av Tonje Røste Gulliksen. Hun ble ansatt som seniorrådgiver i Fornøyingsdepartementet med tiltredelse 1. mars 2006 for å arbeide i Personvernemndas sekretariat. Sekretariatet ble fra samme dato samlokalisert med Forbrukerrådet og Forbrukerombudet i Rolf Wickstrøms vei 15 i Nydalen. Leieforholdet ble avviklet i juli 2009. Fra august 2009 har sekretæren leid kontor i Sandefjord der hun bor, men hun reiser jevnlig til Oslo i forbindelse med nemndas arbeid og møter. Dette har ikke skapt praktiske problemer for nemndas arbeid.

Personvernemnda holder sine møter i Oslo, i lokaler utenfor Datatilsynet og Regjeringskvartalet for også på denne måten å markere uavhengighet.

Personvernemnda har egen hjemmeside, www.personvernemnda.no, hvor blant annet vedtakene er publisert i sin helhet. Hjemmesiden har lenke fra Datatilsynets hjemmeside, og lenker til personvernrelatert materiale tilgjengelig på Internettet. Personvernemndas vedtak publiseres også i en egen database hos Lovdata lenket til det øvrige dokumenterte materialet. Dermed kan en bruker lett slå opp på Personvernemndas vedtak ved oppslag på paragraf i personopplysningsloven, andre lover, dommer mv. som vedtakene viser til.

5 Møter og konferanser 2009

Personvernemnda har i 2009 hatt i alt 12 møter. Møtene ble i hovedsak nyttet til å behandle klagesaker, men også administrative forhold har blitt behandlet.

I tillegg til nemndmøter har det vært forberedende møter med sekretariatet og leder.

Personvernemnda hadde to kontaktmøter med departementet i 2009.

Personvernemnda deltok på den internasjonale konferansen for datatilsynsmyndigheter i Madrid, Spania, 4. – 6. november. Leder Eva I E Jarbekk representerte nemnda.

Personvernemnda ytet økonomisk støtte til «Personvernkonferansen 2009», som ble arrangert av Avdeling for forvaltningsinformatikk, Universitetet i Oslo, 4.12.2009.

6 Klagesaksbehandling

Personvernemnda mottok i 2009 totalt 25 klagesaker. Av disse var 15 ferdigbehandlet ved utgangen av året. Oversikt over vedtakene, samt vedta-

kene i sin helhet, er publisert på Personvernemndas hjemmesider. I tillegg er vedtakene publisert i egen database hos Lovdata.

Saksmengden har økt kraftig i forhold til 2007 og 2008. Flere av sakene har vært prinsipielle. Det store antall saker i 2009 har medført merarbeid for medlemmene. Dette skyldes også at flere av sakene har hatt et ikke uvesentlig omfang med svært mange vedlegg. Dette har medført arbeid for medlemmene ut over de tilmålte fire timers forberedelse til hvert møte.

Nemnda har i løpet av 2009 funnet det nødvendig å avholde flere møter enn planlagt, for å sikre en tilfredsstillende fremdrift i forhold til saksmengden.

Personvernemnda vil særlig fremheve følgende forhold i årsmeldingen:

Det første forholdet gjelder sakene om helseforskning, PVN-2009-04, PVN-2009-05, PVN-2009-06, PVN-2009-07, PVN-2009-08 og PVN-2009-09. Nemnda finner det bekymringsverdig at det tilsynelatende er en tendens til å forsøke å unngå å måtte varsle eller informere forskningsobjekter. I sak PVN-2009-07 (Gjennombrudds-prosjekt keisersnitt) uttalte Personvernemnda at det ikke kan være slik at hovedregelen ikke skal følges når det gjelder de manges personvern, bare når det gjelder de fås personvern. Dette er et prinsipielt poeng som nemnda vil fremheve fordi det anføres stadig oftere at det er «uforholdsmessig vanskelig» å informere utvalget når det dreier seg om et større antall personer. De samtykkeskjemaene som brukes i forskning synes også å lide av vesentlige mangler. Nemnda viser særlig til sakene PVN-2009-05 (Kobling av helseregistre – levertransplantasjon) og PVN-2009-06 (Krefregisterets mammografiprogram). Videre vises det til PVN-2009-08 (CoCa-banken) hvor klager ville beholde personidentifiserbare opplysninger til 2011 til tross for at forsker manglet alle de nødvendige offentlige godkjenninger av prosjektet. Nemnda uttalte at det ligger en personverntrusel i den praksis at regelverket neglisjeres og så tror man at skaden lar seg enkelt reparere i ettertid.

Det andre forholdet gjelder det store antallet midlertidige konsesjoner som Datatilsynet gir «i påvente av lovgiver». Selv om en midlertidig konsesjon kan være velbegrunnet i det enkelte tilfellet, så er Personvernemnda noe betenkt over antall tilfeller der det brukes.

Det tredje forholdet Personvernemnda vil peke på er det generelle problemet forbundet med at det gis standardkonsesjoner i stedet for forskrift. For eksempel har kredittopplysningsbransjen fått en standardkonsesjon. Standardkonsesjoner er

ikke gjenstand for den samme demokratiske prosessen som en forskrift. Dette ble også påpekt av nemnda i forrige årsmelding og nemnda finner denne praksisen uheldig. Etter nemndas syn ville det være mer hensiktsmessig å lage en forskrift med de rettssikkerhetsgarantier det medfører.

Saker som ble behandlet i 2009 er:

PVN-2009-01 Gjenpartsbrief ved kredittvurdering

Klage på tre vedtak fra Datatilsynet vedrørende gjenpartsbrief ved kredittvurdering

Klage på vedtak fra Datatilsynet hvor Datatilsynet påla tre kredittopplysningsforetak å endre sine gjenpartsbrief slik at også «score» fremkommer av gjenparten. Klager anfører at det ikke er rettslig grunnlag for å gi pålegg om at selve kredittvurderingen skal fremgå av gjenparten. Formålet med gjenpartsplikten er oppfylt når den registrerte får informasjon om hvilke opplysninger som er utlevert til spørre eller lagt til grunn for kredittvurderingen. Datatilsynet mener at en score sier noe om en persons kredittverdighet og er følgelig å anse som en personopplysning. Personvernmemnda er enig med Datatilsynet og mener at når personopplysninger er definert som både fakta og vurderinger, blir det uriktig å skille mellom opplysningene og scoren. Personvernmemnda er derfor av den oppfatning at også scoren skal fremgå av gjenparten.

PVN-2009-02 Vekting av momenter ved kredittvurdering

Klage på Datatilsynets beslutning hvor tilsynet finner at det ikke har kompetanse til å vurdere vektningen av opplysninger som kredittopplysningsvirksomheter har lovlig adgang til å innhente i forbindelse med en kredittvurdering

Klage på Datatilsynets vedtak om at tilsynet ikke har kompetanse til å vurdere vektningen av opplysninger som kredittopplysningsvirksomheter har lovlig adgang til å innhente. Nemnda var enig med tilsynet om at den ikke har myndighet til å overprøve Lindorffs valg av metoder. Heller ikke påstandene om retting etter personopplysningsloven § 27 eller sletting etter personopplysningsloven § 28 førte frem.

PVN-2009-03 Forskningsprosjekter – helseopplysninger

Klage på Datatilsynets saksbehandling vedrørende påberopte brudd på personvernlovgivningen i forskningsprosjekter

Klage på Datatilsynets saksbehandling vedrørende påberopte brudd på personvernlovgivningen i forskningsprosjekter. Klager mente at Datatilsynet skulle ha foretatt seg mer i denne saken. Datatilsynet svarte at det har fulgt opp saken på en adekvat måte, blant annet med både brevlig og stedlig kontroll – uten at det ble funnet noen behandling som var ulovlig. Personvernmemnda var enig med tilsynet og konkluderte med at saken var tilstrekkelig opplyst og Datatilsynet hadde oppfylt sin utredningsplikt etter forvaltningsloven § 17.

PVN-2009-04 Kobling av helseregistre – St Olavs Hospital

Klage på Datatilsynets avslag på søknad om endring av konsesjon – kobling av helseregistre uten å informere pasientene

Kobling av helseregistre. Det ble søkt om konsesjon til å foreta en kobling not Dødsårsaksregisteret uten å informere utvalget. Datatilsynet ga delvis avslag på søknaden. Klager fikk konsesjon, men Datatilsynet satte som krav at utvalget ble informert om koblingen. Personvernmemnda vurderte hvorvidt informasjon til pasientene om at det skal foretas en kobling mot Dødsårsaksregisteret er «utilrådelig». Nemnda bemerket at denne saken er annerledes enn de to sakene hvor Datatilsynet brukte unntaksregelen i helseregisterloven § 25, 2. ledd nr 3. Tolkning av begrepet «utilrådelig» skal ta utgangspunkt i et faglig skjønn, men dette er ikke avgjørende selv om det er av betydning. Nemnda kom til at kravet om informasjon etter helseregisterlovens §§ 20, 23 og 24 må opprettholdes.

PVN-2009-05 Kobling av helseregistre – levertransplantasjon

Klage på Datatilsynets avslag på søknad om helseforskning – kobling av helseregistre og samtykke

Kobling av helseregistre. Klage på Datatilsynets vedtak om at konsesjon for å gjennomføre en kobling mot Kreftregisteret krever at det blir innhentet nye samtykker fra alle registrerte pasienter i Norsk levertransplantasjonsregister. Personvernmemnda vurderte samtykkeskjemaene og kom til at kobling mot Kreftregisteret kan skje uten at man innhenter nye samtykker fra pasientene. Nemnda la særlig vekt på at det fremgikk av ordlyden at registreringen var frivillig. Nemnda anbefalte dog at ordlyden ble enda tydeligere slik at det blir klart at manglende samtykke ikke har

noen betydning for plassen på ventelisten eller oppfølgingen etter en transplantasjon.

PVN-2009-06 Kreftregisterets mammografiprogram

Klage på Datatilsynets vedtak vedrørende Kreftregisterets behandling av opplysninger fra Mammografiprogrammet

Klage på Datatilsynets vedtak om at Kreftregisteret skal slette eller anonymisere opplysninger om negativt funn som er eldre enn seks måneder. Alternativt skal Kreftregisteret utarbeide en fremdriftsplan for innhenting av lovlig samtykke og samtykkene må være innhentet innen utgangen av 2009. Personvernemnda tok klagen delvis til følge. Nemnda er av den oppfatning at en konsesjon kan endres av en etterfølgende forskrift. Kreftregisterforskriften trådte i kraft i 2002. Det betyr at fristen på seks måneder begynte å løpe fra det tidspunktet, for alle innsamlede opplysninger. Kreftregisteret har ikke overholdt tidsfristen. Personvernemnda mener at tidsfristen fastsatt av Datatilsynet er for kort og kom til at samtykker må være innhentet innen utgangen av 2011.

PVN-2009-07 Gjennombruddsprosjekt keisersnitt

Klage på Datatilsynets vedtak om utvidelse og forlengelse av konsesjon til å behandle helseopplysninger i forbindelse med «Gjennombruddsprosjekt keisersnitt». Konsesjon ble gitt under forutsetning at utvalget skulle få informasjon om koblingen og adgang til å reservere seg mot deltakelse

Gjennombruddsprosjekt keisersnitt. Klage på Datatilsynets vedtak om utvidelse og forlengelse av konsesjon til å behandle helseopplysninger i forbindelse med «Gjennombruddsprosjekt keisersnitt». Konsesjon ble gitt under forutsetning at utvalget skulle få informasjon om koblingen og adgang til å reservere seg mot deltakelse. Legeforeningen påklaget vedtaket og anførte at det blir vanskelig å innhente samtykke til kobling fordi klager ikke har navn eller personnummer som i etterkant kan identifisere deltakerne. Videre anføres det at arbeidsbyrden i MFR med å tilskrive over 3000 deltakere er for stor. Personvernemnda kom til at klagen ikke kunne tas til følge. 3200 personer er ikke mange. Det er tvert imot tale om et ganske lite register i forhold til mange registre i Norge i dag. Nemnda bemerket at det kan ikke være slik at hovedregelen ikke skal følges når det gjelder de manges personvern, bare når det gjelder de fås personvern.

PVN-2009-08 CoCa-banken

Klage på Datatilsynets avslag på søknad om konsesjon til helseforskning

Klage på Datatilsynets vedtak hvor det ble gitt avslag på søknad om konsesjon angående Colon Cancer banken (CoCa-banken) til å behandle helseopplysninger. Til tross for at forsker har manglet nødvendige offentlige godkjenninger av prosjektet, ønsker klager likevel å beholde personidentifiserbare opplysninger til 2011. Nemnda kom til, som Datatilsynet, at det i denne saken ikke foreligger hjemmel for å oppbevare materialet. Uttalelse om personverntusselen som ligger i den praksis at regelverket neglisjeres og man tror at skaden lar seg reparere. Etter Personvernemndas syn ville en tildeling av konsesjon i etterhånd i et tilfelle som dette, skapt en uheldig presedens.

PVN-2009-09 Tvillingundersøkelse

Klage på Datatilsynets avslag på søknad om konsesjon til helseforskning

Klage på Datatilsynets vedtak hvor det ble gitt avslag på søknad om konsesjon til å behandle helseopplysninger i forbindelse med forskning. Konsesjonssøker ønsket å koble Tvillingregisteret med en rekke andre registre. Datatilsynet ville ikke gi konsesjon uten at samtykke fra utvalget først ble innhentet. Nemnda er enig i Datatilsynets interesseavveining, der Datatilsynet legger til grunn at samfunnets behov for behandlingen i dette tilfellet må vike for personverninteressene.

PVN-2009-10 Ila fengsel

Klage på Datatilsynets vedtak hvor Ila fengsel nektes fullt innsyn i den underliggende klage

Klage på Datatilsynets vedtak der Ila fengsel nektes fullt innsyn i den underliggende klage og det innvilges kun delvis innsyn med rettslig grunnlag i forvaltningsloven § 19, 2. ledd bokstav b. Personvernemnda vurderte det slik at samtlige temaer som den innsatte hadde reist, falt utenfor Datatilsynets kompetanse. Personvernemnda kom dermed til at den foreliggende saken var en orienteringssak, ikke en enkeltvedtakssak. Dette medførte at det ikke forelå noen enkeltvedtakssak som Ila fengsel kunne være part i. Dermed hadde Ila heller ikke krav på partsinnsyn etter forvaltningsloven.

PVN-2009-12 Politiets taushetsplikt

Klage på Datatilsynets beslutning om å avslutte sak om et eventuelt brudd på politiets taushetsplikt

Klage på Datatilsynets beslutning om å avslutte sak om et eventuelt brudd på politiets taushetsplikt. Saken gjaldt spørsmål om brudd på taushetsplikt hos politiet, og Personvernemnda var enig med Datatilsynet i at det er en sak for Spesialenheten for politisaker. Saken lå dermed utenfor Datatilsynets kompetanse. Nemnda kom til at saken var tilstrekkelig opplyst og Datatilsynet hadde oppfylt sin utredningsplikt etter forvaltningsloven § 17.

PVN-2009-13 Registrering hos folkeregisteret

Klage på Datatilsynets avgjørelse om å avslutte sak om registrering av opplysninger i folkeregisteret

Klage på Datatilsynets avvisningsvedtak. Klager mener å stå oppført med feil ektefelle i folkeregisteret. Klager påklager avvisningsvedtaket og hevder at saken ikke burde avsluttes men følges opp ytterligere i forhold til Skatt Øst, jf personopplysningsloven § 13. Personvernemnda vurderte Datatilsynets saksbehandling og kom til at saken ble tilstrekkelig opplyst før vedtak ble fattet. Datatilsynet har dermed oppfylt sin utredningsplikt etter forvaltningsloven § 17 og veiledningsplikt etter forvaltningsloven § 11.

PVN-2009-15 Skoleskyssordning

Klage på Datatilsynets vedtak om at Rogaland fylkeskommune ikke kan bruke fødselsnummer for administrering av skoleskyss

Klage på Datatilsynets vedtak om at Rogaland fylkeskommune ikke kan bruke fødselsnummer for administrering av skoleskyss. Datatilsynet viste til at bestemmelsen i personopplysningsloven § 12 er strengt utformet og sikker identifisering kan oppnås ved bruk av navn, adresse og fødselsdato i denne saken. Personvernemnda kom etter en konkret vurdering til at det var «saklig behov» for sikker identifisering og at metoden var «nødvendig» for å oppnå slik identifisering. Bru-

ken av personnummer i denne saken var derfor i samsvar med personopplysningsloven § 12.

PVN-2009-17 Klage på NAV og helsepersonell

Klage på Datatilsynets avvisningsvedtak

Klage på Datatilsynets avvisningsvedtak. Klagen gjaldt behandling hos NAV og ulike personer innen helsevesenet. Personvernemnda vurderte hvorvidt Datatilsynet hadde oppfylt sin utredningsplikt etter forvaltningsloven § 17 og veiledningsplikt i forvaltningsloven § 11. Nemnda kom til at Datatilsynet har oppfylt sin utredningsplikt og veiledningsplikt i denne saken.

PVN-2009-21 Klage på advokat

Klage på Datatilsynets avvisningsvedtak

Klage på Datatilsynets avvisningsvedtak. Klagen gjaldt forhold knyttet til klagers advokat, blant annet manglende og mangelfull bistand. Personvernemnda vurderte hvorvidt Datatilsynet hadde oppfylt sin utredningsplikt etter forvaltningsloven § 17 og veiledningsplikt i forvaltningsloven § 11. Nemnda kom til at Datatilsynet har oppfylt sin utredningsplikt og veiledningsplikt i denne saken.

7 Regnskap og budsjett for 2009

Personvernemnda hadde i 2009 en budsjett-ramme på kr 1 650 000, og fremkommer under kap 1500 Fornyings- og administrasjonsdepartementet i statsbudsjett for 2009.

Totalt forbruk: kr 1 490 714. Personvernemnda disponerte sin bevilgning til innkjøp av litteratur, tjenester, økonomisk støtte til konferanse, arrangement av internt seminar, deltakelse på seminar og den internasjonale konferansen, arbeidsgodtgjørelse og reisegodtgjørelse til nemndas medlemmer, lønn til sekretariat og leie av lokaler.

Oslo, 10. februar 2010
For Personvernemnda
Eva I E Jarbekk (leder)

Offentlige institusjoner kan bestille flere eksemplarer fra:
Departementenes servicesenter
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 20 00

Opplysninger om abonnement, løssalg og pris får man hos:
Fagbokforlaget
Postboks 6050, Postterminalen
5892 Bergen
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00
Faks: 55 38 66 01
www.fagbokforlaget.no/offpub

Publikasjonen er også tilgjengelig på www.regjeringen.no

Omslagsillustrasjon:
Departementenes servicesenter

Trykk: 07 Oslo AS 10/2010

