

# Datatilsynets årsmelding for 2010

Årsmelding R11/01

10.02.2011

Manus til stortingsmelding om Datatilsynets virksomhet, jf. personopplysningslovens § 42.

Oversendt Fornyings-, administrasjons- og kirkedepartementet  
10. februar 2011.





## INNHALDSFORTEGNELSE

<b>Innledning ved direktøren</b> .....	<b>7</b>
<b>1. Om Datatilsynet</b> .....	<b>8</b>
1.1 Datatilsynets oppgaver .....	8
1.2 Organisasjon og administrasjon.....	8
1.2.1 <i>Budsjett og rammevilkår</i> .....	8
1.2.2 <i>Organisering og personale</i> .....	9
1.3 Deltakelse i offentlige råd og utvalg .....	10
1.4 Internasjonalt samarbeid.....	11
1.5 Juridisk saksbehandling .....	13
<b>2. Kommunikasjon og dialog</b> .....	<b>19</b>
2.1 Du Bestemmer .....	19
2.2 ID-tyveritesten.....	20
2.3 Slettmeg.no .....	20
<b>3. Datatilsynets kontrollvirksomhet</b> .....	<b>22</b>
3.1 Nøkkeltall .....	22
3.2 Bransjer underlagt kontroll .....	23
3.3 Samarbeid med andre myndigheter .....	24
3.4 Bruk av formelle reaksjoner .....	24
3.5 Måloppnåelse .....	24
3.6 Generelt om funn og svakheter avdekket ved kontroll .....	25
<b>4. Tendenser og utviklingstrekk</b> .....	<b>27</b>
4.1 Personopplysninger som handelsvare .....	27
4.2 "Klebrig" offentlighet.....	28
4.3 Tap av kontroll i nettskyen? .....	30
4.4 Innebygget personvern blir viktig .....	31
4.5 Gode helseregistre – bedre helse? .....	32
<b>5. Nærmere om utvalgte felter</b> .....	<b>35</b>
5.1 Justis og utlendingsfeltet .....	35
5.1.1 <i>Norge bør si nei til Datalagringsdirektivet</i> .....	35
5.1.2 <i>Personvern i politisektoren - Politiregisterloven</i> .....	36
5.1.3 <i>Dødsstedsundersøkelser ved plutselig og uventet småbarnsdød</i> .....	37
5.1.4 <i>Personvern i fengslene – ny straffegjennomføringslov (ILA-saken)</i> .....	37

5.1.5	<i>Overvåkingsaken ved den amerikanske ambassaden</i>	37
5.1.6	<i>Samarbeid med Utlendingsforvaltningen</i>	38
5.2	Telesektoren	38
5.2.1	<i>Simonsensaken – fortsatt fildelingsjakt etter nemndas avgjørelse</i>	38
5.2.2	<i>Google Street View</i>	39
5.2.3	<i>Tilsyn – Politiets innhenting av opplysninger fra teleselskapene</i>	40
5.2.4	<i>Tilsyn – Nummeropplysningsvirksomheter</i>	40
5.3	Sosiale nettsamfunn	41
5.3.1	<i>Prosjekt om sosiale nettsamfunn</i>	41
5.3.2	<i>Tilsyn – sosiale nettsamfunn</i>	42
5.3.3	<i>Klage på Facebook og Zinga fra Forbrukerrådet</i>	42
5.4	Skole, barn og unge	43
5.4.1	<i>Tilsyn – opptakssystemet for videregående opplæring (VIGO)</i>	43
5.4.2	<i>Tilsyn – elektroniske klassestyringsprogrammer</i>	44
5.4.3	<i>Tilsyn – institusjoner som hjelper barn og ungdom</i>	44
5.4.4	<i>Personvernskolen i regi av Universitetet i Oslo</i>	45
5.5	Arbeidsliv	45
5.5.1	<i>Innsyn i e-post</i>	46
5.5.2	<i>Tilsyn - innsyn i e-post</i>	46
5.5.3	<i>Tilsyn – Adgangskontrollsystem</i>	47
5.5.4	<i>Tilsyn – GPS-sporing</i>	47
5.5.5	<i>ID-kort i byggebransjen</i>	48
5.5.6	<i>Telefonopptak i finanssektoren</i>	48
5.5.7	<i>Tilsyn – kameraovervåking i arbeidslivet</i>	49
5.5.8	<i>Overføring av personlister til USA for terrorscreening</i>	49
5.6	Idrett	50
5.6.1	<i>Tilsyn – antidopingkontroller på treningssentre</i>	50
5.7	Kameraovervåking	50
5.7.1	<i>Tilsyn – kjøpesentre</i>	51
5.7.2	<i>Tilsyn – bruk av kameraovervåking ved parkeringskontroll</i>	51
5.7.3	<i>Tilsyn – Akershus universitetssykehus</i>	52
5.8	Samferdsel	52
5.8.1	<i>Bransjenorm for betalingssystemer i kollektivtransporten</i>	53

5.8.2	<i>Samarbeid med Statens vegvesen</i> .....	53
5.8.3	<i>ITS-direktivet</i> .....	54
5.8.4	<i>eCall</i> .....	54
5.9	<i>Velferd, forskning og helse</i> .....	55
5.9.1	<i>Tilsyn – Folkehelseinstituttet</i> .....	55
5.9.2	<i>Tilsyn – Kreftregisteret</i> .....	56
5.9.3	<i>Tilsyn – Norsk pasientskadeerstatning</i> .....	57
5.9.4	<i>Tilsyn - helseregistre</i> .....	57
5.9.5	<i>Tilsyn – NTNU</i> .....	58
5.9.6	<i>Avslag på søknad om konsesjon for forskningsprosjekt i regi av NOVA</i> .....	58
5.9.7	<i>Høring – tilgang på tvers</i> .....	59
5.9.8	<i>Høring – strategi for Norsk Helsenett</i> .....	60
5.9.9	<i>Høring – Drap i Norge</i> .....	60
5.9.10	<i>NAV</i> .....	60
5.9.11	<i>Velferdsteknologi</i> .....	61
5.10	<i>Finans og forsikring</i> .....	62
5.10.1	<i>Kredittopplysningsvirksomheten</i> .....	62
5.10.2	<i>Tilsyn – BBS og eFaktura</i> .....	63
5.10.3	<i>Tilsyn – utlevering av personopplysninger til land utenfor EØS-sonen</i> .....	63
5.11	<i>Personvern i Kommunesektoren</i> .....	64
5.11.1	<i>Tilsyn med kommuner</i> .....	64
5.11.2	<i>Dagsseminarer og oppdatert veileder</i> .....	64
5.11.3	<i>Kartlegging av status for arbeid med personvern</i> .....	65
5.12	<i>Personvernombud</i> .....	65



## INNLEDNING VED DIREKTØREN

Med dette legger Datatilsynet fram årsmeldingen for 2010. Å trekke fram hva som har vært viktigst i et begivenhetsrikt år er ingen enkel oppgave, særlig ikke når jeg har sittet i direktørskolen under halve året. Men vi har forsøkt å gi en oversikt over hvordan vi jobber, hva vi har gjort og pekt på noen hovedtrender fra året, og for årene som kommer.

Den teknologiske utviklingen går i rasende fart, og utfordrer personvernet på mange områder. Folk deler villig personlige opplysninger på Facebook og andre sosiale nettsamfunn, og smarttelefoner og nye håndholdte lesebrett har tatt landet med storm. Såkalte ”apper” har blitt en milliardindustri. Datatilsynet har satt sosiale nettsamfunn, lokaliseringstjenester, apper og Internett på den interne dagsorden som et viktig område, og har hatt økt fokus på dette sammenlignet med tidligere år.

Helse og personvern er et viktig felt. Pasienten må være sikker på at helsepersonell får tilgang til viktige opplysninger i en behandlingssituasjon. Samtidig må pasienten være sikker på at opplysninger hun gir til for eksempel legen sin forblir konfidensiell og ikke kommer på avveie. Datatilsynet har støttet økt bruk av IKT og personvern fremmende teknologi i helsesektoren. Samtidig har vi sett at for eksempel tilgangsstyringen til pasientjournaler er for dårlig. Det har vært viktig å påpeke feil og mangler, samtidig som Datatilsynet har uttrykt et ønske om samarbeid og samhandling for i fellesskap å etablere løsninger som fremmer både kvalitet i behandlingen og et godt personvern i helsesektoren.

I en verden der nesten alt dreier seg om teknologi må vi også bruke teknologien til å skape et bedre personvern. Datatilsynet har tatt en beslutning om at personvern fremmende teknologi vil være et satsingsfelt i årene som kommer. Ved å bygge inn godt personvern i den teknologiske løsning allerede fra starten får vi en vinn vinn situasjon; god funksjonalitet og godt personvern.

I 2010 har vi lagt grunnlaget for en endringsprosess internt i Datatilsynet. Vi lanserte en helt ny virksomhetsplan bygd på klare prioriteringer, mål og konkrete tiltak. Vi vil ha en mer strategisk tilnærming til personvernutfordringene, samtidig som vi vil knytte personvernet nærmere folks hverdag. Personvern i arbeidslivet er derfor en av de høyest prioriterte områdene. Vi ser stadig mer registrering og overvåkning i arbeidslivet, og opplysninger innsamlet for et formål brukes til et annet. I tillegg vil vi ha særlig fokus på helse, justis og politi, IKT og sosiale nettsamfunn, samferdsel og økonomi og finans.

Tilstanden for personvernet i Norge bestemmes i stor grad av det som skjer internasjonalt. Datatilsynet har deltatt på en rekke internasjonale møter og konferanser blant annet i regi av EU og OECD. Internasjonalt arbeid er viktig for Datatilsynet og vi er avhengig av å finne samarbeidspartnere for å få gjennomslag for personvernet. Blant annet gjennom tjenesten slettmeg.no har Datatilsynet bygd opp et godt kontaktnett i internasjonale selskaper som vil få stor betydning framover.

Bjørn Erik Thon  
Direktør

## **1. OM DATATILSYNET**

Datatilsynet har til oppgave å bidra til å beskytte den enkelte mot at personverninteressene krenkes gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvern hensyn, slik som behovet for vern av personlig integritet og privatlivets fred. Datatilsynets virksomhet er i første rekke 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-, administrasjons- og kirke departementet. 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.

### **1.1 DATATILSYNETS OPPGAVER**

Datatilsynet skal identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses. 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. Deltakelse i råd og utvalg er derfor en viktig del av Datatilsynets arbeid. Også som høringsinstans i saker som kan ha en personvernmessig konsekvens forsøker Datatilsynet å påvirke 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.

Datatilsynet har 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 meroffentlighet.

### **1.2 ORGANISASJON OG ADMINISTRASJON**

#### **1.2.1 Budsjett og rammevilkår**

Datatilsynets budsjett var i meldingsåret på 31 millioner kroner. I tillegg fikk Datatilsynet 4 millioner kroner til videreføring av prosjekter oppstartet i 2009 på personvernområdet.



Prosjektene retter seg mot internkontroll og informasjonssikkerhet i norske virksomheter (herunder personvernombudsordningen) og etablering av en veiledningstjeneste for publikum som opplever å få sitt personvern krenket på Internett (slettmeg.no).

Omlag 75 prosent av det ordinære budsjettet dekket lønnskostnader. Seks medarbeidere var ute i permisjon hele eller deler av 2010, hvorav fem i svangerskapspermisjon. Vikarer og ekstrahjelp ble tilsatt som erstatning for disse. Fem 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 engasjement.

### 1.2.2 Organisering og personale

Den 8.april 2010 fratradte Georg Apenes som direktør i Datatilsynet for aldersgrensen på 70 år. Bjørn Erik Thon tiltrådte som ny direktør 2.8.2010.

Datatilsynet har i meldingsåret bestått av til sammen 37 årsverk. De ansatte er delt på fire ulike avdelinger. Avdelingslederne rapporterer til direktøren. Tabellen viser antall ansatte i hver avdeling i Datatilsynet pr. 31.12.2010.

Stillinger fordelt på avdeling i Datatilsynet			
Avdeling	Totalt	Kvinner	Menn
Ledere	5	1	4
Informasjonsavdelingen	3	3	0
Tilsyns- og sikkerhetsavdelingen	8	2	6
Juridisk avdeling	15	9	6
Administrasjonsavdelingen	6	6	0
<b>Totalt</b>	<b>37</b>	<b>21</b>	<b>16</b>

Det har i meldingsåret dessuten vært tilsatt to menn i prosjektet slettmeg.no, og én mann i prosjektet internkontroll og informasjonssikkerhet.

Med hensyn til rekruttering har Datatilsynet som målsetting å stimulere til et kulturelt og kompetansemessig mangfold i staben. Det tilrettelegges videre for en personalpolitikk som skal virke motiverende og som skal hindre utstøting av eldre personer og personer med nedsatt funksjonsevne. Som arbeidsgiver søker tilsynet å hindre diskriminering på grunn av kjønn, etnisitet og nedsatt funksjonsevne.

### Kjønnsfordeling

Datatilsynet har som målsetting å arbeide aktivt for å fremme likestilling mellom kjønnene, med særlig sikte å gi kvinner og menn like arbeidsforhold og like muligheter til karriereutvikling og faglig utvikling. Datatilsynet tilstreber at menn og kvinner skal gis like rettigheter. I 2010 var

det tilsatt 16 menn og 21 kvinner i Datatilsynet. Gjennomsnittsalderen for menn er 40,8 år og for kvinner 39,9 år. Gjennomsnittsalder totalt er 40,3 år.

### **Bruk av overtid**

Datatilsynet har ikke utstrakt bruk av overtid. Overtid benyttes for å ta ”topper” og ved spesielle behov for å få konkrete arbeidsoppdrag fullført i tide.

### **Velferdspermisjoner/omsorgspermisjoner og sykefravær**

Datatilsynet har generelt et lavt sykefravær. Fravær knyttes i stor grad til barns sykdom og svangerskapsrelatert sykdom. Velferdspermisjoner gis i henhold til retningslinjer i Statens personalhåndbok og til interne retningslinjer for ønsket praksis.

### **Kompetansehevende tiltak**

Det foreligger per i dag ingen statistikk for bruk av tid og ressurser til kompetansehevende tiltak. Det settes imidlertid av en ”pott” til kurs/kompetansehevende tiltak per ansatt i budsjettet. Datatilsynet har gitt permisjon til medarbeidere som ønsker å ta tilleggsutdanning der det har vært definert som relevante kompetanse for etaten. Avdelingsleder har ansvar for at medarbeidere gis faglig utvikling og alle søknader om kompetansehevende tiltak behandles individuelt.

## **1.3 DELTAKELSE I OFFENTLIGE RÅD OG UTVALG**

I meldingsåret har Datatilsynet deltatt i følgende råd og utvalg:

### **E-valg – referansegruppe**

Datatilsynet har i flere år deltatt i en departemental referansegruppe for å gi innspill til en løsning for elektronisk stemmegivning hjemmefra. Det vil snarlig komme regler om dette på høring.

### **Evalueringsutvalg av INFOFLYT-systemet**

Datatilsynet har vært med i et utvalg som skal se nærmere på INFOFLYT-systemet. Systemet ble etablert i 2005 av Justisdepartementet for utveksling av informasjon mellom kriminalomsorgen og politiet.

Sivilombudsmannen har flere ganger stilt kritiske spørsmål ved sider av dette systemet. Justisdepartementet besluttet derfor å nedsette et utvalg som skal gjennomgå systemet. Utvalget skal i første omgang kartlegge og vurdere hvordan kriminalomsorgens utveksling av informasjon med politiet fungerer i dag. Dette gjelder behandlingen av personopplysninger og bruken av slike opplysninger i saksbehandlingen – både i forvaltnings- og domstolsbehandlingen.

Utvalget skal foreslå hvordan dette kan reguleres i fremtiden, og om det er behov for endringer i tilgrensende regelverk. Arbeidet har i 2010 i all hovedsak bestått i å innhente fakta fra kriminalomsorgen og politiet sentralt, og fra kriminalomsorgens ytre etat i form av besøk på forskjellige institusjoner og etater. Utvalget skal avlevere sin rapport i løpet av våren 2011.

### **Koordineringsutvalget for informasjonssikkerhet - KIS**

Utvalget består av representanter fra syv departementer, Statsministerens kontor og ni direktorater. Opprettelsen av utvalget er et ledd i gjennomføringen av en nasjonal strategi for informasjonssikkerhet. Datatilsynet deltar med én representant. Det arrangeres fire til seks møter per år.

### **Samarbeidstrådet for helsesektoren**

Datatilsynet deltar som observatør. Rådet er opprettet av Helsedirektoratet med sikte på å koordinere arbeid med informasjonsteknologi i helsesektoren. Datatilsynet deltar med én representant. Det avholdes fire møter i året.

### **Styringsgruppe for bransjenorm innen helse**

Bransjenorm om informasjonssikkerhet for helsesektoren ble lansert i september 2006. Arbeidet består i å få en hensiktsmessig spredning og implementering av normen i sektoren. Dette skaper store utfordringer gitt sammensetningen av små, mellomstore og store aktører. Datatilsynet deltar som observatør i styringsgruppen. Det arrangeres tre møter per år.

### **Samarbeidsgruppe id-tyveri**

Datatilsynet har valgt å gå aktivt inn i et prosjekt som arbeider for å forebygge identitetstyveri. Tilsynet utredet på eget initiativ problemstillingen i 2008/2009 og konkluderte med at det er behov for en rekke forebyggende tiltak. Datatilsynet har sett prosjektet som en viktig kanal for å få gjennomført en del av disse tiltakene. Datatilsynet deltar med én fast representant, men avser i perioder ytterligere ressurser.

### **Europakommisjonens ”E-call-initiativ”**

EU-kommisjonen arbeider med innføring av system for automatisk anrop fra biler som har vært utsatt for ulykker, til relevant alarmsentral. Datatilsynet deltar i eCall-arbeidet som observatør i den nasjonale styringsgruppen. Deltakelsen gir Datatilsynet mulighet for å medvirke til at systemet blir tilrettelagt på en måte som i størst mulig grad ivaretar personvern hensyn. Arbeidet med e-call står nærmere beskrevet under punkt 5.8.4

### **Arbeidsgruppe – helautomatiske bomstasjoner**

Etter kontroller Datatilsynet gjennomførte mot utvalgte bomstasjonsselskaper inviterte Samferdselsdepartementet til deltakelse i en arbeidsgruppe som skal se på personvern i forbindelse med overgangen til helautomatiske bomstasjoner. Med i arbeidet er også Statens Vegvesen, som er en sentral instans for utbygging av bomstasjoner og den tekniske løsningen. Dette arbeidet står nærmere beskrevet under punkt 5.8.2

## **1.4 INTERNASJONALT SAMARBEID**

I meldingsåret har tilsynet vært særlig aktive i Artikkel 29-gruppen med undergrupper, i Berlin-gruppen og i OECD-arbeidet. I tillegg deltar tilsynet i Working Party on Police and Justice, Joint Supervisory Authority og i nordisk samarbeid.

**Artikkel 29-gruppen** er EUs viktigste personvernfora. Det er nedfelt i EØS- avtalen at Datatilsynet kun har observatørstatus i denne gruppen. Dette er beklagelig, og Datatilsynet vil

igangsette et arbeid for å se om tilsynet kan få status som fullt medlem. Uansett er Artikkel 29- gruppen et viktig forum for å bygge nettverk, holde seg oppdatert om viktige prosesser på EU-området og bidra med innspill til de ulike uttalelsene gruppen kommer med.

**Working Party on Police and Justice (WPPJ).** Det har i meldingsåret vært diskutert om dette er et forum som skal bestå etter at Lisboa-traktaten er vedtatt. Det vil si at personvernspørsmål for politi og justis ikke lenger skal være adskilt fra det arbeidet som tradisjonelt hører inn under Artikkel 29-gruppen.

Datatilsynet er også medlem i **Technology Subgroup**, som er har som oppgave å utrede og gå innspill til artikkel 29-gruppen. I meldingsåret har det vært en prioritert oppgave å bidra med konkrete innspill til hvordan nytt teknologisk utstyr som lesebrett og smarttelefoner innhenter og bruker personopplysninger. Etter tilsynets vurdering har dette vært nyttige innspill.

**Berlin-gruppen** er et globalt nettverk med teknologifokus. Her diskuteres tema som geolokalisering, Google Street View og intelligente trafikksystemer. Det legges stor vekt på informasjonsdeling og diskusjon om den teknologiske utvikling. Tilsynet holdt i meldingsåret et innlegg om slettmeg.no som fikk svært positiv respons. Også ID-tyveri-selvtesten ble presentert for Berlin-gruppen. Dette viser at Datatilsynet, ved å legge fram gode eksempler på enkeltsaker og prosjekter, kan ha innflytelse og ikke minst eksportere vårt arbeid til andre land.

**Joint Supervisory Authority (JSA)** er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). SIS inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengen-området eller er straffedømt i et av medlemslandene. Norge er et av landene som skal inspiseres av JSA i 2011. JSA diskuterer også SIS II, som skal ta erstatte dagens informasjonsutvekslingssystem. Datatilsynet er Norges representant i prosjektets referansegruppe som skal klargjøre for implementering av SIS II i Norge. En representant fra Datatilsynet var med i et inspeksjonsteam i regi av JSA i 2010.

Årlig arrangeres det dessuten **møter på saksbehandlernivå** både mellom de nordiske landene og på internasjonalt nivå. Datatilsynet har vært representert i begge fora for å få innspill om hva andre lands myndigheter er opptatt av, samt erfaringsutveksling. Møtene er også gode arenaer for å utvikle kontaktnett.

Datatilsynet deltok dessuten på den årlige **personvernkonferansen** og **OECD-møtet**. I førstnevnte satt tilsynets direktør i et panel om sosiale medier som blant annet diskuterte hvorvidt folk har god nok kunnskap om det som skjer i de ulike sosiale mediene og om Facebook og andre er seg sitt ansvar bevisst.

Det er særlig interessant å trekke frem noen gjennomgående observasjoner fra de internasjonale møtene. Her vil tilsynet særlig trekke fram:

- Det er billigere å lagre enn å slette. Dette fører til at enorme datamengder samles opp.
- Lagring skjer i nettskyen, og vi vet ofte ikke hvor dataene våre faktisk er.

- Det samles inn store mengder informasjon blant annet gjennom private Wifi-anlegg som brukes i lokaliseringstjenester, ofte uten borgernes kjennskap.
- Retten til å bli glemt blir borte, og vi risikerer at det for all tid vil finnes spor av alt vi har gjort i løpet av våre liv.

## **1.5 JURIDISK SAKSBEHANDLING**

Det har i meldingsåret vært registrert inn omlag 1 600 nye saker til behandling som forvaltningssaker. De fleste sakene er fra private aktører som har spørsmål om personopplysningsloven er fulgt, eller som har konkrete påstander om at loven ikke er fulgt. Av det som går igjen er spørsmål omkring kameraovervåkning av privat grunn og i tilknytning til arbeidsplasser, kredittvurderinger, samt bruk av fullt fødselsnummer i forskjellige sammenhenger. En ny trend er stadig flere spørsmål rundt arbeidsgiveres elektroniske ID-løsninger.

### **Konsesjoner**

Datatilsynet behandler fortløpende innkomne søknader om konsesjoner. Det totale antallet søknader som kom inn i 2010 var 357, hvorav 251 var nye bankkonsesjoner. Dette er noe færre enn tidligere år da søknad om helseforskning nå skal til de regionale etiske komiteene.

Det er i 2010 utarbeidet en ny bankkonsesjon i samarbeid med Finansnæringens hovedorganisasjon. Det har vært en del kommunikasjon med bransjen i etterkant av utsendelsen for å klargjøre innholdet og de krav konsesjonen stiller.

### **Meldinger**

I meldingsåret kom det inn 3 693 nye meldinger om behandling av personopplysninger mot 3 778 i 2009. Totalt var det 10 055 meldinger i meldingsdatabasen ved årsskiftet mot 9 292 året før. Det ble i meldingsåret slettet 2 930 meldinger fra databasen som hadde utløpt på dato i forhold til treårsregelen, mot 3 126 året før.

Tilsynet antar at en del av meldingene som er slettet fra meldingsbasen burde vært fornyet av den behandlingsansvarlige. Datatilsynet erfarer at manglede melding til tilsynet er en vanlig feil hos mange behandlingsansvarlige.

En utfordring ved dagens meldingssystem er å håndtere saker som dreier seg om virksomheter som i spesielle tilfeller har behov for å behandle personopplysninger i et begrenset tidsrom. Et typisk eksempel er arbeidsgivers innsyn i ansattes e-post ved begrunnet mistanke om at bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet. Et relevant spørsmål er hvorvidt slike saker skal falle inn under den alminnelige meldingsplikten slik de gjør i dag. Slike saker må tidvis unntas fra offentlig innsyn for en tidsbegrenset periode, og dette gjør det utfordrende å behandle denne typen saker i et offentlig meldingssystem.

## Høringer

Datatilsynet mottok i meldingsåret 123 offentlige høringssaker, og avgav uttalelse i litt over halvparten av disse. Oppsummert har mange av høringene vært knyttet til justisfeltet og helsefeltet.

## Klagesaker til Personvernemnda

I meldingsåret oversendte Datatilsynet 13 saker til Personvernemnda for videre klagebehandling. Dette er færre enn i 2009, et år hvor antallet oversendelser var over gjennomsnittet. Personvernemnda avgjorde 14 saker i 2010, noen av dem oversendt i 2009. Av de sakene som ble behandlet ble én sendt tilbake til Datatilsynet for ytterligere undersøkelser, mens fire av klagen ble tatt til følge. I to av sakene ble klagen delvis tatt til følge. I de øvrige sakene ble tilsynets vedtak stående.

Listen viser saker som er oversendt til Personvernemnda og resultat av behandlingen i nemnda i 2010. (blanke felt viser at saken ikke er ferdig behandlet)

Tittel	Sendt PVN Brevdato	Vedtak i PVN	Vedtak
Klage på Datatilsynets avvisningsvedtak vedrørende kredittvurdering i journalistisk virksomhet	14.01.2010	23.06.2010	Klagen tas ikke til følge
Klage på Datatilsynets vedtak om vurdering av krav til behandlingsgrunnlag ved screening	02.03.2010		
Klage på Datatilsynets vedtak om å avslutte sak om feilaktige opplysninger i en kommunes register.	26.03.2010	09.11.2010	Klagen tas til følge
Klage på Datatilsynets vedtak om at det forelå saklig behov for kredittvurdering.	25.03.2010	09.11.2010	Klagen tas ikke til følge
Klage på Datatilsynets vedtak om å avslutte sak som gjelder kredittvurdering ved opprettelse av ny inkassosak	26.03.2010	09.11.2010	Klagen tas ikke til følge
Anmodning om endring av konsesjonsvilkår for behandling av personopplysninger hos tilbydere av forsikringstjenester	29.03.2010		
Klage på Datatilsynet vedtak om pålegg etter kontroll hos E18 Vestfold AS – Elektronisk billettering	19.04.2010		
Klage på Datatilsynets vedtak om pålegg etter kontroll hos Fjellinjen – Elektronisk billettering	19.04.2010		
Klage på delvis avslag på søknad om konsesjon til å behandle personopplysninger ifm forskning – Nordisk omfangsundersøkelse – Ung i Norden 2009	04.05.2010		
Klage på vedtak etter kontroll – Behandling av personopplysninger ifm gjennomføring av automatisk trafikkontroll	27.05.2010		

Klage på vedtak om sletting av personopplysninger på Internett	28.07.2010		
Klage på vedtak etter kontroll hos Ruter AS	16.09.2010		
Klage på vedtak etter kontroll hos Kolumbus Rogaland Kollektivtrafikk	16.09.2010		
Klage på vedtak om tidsbegrenset konsesjon til å behandle personopplysninger – innsamling av nettdokumenter fra internett – Paradigma-prosjektet	08.07.2009	02.02.2010	Klagen tas delvis til følge
Klage på vedtak om at Altinn sentralforvaltning må avslutte logging av fødselsnummer og tilhørende IP-adresse	17.08.2009	02.02.2010	Klagen tas til følge
Klage på vedtak om opphør av innhenting av vandelsopplysninger ved tildeling av drosjeløyve samt pålegg om sletting av allerede innhentede personopplysninger	31.08.2009	01.03.2010	Klagen tas delvis til følge
Klage på avslag på søknad om forlengelse av tidsbegrenset konsesjon til å behandle personopplysninger – Anti-piratarbeid	04.09.2009	05.11.2010	Klagen tas til følge
Klage på pålegg om sletting av betalingsanmerkninger	16.09.2009	13.01.2010	Klagen tas til følge
Klage på avslag på søknad om konsesjon til å behandle personopplysninger	24.09.2009	28.07.2010	Klagen returneres Datatilsynet for videre behandling
Klage på Datatilsynets vedtak om plikt til å gi informasjon etter pol § 20 første ledd	12.11.2009	23.03.2010	Klagen tas ikke til følge
Klage på Datatilsynets vedtak om å avslutte sak	27.11.2009	24.03.2010	Klagen tas ikke til følge
Klag på Datatilsynets vedtak om sletting av opplysninger – Coca Bank	09.12.2009	26.05.2010	Klagen tas ikke til følge
Klage på vedtak om utlevering av opplysninger om klager til Datatilsynet	09.12.2009	23.06.2010	Klagen tas ikke til følge

Flere av sakene som ble påklaget var kompliserte og inneholdt vurderinger av motstridende hensyn. Datatilsynet mener det er akseptabelt at saker blir omgjort av Personvernemnda, da de kan ha en annen vektlegging av hensyn enn det tilsynet har lagt til grunn. Dette fører til avklaringer av rettstilstand og øker forutberegneligheten for enkeltindividet.

Et eksempel er saken hvor Altinn fikk medhold i sin klage på Datatilsynets vedtak om å stanse logging av IP-adresser. Nemnda var enig i at Altinn ikke hadde hjemmel til slik logging i personopplysningsforskriften, men la til grunn at de hadde grunnlag for slik logging i personopplysningsloven § 8 f. Etter denne bestemmelsen skal det foretas en interesseavveining mellom behovet for å lagre opplysningene holdt opp mot personvernet til den enkelte.

Det interessante ved denne avgjørelsen er at selv om det opprinnelige formålet som lå til grunn for tillatelsen ikke umiddelbart var forenlig med en ny tiltenkt bruk, har den behandlingsansvarlige mulighet til å se om det finnes andre rettslige grunnlag som kan forsvare den nye behandlingen.

## **Noen temaer fra saksbehandlingen**

Datatilsynet etterstreber å forbedre regelverket på områder hvor tilsynet mottar gjentatte henvendelser om problematiske forhold. Datatilsynet har i år revidert bankkonsesjonen for å klargjøre forpliktelsene bankene har overfor sine kunder. Innen samme tematikk mottar Datatilsynet en rekke henvendelser fra enkeltpersoner som enten ikke forstår hvorfor de har blitt kredittvurdert, eller de er uenig i at vilkårene for slik vurdering er tilstede.

Tilsynet har notert at kredittselskapene ønsker å ta i bruk flere vurderingskriterier enn tidligere. Adressehistorikk har blant annet blitt innført som parameter på hvor god betaler en person vurderes å være. En tilsvarende utvikling har tilsynet også sett innenfor forsikringsbransjen. Enkelte forsikringsselskaper ønsker å ha med betalingsanmerkninger som parameter for å vurdere skaderisiko, noe som vil gi utslag i premien som forsikringstaker må betale.

Utviklingen synes å gå i retning av at flere og flere opplysninger om enkeltindivider hentes inn og analyseres med henblikk på å kartlegge hvorvidt man er en god kunde eller ikke. En mulig konsekvens av denne utviklingen er at det skapes et A- og B-lag av individer basert på historiske data.

Bruk av ny teknologi bidrar til å viske ut skillet mellom arbeidsliv og privatliv. Henvendelser om arbeidsgiveres innsyn i ansattes e-post og personlige filer på arbeidsgivers nettverk kan betraktes som en indikasjon på denne sammenblandingen. Personvernet utfordres ved at arbeidsgivere mener de har behov for innsyn i data som i utgangspunktet omfattes av privatlivet på jobb. Reglene i personopplysningsloven brytes ved at e-postkasser ikke avsluttes når noen slutter og ved at vedtatte rutiner for innsyn i ansattes e-post utfordres på bekostning av personvernet. Saker om innsyn i e-post er omtalt senere i meldingen.

Mange av sakene som kommer inn viser at publikum har begynt å stille spørsmål ved den alt mer omfattende registrering i arbeidslivet. Saker som går igjen er kameraovervåkning på arbeidsplassen, bruk av sporingsteknologi i kjøretøyer og adgangskontrollsystemer. Det er en økende trend at opplysninger fra forskjellige systemer ønskes sammenkoblet blant annet for kontrollformål. Dette fenomenet kalles formålsutglidning. Det vil se at et system eller en rutine som var ment brukt til et begrenset formål, nyttes til andre formål utover det opprinnelige. Datatilsynet har eksempler på at dette skjer uten at det er gjort kjent for de ansatte i forkant. Slike hendelser skaper mindre forutsigbarhet og vanskeliggjør den ansattes mulighet for å kontrollere hva arbeidsgiver vet om dem, noe som kan rokke ved tillitsforholdet på en arbeidsplass.

## **Juridisk veiledningstjeneste**

I tillegg til saksbehandlingen har den juridiske veiledningstjenesten besvart 2 727 e-poster. Svarene som sendes på e-post er mer uformelle svar på direkte spørsmål og av veiledende karakter. Dersom spørsmålene er mer kompliserte eller bør vurderes som forvaltningsaker, overføres de til saksbehandling i juridisk avdeling og journalføres. Målsettingen er å gi publikum svar innen tre dager på spørsmål som kommer via e-post. I løpet av året besvarte den juridiske veiledningstjenesten dessuten 7 309 henvendelser via telefon.



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.

Tema	Plikt	Rett	Total	Prosent
Annet	190	472	662	9 %
Arbeidsgivers kontroll/innsyn	640	579	1219	17 %
Biometri	20	16	36	0 %
Fødselsnummer	120	440	560	8 %
Helse, forskning	221	136	357	5 %
Internasjonalt (overføring utland)	105	23	128	2 %
Internett (publisering mv)	167	412	579	8 %
Internkontroll/informasjonsikkerhet	316	149	465	6 %
Kameraovervåking	510	362	872	12 %
Kredittopplysning	71	242	313	4 %
Kunderregister/Medlemsregister	255	236	491	7 %
Lokalisering, sensortechnologi	79	91	170	2 %
Lydopptak	92	71	163	2 %
Melding/Konsesjon (rutiner)	686	53	739	10 %
Offentlige registre	147	173	320	4 %
Reservasjon/DM	20	70	90	1 %
Skoles kontroll/innsyn	95	50	145	2 %
<b>Sum</b>	<b>3734</b>	<b>3575</b>	<b>7309</b>	<b>100 %</b>

Det har vært mange spørsmål om GPS-sporing av arbeidstakere, innsyn i e-post og bruk av adgangskontroll på jobben til ulike andre formål. Det har også vært en del spørsmål om e-billettering. Hver tiende henvendelse handler fortsatt om hvordan man skal forstå melde- og konsesjonsplikten og praktiske spørsmål knyttet til innsending av konsesjonssøknader og meldeskjemaer.

### **Overtredelsesgebyr og tvangsmulkt**

Datatilsynet har siden 2009 hatt lovhjemmel til å utstede overtredelsesgebyr og tvangsmulkt overfor pliktsubjekter som enten har overtrådt personopplysningsloven eller som ikke har etterkommet pålegg gitt av Datatilsynet.

For å få benyttet disse sanksjoner har Datatilsynet inngått en avtale med Statens Innkrevingsentral om innkreving av gebyrer/mulkt. Avtalen ble revidert mot slutten av 2010, med mål om å være operativ fra starten av 2011.

Datatilsynet har i 2010 fattet vedtak om overtredelsesgebyr i enkelte av de mest alvorlige sakene. Gebyrets størrelse sier i seg selv ikke noe om alvorligheten i overtredelsen da Datatilsynet har foretatt en totalvurdering, hvor blant annet økonomisk evne er tatt med i vurderingen.

Eksempler på saker tilsynet har tatt stilling til:

- En virksomhet med konsesjon som teleoperatør, ble ilagt et overtredelsesgebyr på kr 30 000,- for å ha lagret ringehistorikk for lenge i henhold til personopplysningsloven og i strid med vilkår i konsesjonen.
- I to ulike saker ble det ilagt overtredelsesgebyr i forbindelse med innsyn i e-postkasse til arbeidstakere. Les mer om dette i kapittel 5.5.1.
- En annen kategori saker det er besluttet overtredelsesgebyr gjelder publisering av opptak fra kameraovervåking som viser personer som tilsynelatende stjeler fra utsalgssteder. Det kan være mange grunner til at virksomhetene tyr til slike metoder, men Datatilsynet er klare på at dette er en gapestokkmentalitet som ikke er ønskelig. Det har i 2010 vært to saker i denne kategorien hvor virksomhetene henholdsvis er ilagt kr 5 000,- og kr 10 000,- i overtredelsesgebyr.
- Et helseforetak hadde over tid unnlatt å gi en pasient innsyn i loggen over hvem som hadde vært inne i vedkommendes pasientjournal - noe de er forpliktet til etter loven. I tillegg unnlot de å svare Datatilsynet på hva som var gjort for å sikre at pasientene i fremtiden fikk praktisert denne rettigheten. Det ble utstedt tvangsmulkt på 5000 kroner per dag til påleggene ble etterfulgt. Datatilsynet er tilfreds med at saken fikk sin avslutning etter at dette tvangsmiddelet ble benyttet.

## **2. KOMMUNIKASJON OG DIALOG**

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

### **Stor medieoppmerksomhet**

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

I løpet av meldingsåret har Datatilsynet besvart over 1 400 henvendelser fra mediene. Dette førte til nær 5 600 registrerte medieoppslag hvor Datatilsynet var nevnt. Temaer som fikk særlig oppmerksomhet var datalagringsdirektivet, krenkelser på Internett, skattelister, saker om helseregistre og bruk av såkalt lokaliseringsteknologi.

Det ble utarbeidet 13 kronikker og debattinnlegg til bruk i medier utenfor Datatilsynet. Videre ble det produsert 92 egne nyhetssaker til hjemmesidene, noen færre enn året før.

168 meldinger ble lagt ut på Twitter. Ved årsskiftet hadde Datatilsynet over 3 000 "followers" på tjenesten. Dette innebærer en tredobling fra året før.

Etterspørselen etter foredragsholdere fra Datatilsynet er fortsatt stor. Det er blitt holdt 136 foredrag ut over Datatilsynets egne kurs og seminarer overfor personvernombudene, mot 110 året før.

### **2.1 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, samt respektere andres integritet. Undervisningsopplegget ble lansert januar 2007, og har siden blitt bygd ut i flere faser.

I mai 2010 ble undervisningsopplegget bygd ut med en ny modul om digital mobbing. Denne er lagt opp som et interaktivt opplegg som kan kjøres i løpet av en eller flere skoletimer. Her finner elevene en quiz om mobbing, faktasetninger, bilder og film som skal gjøre inntrykk. Det er også laget et diskusjonsgrunnlag med ulike situasjoner som klassen skal gå gjennom i fellesskap for så å komme frem til et standpunkt mot digital mobbing. I forbindelse med lanseringen av mobbemodulen ble det i samarbeid med TNS Gallup arrangert en

spørreundersøkelse blant ungdom for blant annet å se omfanget av digital mobbing. Denne ble gjenstand for god mediedekning.

Det har i løpet av meldingsåret vært en nedgang i antall bestillinger av materiell fra skolene, sammenliknet med tidligere år. Høsten 2010 ble det derfor satt i gang et markedsføringsfremstøt som har resultert i en oppgang av antall bestillinger.

Samarbeidet med Teknologirådet og Senter for IKT i utdanningen (som har blitt ny samarbeidspartner i stedet for Utdanningsdirektoratet) fungerer fortsatt meget godt, og er i tråd med mål og prinsipper i den statlige kommunikasjonspolitikken.

## **2.2 ID-TYVERITESTEN**

Datatilsynet sitter i styringsgruppa og er aktivt medlem i ”ID-tyveriprojektet”, som ledes av NorSIS (Norsk senter for informasjonssikring).

En selvtest for ID-tyveri, utviklet i 2009, er et av Datatilsynets bidrag til prosjektet. Kildekoden for testen er nå distribuert til 16 land og testen er tatt i bruk verden over, på seks ulike språk. Id-tyveriprojektet ble i november 2010 tildelt Dataforeningens Rosing IT-sikkerhetspris for denne selvtesten.

Høsten 2010 startet planleggingen av en ny selvtest, denne gang rettet mot næringslivet. Ideen er at testen skal ta for seg ”personopplysningenes liv i en virksomhet”. Også arbeidet med ID-tyveri er i tråd med blant annet helhetsprinsippet i den statlige kommunikasjonspolitikken.

## **2.3 SLETTMEG.NO**

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

Tjenesten slettmeg.no ble lansert 8.mars 2010 som et prøveprosjekt, bemannet med to medarbeidere. Prosjektperioden går ut sommeren 2011.

Siden oppstarten er det blitt ført systematisk statistikk over innkomne henvendelser til slettmeg.no. Det gjør at Datatilsynet sitter på erfaringsbasert kunnskap om hvor skoen trykker for vanlige folks personvern på Internett. Medarbeiderne på Slettmeg.no har kunnskap om hvilke netjtjenester/-sider som er mest problematiske, hvordan man i praksis kan gå frem for å redusere skadevirkningene av nettkrænkelser og hvordan dagens lovgivning fungerer i praksis. Slettmeg.no har dessuten opparbeidet seg unike kontakter hos de viktigste tjenestetilbyderne på Internett, utenlandske så vel som norske. I sum gjør dette at slettmeg.no etter mindre enn ett driftsår sitter på en helt unik erfaringsbasert kompetanse relatert til krænkelser på Internett. Dette kommer også andre aktører til gode. Blant annet har politiet ved flere anledninger fått bistand i saker som involverer utenlandske netjtjenester, for eksempel Facebook.

Fra lanseringsdatoen og ut året håndterte tjenesten i alt 3 236 henvendelser via e-post, telefon, kontaktskjema og chat. I samme periode ble det i gjennomsnitt registrert 70 000 månedlige sidevisninger på [www.slettmeg.no](http://www.slettmeg.no).

Tjenesten har langt på vei lyktes i å nå ut til alle aldersgrupper, ikke bare ungdom. For eksempel kom 22 prosent av henvendelsene fra personer over 45 år.

Det er sendt ut informasjonsmateriell om slettmeg.no til alle landets ungdoms- og videregående skoler. Det ble også produsert to reklamefilmer som ble vist på tv og på kino julen 2010. Slettmeg.no har i rapporteringsåret blitt omtalt i mer enn 500 nyhetsartikler/-reportasjer og medarbeiderne i tjenesten har holdt 13 foredrag over hele landet.

Siden det ikke finnes noen tilsvarende tjenester i andre land har slettmeg.no fått mye oppmerksomhet i utlandet. Det er blitt gitt egne presentasjoner om tjenesten til de nordiske personvernmyndighetene og på et større europeisk møte for personvernmyndigheter. Datatilsynet har på grunn av den store interessen fra utlandet utarbeidet en egen informasjonsbrosjyre om slettmeg.no på engelsk.

At tjenesten har klart å hjelpe så mange forskjellige personer, enten problemet har vært falske profiler, uønsket bildepublisering eller sjikane, må i stor grad tilskrives tjenestens uformelle og praktiske arbeidsmetodikk. Fremfor å fokusere på lovverk og formell saksbehandling, slik man kanskje forventer seg av en offentlig hjelptjeneste, forsøker medarbeiderne på slettmeg.no så langt mulig å holde jussen utenfor. Det har ofte vist seg at enkeltpersoner, så vel som store nettsteder, er langt mer lydhøre overfor konkrete løsningsforslag enn overfor paragrafer og offentlig myndighetsutøvelse. En juridisk tilnærming til personvernkrænkelser på nett munner dessuten fort ut i spørsmålet om hvorvidt den aktuelle nettside/-tjeneste er underlagt norsk jurisdiksjon eller ikke.

Et fellestrekk ved mange av de henvendelsene som slettmeg.no har mottatt er at de som tok kontakt ikke ville ha fått hjelp av andre instanser.

Slettmeg.no bør bli en enda mer benyttet ressurs for alle som arbeider med krenkelsesproblematikk på Internett. Det bør tilrettelegges slik at de erfaringene som tjenesten har opparbeidet seg, og det unike kontaktnettet som medarbeiderne på slettmeg.no har fått utviklet, i enda større grad enn hittil kommer andre til gode. Det vil føre til et bedre forebyggende arbeid, samtidig som skadevirkningene som følge av krenkelser på Internett kan bli ytterligere redusert. Samlet sett vil et virkemiddel som slettmeg.no åpenbart føre til en reduksjon av de samfunnsøkonomiske kostnadene ved nettkrenkelser.

Datatilsynet har derfor overfor Fornyings- administrasjons- og kirke departementet foreslått at slettmeg.no etableres som en permanent veiledningstjeneste.

### 3. DATATILSYNETS KONTROLLVIRKSOMHET

Datatilsynet baserer kontrollvirksomheten på dokumentet ”*Strategi og metodikk for operativt tilsyn med personopplysningsloven*”. Dokumentet legger overordnede strategiske og metodiske føringer for kontrollvirksomheten. Departementets tildelingsbrev, etatsstyringsmøter og virksomhetsplan legger på samme måte spesifikke føringer for prioriteringer, herunder føringer for valg av sektorer, bransje og/eller tema.

Kontrollvirksomheten har vært styrt gjennom halvårlige tilsynsplaner. Det har gitt en god dynamikk og setter etaten i stand til å justere kursen til foreliggende situasjon. En viktig premis er at det skal gjennomføres risikobaserte kontroller. Det innebærer at innsatsen rettes inn mot områder hvor sannsynlighet for regelverksbrudd anses høyt og/eller at konsekvensene ved brudd er mest alvorlige.

Målet med den operative kontrollvirksomheten er å:

- skaffe god kunnskap om trusler mot personvernet innen ulike bransjer
- bruke erfaringene til å sette fokus på personvern i ulike sektorer
- kunne identifisere om visse grupper er spesielt utsatt for krenkelse av personvernet
- overvåke den teknologiske utviklingen og hvilke trusler det innebærer for den enkelte
- bruke erfaringene til å kommunisere med samfunnet forøvrig
- sørge for at avvik fra regelverket hos en behandlingsansvarlig rettes opp

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

#### 3.1 NØKKELTALL

Datatilsynets kontrollvirksomhet omfatter aktiviteter mot i alt 135 virksomheter. Datatilsynet gjennomførte også datainnsamling fra 20 nettsteder hvor informasjon om behandling av personopplysninger og tilstedeværelse av personvernpolicy ble kontrollert. Datainnsamlingen er ikke talt med som kontroller i tabellen i 3.2.

En kontroll krever i gjennomsnitt rundt fem arbeidsdager. Det er imidlertid store variasjoner i ressursbruken, fra tre-fire timer for de enkleste innen kameraovervåking, til kontroller som innebærer ny forvaltningspraksis som kan kreve opp til 10-15 arbeidsdager.

Kontrollvirksomheten medførte 266 varsler om vedtak, hvorav 96 ble ført videre til endelig vedtak. En del saker er stilt i bero i påvente av nødvendige avklaringer mot andre myndigheter. Av de forhold som ledet til formell reaksjon, ble 48 forhold karakterisert som alvorlige.

### 3.2 BRANSJER UNDERLAGT KONTROLL

Følgende bransjer (eller temaområder) var underlagt kontroll i rapporteringsåret:

Bransje / Sektor	Antall	Omtrentlig ressursbruk i ant. ukeverk	Varsel <sup>1</sup>	Vedtak <sup>2</sup>	Alvorlig <sup>3</sup>
Arbeidsliv – adgangskontrollsystem og	11	13	30	10	0
Barn og unge	6	5	12	3	2
Billettformidling	1	2	0	0	0
Finans - betalingsformidling	2	4	6	0	0
Forsikring – barn og livsforsikring	5	5	7	1	1
Helseforskning	10	10	25	0	12
Helse	14	14	21	8	7
Idrett – dopingkontroll	7	7	35	32	5
Justis – utlevering <sup>4</sup>	7	11	0	0	0
Kameraovervåking – kjøpesentre	44	18	71	27	4
Kommune	7	6	22	0	7
Schengen Informasjonssystem (SIS)	2	2	0	0	0
Sosiale nettsamfunn	4	5	12	9	2
Telekom <sup>5</sup>	5	6	3	2	1
Utdanning	8	6	22	4	7
Velferd	2	3	0	0	0
<b>SUM</b>	<b>135</b>	<b>117</b>	<b>266</b>	<b>96</b>	<b>48</b>

Kontrollene fordelte seg på virksomheter i hele 17 sektorer eller bransjer. Dette gir en stor spredning med hensyn til hvilke problemstillinger som er mest fremtredende. Disse trekkes frem under omtale av sektorer i kapittel 5.

<sup>1</sup> Antall såkalte ”varsel om vedtak” som er gitt innen kontrollert sektor.

<sup>2</sup> Antall såkalt ”vedtak om pålegg” som er gitt innen kontrollert sektor. Det gjøres oppmerksom på at en del saker ikke har nådd dette forvaltningsskrittet ved utløp av rapporteringsåret.

<sup>3</sup> Antall forhold som er karakterisert som alvorlige avvik fra regelverket.

<sup>4</sup> Sakene er stilt i bero i påvente av nødvendige avklaringer mot tilgrensende forvaltningsorgan.

<sup>5</sup> Sakene er stilt i bero i påvente av avklaring mot annet forvaltningsorgan. Vedtak vil trolig kunne komme senere.

Etter tilsynets vurdering gir antall ”varsel om vedtak” det mest korrekte bildet av personvernets stilling innenfor ulike sektorer. Vedtak om pålegg vil i mange tilfeller falle bort, enten på grunn av at et forhold er brakt i orden eller at det stilles i bero i påvente av andre prosesser. Det er imidlertid sjelden at et vedtak faller på grunn av nye opplysninger fra tilsynsobjektet.

### **3.3 SAMARBEID MED ANDRE MYNDIGHETER**

Datatilsynet gjennomfører tidvis kontroller innen områder hvor det finnes en sektormyndighet. Datatilsynets praksis i slike situasjoner er å søke kontakt med den relevante sektormyndigheten for å avklare rammene for samarbeidet.

Tilsynet samarbeider tettest med Statens Helsetilsyn og Finanstilsynet. Årsaken til det er at både helse- og finanssektoren er områder hvor Datatilsynet har vært aktiv over tid. Det er også et økende samarbeid med Post- og Teletilsynet ettersom flere av kontrollaktivitetene har vært rettet mot telesektoren i meldingssåret.

### **3.4 BRUK AV FORMELLE REAKSJONER**

Datatilsynets praksis er å benytte formelle reaksjoner ved regelverksbrudd. Påpekning av plikt benyttes i tilfeller hvor det lovstridige forholdet anses å være mindre alvorlig, eller at tilsynet ikke har ført tilstrekkelig bevis for overtredelsen. I øvrige tilfeller hvor det foreligger regelverksbrudd, benyttes vedtak.

Et vedtak stiller strenge krav til kvalitet i saksbehandlingen og gir kontrollobjektene formelle 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 de berørte virksomhetene må høres før tilsynet fatter sin beslutning.

Bruk av tvangsmulkt kan benyttes i de tilfeller hvor vedtak ikke følges opp fra virksomhetens side. Videre kan overtredelsesgebyr benyttes i tilfeller hvor det avdekkes svært alvorlige brudd på regelverket.

### **3.5 MÅLOPPNÅELSE**

Datatilsynet har gjennomført kontroller innen et bredt spekter av virksomheter. Kontrollene og rapportene som er utarbeidet på basis av disse, har vært viktige bidrag til å avklare personvernets stilling innen ulike sektorer. I mange av sektorene har kontrollene videre utløst etterfølgende prosesser i berørte sektorer.

Datatilsynet mener å ha oppnådd de resultater som har vært planlagt i rapporteringsåret. Produksjonen av antall kontroller ligger noe over det som fremgår av tilsynsplanen, men ressursbruken ligger innenfor de fastlagte rammene. Det relativt høye innslaget av kontroller innen kameraovervåkning vil påvirke antallet, uten at uttaket av ressurser påvirkes vesentlig.



### **3.6 GENERELT OM FUNN OG SVAKHETER AVDEKKET VED KONTROLL**

#### **Variierende kjennskap til regelverket**

Kjennskapet til regelverket er varierende hos virksomhetene som er kontrollert. Hos noen sektorer er kunnskapsnivået tilfredsstillende, mens den i andre er tilnærmet fraværende.

Datatilsynet opplever at en kombinasjon av tilrettelagt informasjon, en opplevd sannsynlighet for kontroll og aktiv oppfølging av bransjeforeninger er den mest effektive metoden for å fremme etterlevelse av regelverket. Det hjelper lite å ha tilrettelagt informasjon dersom virksomhetenes mottakelighet ikke er tilstede.

Store virksomheter, omfattet av en høy grad av offentlig regulering, synes å slite med prioritering mellom regelverk. Med det menes uklarhet med hensyn til hvilke rettsregler som kommer til anvendelse, og hvilke av disse som bør prioriteres. Mange virksomheter har et sterkt fokus på sektorregelverk (i den grad slikt finnes), mens de glemmer andre sektorovergripende regler.

#### **Mangelfull ansvars plassering**

Stadfesting av behandlingsansvar er meget viktig for å få god etterlevelse av regelverket. 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. Tilsynet har blant annet sett eksempler på at offentlige aktører har etablert fellesløsninger uten særlig blick på regelverkets krav.

Datatilsynet registrer også utfordringer i forhold til større private virksomheter. Selv om det er plassert et ansvar hos øverste leder, kan det være svikt i den videre organiseringen. Det kan være at interne rutiner ikke er kjent og at det ikke rapporteres om avvik. I slike tilfeller vil det kunne skje systematiske avvik uten at dette "fanges opp av radaren".

Når det gjelder små og mellomstore private virksomheter er den kritiske faktoren ofte manglende kunnskap til regelverket. Det hviler et bredt ansvar på daglig leder. Manglende oversikt og kunnskap gjør at vedkommende i mange tilfeller ikke er fullt ut klar over sitt ansvar. Her synes bransjeforeningene å være en avgjørende faktor. Disse kan både bidra til å klargjøre hvilke rettsregler som gjelder og se disse i sammenheng med andre.

Ansvar handler ikke bare om interne forhold i virksomheten. Behov for samhandling på tvers i en sektor utløser gjerne behov for felles løsninger. I slike sammenhenger er det viktig å holde ryddighet i forhold til ansvarsforhold. Virksomhetene kan ikke uten videre etablere løsninger uten at de rettslige rammene er klarlagt. Kontroller foretatt i meldingsåret, avdekket sviktende ansvars plassering i to samarbeidende konstellasjoner: organisering av opptak til videregående skole (VIGO) og i E-fakturasystemet. Disse sakene er gjennomgått under henholdsvis punkt 5.4.1 og 5.10.2

### **Motstand mot sletting**

Datatilsynet observerer en økende tendens til lagring av personopplysninger. Registreringen synes også i økende grad å være mer ”klebrig” enn før. Er opplysningene først registrert, vegrer behandlingsansvarlige seg for å slette dem. Videre er det vanskelig å få gjennomslag for teknikker som kan bedre personvernets kår, for eksempel gjennom bruk av aidentifisering, pseudonymisering eller anonymisering. Slike teknikker oppfattes ofte som kompliserte og fordyrende av behandlingsansvarlige.

Når Datatilsynet avdekker brudd på slettebestemmelsene bestrider virksomhetene i det lengste å følge tilsynets pålegg om strengere slettepraksis. Ulik argumentasjon blir anført. Stort sett finner de behandlingsansvarlige støtte for sin argumentasjon enten i arkivlov, skatte- og regnskapslov eller forbrukerhensyn. Slik settes den registrertes personvern opp mot andre interesser.

### **Internkontroll og informasjonssikkerhet**

Internkontroll og informasjonssikkerhet er fortsatt en utfordring for virksomhetene. Det er mange som ikke har fått dette på plass, systemene er mangelfulle eller er ikke oppdatert. Ofte savnes ledelsens hånd på rattet. Manglende internkontroll øker risikoen for en lovstridig behandling av personopplysninger. Dette gjør det igjen vanskeligere for den registrerte å kunne ivareta sine lovfestede rettigheter.

Når det gjelder informasjonssikkerhet stiller mange av de kontrollerte objektene svakt i forhold til å dokumentere en god sikkerhet. De mangler klare rammer for å oppnå tilfredsstillende sikkerhet, risikovurdering og dokumentasjon av informasjonssystemet.

Det er fortsatt store utfordringer når det gjelder å understøtte gode prosesser i virksomhetene. Tilrettelegging av informasjonsmateriell er alene ikke tilstrekkelig. Slikt materiell har vært tilgjengelig i mange år, tidvis med aktiv markedsføring. Virksomhetene må ha en egenvilje til å få ting på plass. Den viktigste drahjelpen er trolig at bransjeforeninger engasjeres i arbeidet med å motivere egne medlemmer.

## 4. TENDENSER OG UTVIKLINGSTREKK

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 personvernets stilling i Norge.

### 4.1 PERSONOPPLYSNINGER SOM HANDELSVARE

Personopplysninger er en raskt voksende handelsvare. Det er særlig på Internett, herunder sosiale medier, og gjennom bruk av såkalte apps<sup>6</sup> at innsamling av personopplysninger er i kraftig vekst. Foredling og salg av opplysningene eller, tilgjengeliggjøring av profil dannet på bakgrunn av disse, formidles enten via nettet eller i andre kanaler. ”It’s free, and will always be”, står det blant annet på nettsiden til en av de største tilbyderne av sosialt nettverk. Dette er misledende informasjon, siden brukerne i praksis betaler i form av egne personopplysninger. Slike selskaper er ikke veldedige organisasjoner, men selskaper som tjener penger på personlige opplysninger generert fra sine brukere. Det samme gjelder for andre ”gratistjenester”, og tusenvis apps som man kan laste ned på telefonen.

De såkalte gratistjenestene har ofte som forretningsidé at brukeren betaler ved å stille sine personopplysninger til rådighet for videresalg i bytte mot et gode. Brukeren er sjelden bevisst at det faktisk skjer, men lever på forestillingen om at det er skaffet til veie et vederlagsfritt produkt.

Personopplysninger er en verdifull handelsvare fordi den gjør det enklere for blant annet annonsører å treffe riktige målgrupper. Det har vokst frem en industri av selskaper som spesialiserte seg på å selge profiler basert på innsamlede personopplysninger fra nett og app-brukere til annonsører og andre som ønsker å drive mer direkte rettet reklame. Økningen i antall opplysninger som samles inn øker treffsikkerheten og dermed betalingsviljen hos en kommersiell virksomhet.

Datatilsynet ser for seg at denne utviklingen vil forsterkes i årene som kommer.

Kombinasjonen av å motta ”gratis” tjenester i bytte mot informasjon om adferd og preferanser sitter tilsynelatende løst hos mange. Brukerne overskuer ikke nødvendigvis rekkevidden av sine valg, og mange er kanskje heller ikke særlig interessert i å holde seg informert om hva som faktisk skjer bak fasaden: Hvem er det virksomheten deler informasjon med, og på hvilken måte? Problemet som oppstår er dermed at mange samtykker til en behandling av personopplysninger som de ikke overskuer rekkevidden av. Med gyldig samtykke i hånd kan markedsføringskanalen gå langt i retning av å tilby stadig flere personopplysninger til annonsørene. Borgeren strippest for stadig flere og mer inngripende opplysninger, uten at vedkommende er bevisst hvilken krets disse opplysningene blir spredt til.

Når det gjelder apps lastet ned på smarttelefoner, finnes det ofte ikke en personvernerklæring å samtykke til i det hele tatt. Når man laster ned og installerer et program på en datamaskin

---

<sup>6</sup> App er forkortelse på applikasjon, som den siste tiden særlig har blitt brukt om mobiltelefonapplikasjoner, og da særlig i sammenheng med etableringen av Apples App Store i 2008, og senere Androids app store.

vil man så å si uten unntak måtte godkjenne en brukerlisens og personvernerklæring før man får installert programmet. Enkelte apps har sin personvernerklæring liggende på en nettside, men ikke inne i selve applikasjonen. Det vil derfor i tiden fremover være særlig viktig å følge med på utviklingen av applikasjoner for smarttelefonmarkedet, og hvordan de behandler personopplysningene de samler inn.

Det sendes mye informasjon ut fra mobiltelefoner som ikke avklares med brukeren på forhånd. Wall Street Journal har overvåket verdens 100 mest brukte apps, og funnet ut at halvparten sender ut informasjon om brukernes telefonbruk<sup>7</sup>. Dette rammer nesten alle som bruker apps aktivt. Å regulere dette området er utfordrende da markedet er globalt og jurisdiksjonen uklar. Ansvarsforholdet mellom plattformtilbydere og tredjepartsutviklere av apps er også ofte uavklart. EU jobber i dag med en modernisering av sine personvernregler for å tilpasse disse til netjtjenester som Facebook og applikasjoner og tjenester på smarttelefoner og nettbrett.

Datatilsynet nedsatte i 2010 en arbeidsgruppe som skal se på personvernmessige utfordringer knyttet til sosiale nettsamfunn og apps. Gruppen leverte et forprosjekt om sosiale medier med utgangspunkt i Facebook høsten 2010. Dette arbeidet står nærmere beskrevet under punkt 5.3.1 i årsmeldingen.

#### **4.2 "KLEBRIG" OFFENTLIGHET**

Fra sentrale, statlige myndigheters side er man opptatt av å fortelle, særlig de unge, om betydningen av å respektere hverandres personvern og om mulige konsekvenser ved publisering av personopplysninger på Internett. Men hva med oss selv? Er statlige og kommunale myndigheter bevisst sitt ansvar ovenfor enkeltindivider når postjournaler og andre offentlige dokumenter og opplysninger publiseres på Internett?

En åpen statsforvaltning er et viktig demokratisk gode. Offentleglova er et viktig verktøy for å sette presse og borgerne i stand til å føre demokratisk kontroll med myndighetene.

I 2009 fikk vi en ny offentlighetslov som er langt klarere enn tidligere med hensyn til hva stat og kommune kan og skal publisere på Internett. Det gjør det lettere for offentlige etater å forholde seg til reglene. Tilgjengeliggjøring og tilrettelegging av offentlig informasjon for viderebruk, som for eksempel karttjenester, værdata og befolkningsstatistikk, er også en god ting.

Men hva med saksdokumenter som inneholder personopplysninger om deg og meg? Datatilsynet registrerer at det er en tendens til at offentlige myndigheter i stadig større grad også offentliggjør slike opplysninger, enten ved en glipp eller fordi det ikke er tilstrekkelig med bevissthet rundt hvilke dokumenter som egner seg for publisering. Isolert sett vil publisering av enkeltdokumenter muligens ikke ha en krenkende effekt, men kraftige søkermotorer gjør personopplysninger tilgjengelige i *samlet form*, til tross for at de i

---

<sup>7</sup> The Wall Street Journal: *Your Apps Are Watching You*, 17. desember 2010.

utgangspunktet er publisert hos *ulike* aktører. Den personifiserte offentlighet gjør borgeren sårbar, spesielt sett over tid.

Vi føler vårt personvern krenket ikke bare når hemmelig og taushetsbelagt informasjon kommer på avveie, men også når allerede offentlig tilgjengelige opplysninger blir gjort enda mer tilgjengelige – når vi føler at vi mister kontrollen over opplysningene om oss selv. Derfor reagerer en stor andel av befolkningen på mediernes publisering av skattelister. Det strider mot sentrale personvernprinsipper at opplysninger den enkelte norske borger er pliktig til å levere inn, skal kunne brukes til underholdning eller tilbys for salg. Slik informasjon har også blitt lettere tilgjengelig i form av diverse applikasjoner, som kobles opp mot andre eksisterende nettjenester eller lignende.

Denne problematikken er som nevnt særlig relevant i forhold til frislippet av skatteopplysninger, men også personopplysninger fra andre offentlige registre, som for eksempel Brønnøysundregisteret, motorvognregisteret og aksjonærregisteret, kan ha kommersiell interesse for aktører i og utenfor Norge. Det offentlige har i enkelte situasjoner pålagt seg selv å lage begrensinger i søkefunksjonaliteten. Dette gjelder blant annet for offentlig postjournal for departementer og direktorater og konkursregisteret der det kun er mulig å søke på navn i ett år. Fra tidligere tider husker vi skattelister som kun var tilgjengelig fra Skattedirektoratet og på kommunehuset i tre uker. Slike selv pålagte begrensinger blir imidlertid virkningsløse når opplysningene lastes ned og publiseres av andre.

### **Demokratisk paradoks**

Datatilsynet er bekymret, ikke bare for at enkeltpersoner skal oppleve at det ved feil legges ut sensitive personopplysninger om dem, men også for at frykten for feil, identitetstyveri og profildannelse skal medføre at befolkningen avstår fra å klage eller på annen måte benytte seg av rettigheter de har overfor det offentlige. Dette utgjør i så fall et betydelig demokratisk problem.

Slik offentleglova praktiseres i dag kan det diskuteres hvorvidt formålet med loven oppfylles. Formålet med en åpen offentlighet er at den skal gi borgerne *kontroll med myndighetene*. Men hvis ikke myndighetene har en helhetlig tilnærming til hvilke opplysninger som publiseres på Internett, kan åpenheten i verste fall også føre til *tap av kontroll* for den enkelte borger.

Datatilsynet støtter tanken om en åpen forvaltning, men mener statlige og kommunale myndigheter må bli mer bevisste hvilke opplysninger som publiseres. Det er ikke åpenhet om saker i seg selv som er problemet, men at en sak gjøres tilgjengelig på Internett på en slik måte at den "klebres" til enkeltpersoner i årevis via søkemotorer. Offentlige virksomheter må i større grad vurdere risikoen knyttet til publisering av personopplysninger, og hvordan disse potensielt kan gjenbrukes eller misbrukes av andre aktører på Internett i etterkant. Praksis med å gjøre postjournaler og andre dokumenter med personopplysninger tilgjengelige for eksterne søkemotorer bør opphøre, fordi dette medfører at myndighetene i praksis *mister kontrollen* over opplysningene de er ansvarlige for. Det er fullt mulig å ivareta offentlighetshensynet uten at opplysninger tilgjengeliggjøres på denne måten. Offentleglova

pålegger ikke virksomhetene å publisere alle offentlige dokumenter på nett, kun å gjøre de tilgjengelige for innsyn ved forespørsel.

### **Staten som informasjonssamler**

I tillegg til at det offentlige er en stor bidragsyter til personopplysninger på Internett, har Nasjonalbiblioteket tatt på seg oppgaven med å samle inn og lagre informasjon som er åpent tilgjengelig på norske nettsider – på samme måte som blant annet trykte bøker, aviser og tidsskrifter blir lagret. Dette innebærer at opplysninger som både private og offentlige har lagt ut kan bli samlet inn – alt fra private og offentlige hjemmesider til blogger og nettaviser. Der det offentlige har lagt ut informasjon med et uhell – noe som dessverre ikke er uvanlig – kan den samme informasjonen bli lagret hos Nasjonalbiblioteket som dokumentasjon fra vår tid.

Nasjonalbiblioteket har i dag en tidsavgrenset konsesjon fra Datatilsynet til å samle inn åpent tilgjengelig informasjon. Datatilsynet har oppfordret lovgiver til å vurdere hva som bør være Nasjonalbibliotekets rolle på dette området innen konsesjonen går ut i 2012. Konsesjonen sier at informasjon som er forsøkt skjermet ikke skal samles inn. Nasjonalbibliotekets innsamling er lite kjent, og mange som legger ut informasjon har nok ingen formening om at informasjonen vil bli lagret for evig tid. Ett av vilkårene for innsamlingen er derfor at Nasjonalbiblioteket setter i gang egnede informasjonstiltak. Datatilsynet har lagt til grunn at lovgiver vil vurdere den videre framtiden til den informasjonen som allerede er samlet inn – om denne skal lagres, tilgangsbegrenses for en kortere eller lengre periode eller om det for deler av informasjonen skal vurderes en begrenset tilgang for allmennheten.

### **4.3 TAP AV KONTROLL I NETTSKYEN?**

Mange flytter i dag mye av den informasjonen som tradisjonelt har vært lagret lokalt på datamaskinen ut på nettet, til den såkalte nettskyen. Dette er en økende trend både blant privatpersoner og virksomheter. Nettskyen (cloud computing) er en felles betegnelse for et vidt spekter av tjenester som leveres over eksterne nettverk, for eksempel over Internett. Slike tjenester kan være datainnsamling, dataprosessering, databasetjenester og datalagring i store eksterne serverparker. Oppdragsgiver sitter ikke nødvendigvis med kunnskap om hvor informasjonen lagres og med hvilke ressurser en eventuell bearbeiding av opplysninger skjer. En viktig drivkraft hos næringsaktører for å ta i bruk slike tjenester er økt fleksibilitet, skalering av datakraft og lagring etter behov, samt betaling etter faktisk bruk av dataressursene. Blant private brukere vil tilsvarende drivkraft kunne være at tjenesten er tilpasset konkrete behov, har tilpassede verktøy integrert i tjenesten, er reklamefinansiert og således uten direkte kostnader.

Det kan være praktisk og kostnadseffektivt å benytte nevnte tjenester. For privatpersoner er det hendig at innholdet kan nå uavhengig av hvilken datamaskin man bruker. Det gjør det også lettere å dele informasjon med andre. Bilder og dokumenter som deles fra en eksternt plassert server, kan suppleres med andres bidrag og gi merverdi til alle deltakerne. Det finnes videre leverandører som tilbyr tjenester som tar sikkerhetskopi av innholdet på private datamaskiner. Kjøper man et nytt kamera kan man for eksempel få tilgang til et

lagringsområde som ligger hos produsenten av kameraet. Bildene kan for eksempel lagres automatisk på en webasert konto når de flyttes over fra kameraet til datamaskinen. Brukeren trenger ikke gjøre noe aktivt, men kan leve i trygg forvisning om at det ved lokalt sammenbrudd av dataressurser eksisterer en sikkerhetskopii der ute et sted. For virksomheter kan lagring i nettskyen være et praktisk og prismessig gunstig alternativ i forhold til å anskaffe og drifte lokale løsninger.

Selv om lagring i nettskyen har positive sider, har Datatilsynet erfart at det reduserer brukernes kontroll med dataene. Mange av tjenestetilbyderne har ikke en egen serverpark, men må bruke en annen leverandør for den faktiske lagringen. Sett fra oppdragsgivers side vil det derfor ofte være liten kontroll over hvor dataene som er lastet opp i realiteten befinner seg. I noen tilfeller flyttes også dataene fra server til server, gjerne mellom flere land, alt etter hvor det er ledig serverkapasitet. Enkelte selskaper unnlater å gi sine kunder garanti for at dataene blir behandlet i henhold til et bestemt lands regelverk.

Datatilsynet mener det er viktig at både privatpersoner og virksomheter er bevisst de usikkerhetsmomentene som gjelder ved kjøp av ovennevnte tjenester. Hva gjelder virksomheter som behandler personopplysninger, må disse forvise seg om at behandlingen av personopplysningene skjer i samsvar med personopplysningsloven. Dette innebærer blant annet at man forvisser seg om at tilstrekkelig sikkerhet er etablert. Overføres personopplysninger til land utenfor EØS krever regelverket en prosess i forhold til Datatilsynet, med mindre vertslandet har inngått avtale eller har etablerte ordninger med medlemsstatene<sup>8</sup>.

Datatilsynet fikk i 2009 varsel om at enkelte bankers IKT-oppgaver ble flyttet til serverparker i lavkostland. Kontroll utført av tilsynet viste at en sparebank gjennom en databehandler hadde utplassert noe av håndteringen av bankens personopplysninger til Ukraina og India. Finanstilsynet sendte i 2010 ut et rundskriv som påpekte at utkontrahering av sentrale IKT-oppgaver til land med høy risiko innebærer en kritisk risiko for driftsstabiliteten i norske banker. Håndtering av kundeopplysninger ble av Finanstilsynet holdt frem som en særlig kritisk IKT-oppgave som ikke kan flyttes til landområder med høy risiko. Datatilsynet støtter Finanstilsynets vurdering.

#### **4.4 INNEBYGGET PERSONVERN BLIR VIKTIG**

Datatilsynet har lagt økende vekt på å medvirke til at personvern bygges inn i nye teknologiske løsninger fra starten. Personvern fremmende teknologi, eller personvernvennlig design (*privacy by design* på engelsk) vil være et satsingsfelt hos Datatilsynet i årene som kommer. Denne tilnærmingen anerkjenner at et godt personvern ikke kan sikres utelukkende ved hjelp av lover og regulering, men at personvern ideelt sett må inngå som en naturlig del av organisasjonenes virksomhetsstyring.

---

<sup>8</sup> Et eksempel på en slik avtale er den såkalte "Safe-harbour" avtalen.

Hensynet til personvern har tradisjonelt ikke vært et viktig nok designkriterium når nye informasjonssystemer har blitt konstruert. En konsekvens av dette er at mange systemer derfor er utformet slik at de ikke uten videre kan tilpasses personvernlovgivningens krav, med mindre det legges inn nye, og ofte store investeringer. Dersom det ikke bygges inn personvern i designfasen ved nyutvikling, viser det seg også ofte å være vanskelig å få dette til i ettertid. Sentrale valg kan være tatt som potensielt kompromitterer personvernet til de registrerte.

Personvernvennlig utforming fordrer oppdragsgivere som har personvern som et element i sitt verdigrunnlag. Brukernes personvern må bety noe for dem og de må stille krav ovenfor utviklerne. Utviklerne på sin side må forstå betydningen av disse verdivalgene og må bygge disse inn i systemene de utvikler. Etter tilsynets oppfatning nås sistnevnte gruppe best ved at tilsynsmyndighetene deltar i og påvirker standarder som systemer bygges etter. Dersom personvern inngår som et kriterium i internasjonalt anerkjente standarder, er det rimelig grunn til å tro at de vil etterleves.

I løpet av få år vil det installeres elektroniske strømmålere i hjemme våre, med direkte oppkobling til energiverket for avlesning av strømforbruket. Datatilsynet har vært i tett dialog med regelverksutvikler på området for å sikre at informasjon som innhentes er relevant og at den slettes når formålet er oppfylt. Gjennom slik dialog kan man sikre at slike systemer ikke utvikler seg til å bli et personvernproblem i fremtiden.

Et eksempel på en annen sektor hvor det er viktig og aktuelt å tenke innebygget personvern, er i helse- og omsorgssektoren. Staten har avsatt milliarder av kroner til å utvikle nye IT-systemer som skal bedre samhandlingen i helsesektoren. Her er det avgjørende at godt personvern bygges inn som en naturlig del av systemutviklingen fra starten, for blant annet å sikre gode systemer for tilgangsstyring.

#### **4.5 GODE HELSEREGISTRE – BEDRE HELSE?**

Datatilsynet observerer at helsesektoren er et område hvor personvernet er under stort press. Sektoren er preget av høyt politisk fokus, en forventningsfull befolkning og økende bruk av informasjonsteknologi. Det foregår mange parallelle prosesser, som delvis griper over i hverandre. Dette gjør at det kan være vanskelig å holde en tilfredsstillende oversikt. Desto viktigere er det at tilsynsmyndighetene er tilstede og samarbeider godt med aktørene. Et godt personvern i sektoren er avgjørende for å ivareta tillitten mellom helsepersonell og pasienter.

Datatilsynet har identifisert noen viktige drivkrefter i helsesektoren:

- Forventning om å kunne samle inn og forske på helseopplysninger.
- Større mobilitet av pasienter, hvor forventning om mobilitet av helseopplysninger gjør seg tilsvarende gjeldene.
- Et ønske om å kunne effektivisere pasientbehandlingen ved bruk av informasjonsteknologi.



I rapporteringsåret har det vært spesielt fokus på modernisering av helseregisterområdet. Helse- og omsorgsdepartementet sendte i meldingsåret rapporten ”*Gode helseregistre – bedre helse*” (*strategi for modernisering og samordning av sentrale helseregistre og medisinske kvalitetsregistre*) på høring. Rapporten var ledet av en topp tung styringsgruppe, med representanter fra departement, helseforetak, Helsedirektoratet og Folkehelseinstituttet. Den vil danne grunnlaget for myndighetenes arbeid på helseregisterområdet fremover.

Datatilsynet hadde flere merknader til strategirapporten. De viktigste merknadene gikk på strategiens valg av registerform og at prinsippet om pasientenes samtykke i ønskende grad settes til side. Datatilsynet er også skeptisk til at det i rapporten åpnes for en sammenslåing av helseregistrene til et altomfattende sentralisert helseregister.

Norge har mange helseregistre sammenlignet med andre land. Formålet med registrene er at vi skal styre og administrere samfunnsoppgaver med større kunnskap, kvalitet, rasjonalitet og effektivitet. Registrene bygges ut i fra gode hensikter, men er ikke uproblematisk selv om hensiktene er gode. Helseregistrene inneholder helseinformasjon om praktisk talt hele den norske befolkningen fra fødselen og livet ut, og må derfor oppfattes som særlig sensitive registre<sup>9</sup>. Hovedregelen som er gitt fra lovgivers side er at opprettelsen av nye sentrale helseregistre skal bygge på samtykke fra de registrerte. Tilsynet registrerer at dette prinsippet ofte fravikes ved praktisk utforming av regelverket i tilknytning til loven.

### **Flere registre – mindre samtykke**

I strategirapporten ”*Gode helseregistre – bedre helse*” tas det til orde for å opprette en lang rekke nye registre — registre som skal omfatte særlig sensitive opplysninger over psykiske lidelser, rusmisbruk, syndromer, sjeldne tilstander, misdannelser, ulykker, vold, traumer. Det legges også opp til at data skal kunne innhentes fra primærhelsetjenesten. Sistnevnte forslag vil innebære en enorm økning av den offentlige fangsten av taushetsbelagt informasjon, og vil etter Datatilsynets oppfatning representere en uthuling av taushetsplikten.

Strategirapporten legger opp til at helseopplysninger om norske borgere skal lagres obligatorisk, uten krav til samtykke og at de samtidig skal være personidentifiserbare. I rapporten har man heller ikke klart gått inn for at man skal kunne reservere seg mot å bli registrert. Datatilsynet er skeptisk til en slik utvikling.

### **Helseregisterdata til biobank-forskning**

Et av formålene med de nye foreslåtte registrene er å legge til rette for forskning på årsaker til sykdom. Helseinformasjon hentet fra helseregistrene skal kombineres med informasjon fra norske biobanker, og deles med forskere internasjonalt. Datatilsynet anser at forslagene omkring utnyttelse av biologisk materiale potensielt kan utgjøre et stort inngrep i den enkeltes personvern. Biologisk materiale må betraktes som spesielt sensitive data, da analyser av biologiske data potensielt kan avsløre mye mer informasjon om en person enn tradisjonelle helseopplysninger.

---

<sup>9</sup> NOU:2009:1, *Individ og integritet. Personvern i det digitale samfunnet*, Oslo 2009, s. 184

### **Et felles sentralisert helseregister**

Slik Datatilsynet forstår det, signaliserer helsemyndighetene gjennom rapporten ”*Gode helseregistre – bedre helse*” og *Strategi for Norsk Helsenett*<sup>10</sup> et ønske å etablere et altomfattende helseregister.

Dette er ikke en ønsket utvikling sett fra Datatilsynets side. Av hensynet til personvernet er det en grunnleggende forutsetning at forvaltningen av de ulike helseregistrene holdes atskilt. En sentral lagring av helseopplysninger, herunder sentralisering av flere uavhengige registre, representerer et økt inngrep i den enkeltes personvern. Ansvar for de ulike helseregistrene bør tillegges ulike organisasjoner, slik at det opprettes skranker ved koblinger og utleveringer. Dersom det ikke opprettes slike skranker vil ulovlig bruk av helseregistrene kunne skje uoppdaget.

På Island ble den foreslåtte sentrale helsedatabasen stanset av Høyesterett da de kom til at den streid mot Grunnlovens bestemmelser om personvern. Registeret er nå etablert med samtykke og kryptering hos ekstern part.

---

<sup>10</sup> *Strategi for Norsk Helsenett*, utarbeidet av Norsk Helsenett og sendt på høring 29. april 2010.

## **5. NÆRMERE OM UTVALGTE FELTER**

### **5.1 JUSTIS OG UTLENDINGSFELTET**

Innenfor denne sektoren håndteres store mengder sensitive personopplysninger. Den registrerte har minimalt med autonomi, og har begrenset kunnskap om hvilke informasjonsbehandlinger som finner sted. Rettssikkerheten settes på prøve i enkeltindividets møte med store systemer og tunge samfunnsinteresser.

Diskusjonen rundt datalagringsdirektivet satte sitt preg også på året som gikk. Andre viktige saker var at Politiregisterloven endelig ble vedtatt og at Stortinget vedtok endringer i straffegjennomføringsloven som vil styrke personvernet til de innsatte i norske fengsler.

#### **5.1.1 Norge bør si nei til Datalagringsdirektivet**

Gjennom sine årsmeldinger til Stortinget har Datatilsynet de siste årene advart mot innføring av Datalagringsdirektivet i norsk rett. En innføring av direktivet vil innebære en statlig pålagt innsamling og lagring av opplysninger om hvilke personer som til enhver tid kommuniserer med hverandre ved hjelp av elektroniske hjelpemidler, når kommunikasjonen skjer, og hvor den enkelte da befinner seg. Opplysningene skal lagres i minst seks, maksimalt 24 måneder.

Datalagringsdirektivet ble også i meldingsåret det dominerende politiske personvernspørsmålet ved at Regjeringen i januar sendte ut en felles høring om implementering av direktivet. Etter en gjennomført høringsrunde ble et lovforslag om innføring av direktivet lagt frem i desember 2010. I tillegg til å avgi høringsuttalelse har Datatilsynet deltatt i møter og debatter, og har skrevet flere leserinnlegg og kronikker. Det har vært en prioritert oppgave å synliggjøre de alvorlige personvernkonsekvensene av forslaget.

At staten iverksetter overvåkingstiltak som retter seg mot hele samfunnet, uten at det foreligger mistanke mot noen, og før det engang er identifisert et mulig lovbrudd, innebærer et paradigmeskifte i norsk strafferettstradisjon. Det kan ikke sees på som annet enn et uttrykk for at hele folket i praksis settes under mistanke.

Forfatningsdomstolene i Romania og Tyskland har da også fastslått at direktivet, slik det er implementert i disse landene, er i strid med landenes nasjonale konstitusjoner. Dette viser hvor tett direktivet går de allmenne demokratiske rettsprinsipper på klingen.

Det stilles også spørsmål ved tiltakets effektivitet. Utviklingen går i retning av at svært mange kanaler for kommunikasjon ikke vil bli omfattet av lagringsplikten. Over 60 prosent av alle nordmenn kommuniserer via Facebook. Folk ringer på Skype og svært mange benytter seg av internettbaserte e-postjenester som det ikke blir lagringsplikt for. Dette vet terrorister og tunge kriminelle. Tiltaket vil derfor i første rekke ramme uskyldige. Dersom direktivet innføres vil det med stor sannsynlighet senere også bli foreslått å tette de stadig flere og stadig større hullene som vil komme i forhold til lagringsplikten.

I tillegg må det advares mot en såkalt 'formålsutglidning'. Et register som inneholder så mange detaljerte opplysninger om folks kommunikasjonsmønstre og bevegelser vil få mange interessenter også utenfor politiet som vil ønske tilgang. NAV kan finne flere trygdemisbrukere, samferdselsmyndighetene kan avsløre brudd på kjøre- og hviletidsbestemmelsene og forsikringsselskaper kan avsløre forsikringssvindlere. Basert på erfaring gjennom flere år mener Datatilsynet at det er all grunn til å frykte en slik utvikling. Og, dersom vi først aksepterer prinsippet om utvidet lagring av denne typen personopplysninger for hele befolkningen. Hvordan kan vi da sette grensen mot neste steg, lagringsplikt for personopplysninger vi etterlater oss også i andre sammenhenger? Hvordan kan vi, etter å ha trådt over en prinsipielt viktig grense, si nei til pålagt og utvidet lagringstid for sosiale nettsamfunn, bomstasjoner eller de nye kameraene for måling av gjennomsnittsfart på veiene? Også disse elektroniske sporene vil naturlig nok kunne være nyttige for politiet til bekjempelse av alvorlig kriminalitet. Eller for andre aktører.

Datatilsynet har også lang erfaring med at data kommer på avveier, selv om disse i utgangspunktet skal være godt sikret. Mennesker gjør feil, foretar feilvurderinger og begår lovbrudd, selv i de mest betrodde stillinger. Tilsynet har derfor pekt på at de registrene som som lagres i henhold til datalagringsdirektivet vil være utsatt for like stor fare for lekkasjer som alle andre registre med personopplysninger.

Endelig har Datatilsynet pekt på usikkerheten rundt hva vi egentlig vedtar. EUs varslede evaluering vil utvilsomt føre til endringer i direktivet. Dersom Norge først sier ja til datalagringsdirektivet vil det være svært vanskelig å si nei til senere endringer.

### **5.1.2 Personvern i politisektoren - Politiregisterloven**

Datatilsynet har i mange år arbeidet for å få på plass et tilfredsstillende regelverk for politiets behandling av personopplysninger, og er svært tilfreds med at politiregisterloven ble vedtatt av Stortinget i meldingsåret. Tilsynet ønsker velkommen et klarere regelverk for politiets behandling av personopplysninger, og ser frem til å få styrket sin tilsynskompetanse i denne sektoren.

Samtidig er tilsynet bekymret for at politiet ikke greier å etterleve kravene i det nye regelverket med de informasjonssystemene som politiet har til rådighet i dag. Datatilsynet har tidligere avdekket mangler ved politiets systemer, særlig knyttet til informasjonssikkerhet.

Betydningen av å ha gode systemer, med blant annet god tilgangsstyring og logging, ble tydeliggjort i den såkalte ambassadesaken som ble avdekket høsten 2010. Der fremkom det påstander om at ansatte i politiet var engasjerte av den amerikanske ambassaden til å samle inn og rapportere opplysninger om norske borgere til amerikanske myndigheter. Tilsynet tviler på om det er mulig med dagens registre å avdekke hvorvidt også opplysninger fra politiets egne registre har tilflytt ambassaden.

Datatilsynet vil også minne om at EU vedtok en rammebeslutning i 2008, om at personverndirektivet skal få delvis anvendelse for behandling av personopplysninger i

justissektoren. Det er forutsatt at dette kravet implementeres, også i Norge, innen september 2011.

Datatilsynet har i 2010 deltatt i referansegruppen for utarbeidelse av forskrift til politiregisterloven.

### **5.1.3 Dødsstedsundersøkelser ved plutselig og uventet småbarnsdød**

Til tross for at tilsynet har pekt på stor fare for rettssikkerhetsbrudd ble ordningen med frivillige dødsstedsundersøkelser likevel etablert i november 2010.

Dødsstedsundersøkelsene medfører at det i regi av Folkehelseinstituttet skal gjennomføres undersøkelser av det sted hvor et barn mellom 0 og 3 år er funnet dødt. De som gjennomfører undersøkelsen skal besitte både medisinfaglig og politifaglig realkompetanse. Undersøkelsen skal være frivillig for den eller de som hadde omsorg for barnet da det døde, og blir å anse som en del av helsehjelpen til det døde barnet.

Justisdepartementets lovavdeling har uttalt at undersøkelsene kan hjemles i samtykke fra den som hadde omsorg for barnet på dødstidspunktet. Departementet forutsatte imidlertid klart at samtykket i det enkelte tilfellet måtte være gyldig etter personopplysningslovens krav.

Datatilsynet, som forvalter personopplysningsloven, har understreket at det å tilfredsstille lovens krav til et samtykke vil være svært vanskelig i denne type saker. Dersom en undersøkelse skjer uten gyldig samtykke, vil det kunne medføre brudd på EMK artikkel 8.

### **5.1.4 Personvern i fengslene – ny straffegjennomføringslov (ILA-saken)**

I 2007 gjennomførte Datatilsynet tilsyn med Kriminalomsorgens behandling av personopplysninger. Tilsynet avdekket store mangler ved etterlevelsen av personopplysningslovens krav, og Datatilsynet anbefalte at straffegjennomføringsloven ble endret.

Datatilsynet er svært tilfreds med at Stortinget i 2010 har vedtatt endringer i straffegjennomføringsloven for å avklare ansvarsforhold og styrke personvernet til de innsatte og deres pårørende.

### **5.1.5 Overvåkingssaken ved den amerikanske ambassaden**

I november avdekket TV2 Nyhetene at det angivelig hadde pågått overvåking av norske borgere i områdene rundt den amerikanske ambassaden i Oslo. Det ble hevdet at også tidligere ansatte i politiet og forsvaret bistod ambassaden i denne aktiviteten. Mål for overvåkingen var folk som hadde demonstrert utenfor den amerikanske ambassaden og i områdene rundt. De påfølgende ukene fulgte andre medier opp med nyhetssaker der påstanden var at enkelte politifolk hadde jobbet dels for den amerikanske ambassaden og dels for norsk politi. Flere medier antydte at amerikansk ambassadepersonell hadde hatt indirekte tilgang til norske politiregistre ved å knytte til seg slik arbeidskraft.

I den offentlige debatten som fulgte var det viktig for Datatilsynet å påpeke at saken i hovedsak dreide seg om seg om suverenitetsspørsmål, i forhold til hvilken myndighet som kan operere på norsk jord. Etter tilsynets syn må ambassader avgrense seg til utøvelse av politilignende myndighet innenfor ambassadeområdet. Saken dreide seg også om at flere viktige rettssikkerhetsgarantier - og prinsipper – i slike prosesser kunne bli satt til side. Det ble særlig påpekt at ”hemmelige aktiviteter” kan medføre at folk ikke innrømmes viktige rettigheter, slik som retten til å gi tilsvaret, retten til å forsvare seg mot anklager og retten til forsvarer.

Tilsynet påpekte også personopplysningene ble sendt til en database i USA, og at det var umulig å vite hvordan de ble lagret, eller hvem som lagret dem. Folk mistet dermed den kontrollen som følger av personvernretten, for eksempel retten til innsyn, til retting og til sletting. Det ble også uttrykt bekymring for at andre lands myndigheter muligens hadde hatt indirekte tilgang til politiregistrene.

### **5.1.6 Samarbeid med Utlendingsforvaltningen**

I løpet av meldingsåret har det vært avholdt en serie møter med Utlendingsdirektoratet (UDI), etter initiativ fra direktoratet. Bakgrunnen for møtene er at UDI har gått gjennom den generelle konsesjonen fra Datatilsynet, i lys av den nye utlendingslovgivningen. I den forbindelse har det blant annet oppstått spørsmål om nye, konkrete databehandlingsmåter faller innenfor konsesjonen, eller om det vil være nødvendig med ytterligere konsesjonssøknader.

Det sentrale spørsmålet har likevel vært om dagens utlendingslovgivning kan sies å oppfylle hjemmelskravet i personopplysningsloven § 33 fjerde ledd, som angir at konsesjonsplikten ikke gjelder for statlige og kommunale organ når behandlingen av personopplysninger har hjemmel i egen lov. Oppfyller utlendingslovgivningen dette hjemmelskravet gir det i så fall unntak fra konsesjonsplikten. Spørsmålet har vært vurdert i relasjon til ulike behandlingsmåter, og forskjellige kategorier av persondata.

Møteserien forventes å fortsette i 2011.

Justis- og politidepartementet sendte i 2010 på høring en rekke forslag til endringer i utlendingsloven. Datatilsynet har blant annet stilt seg kritisk til departementets forslag om å senke terskelen for å iverksette frihetsberøvelse etter utlendingsloven, fra ”*skjellig grunn til mistanke*” til ”*grunn til å anta*”. Det samme gjelder forslaget om en utvidelse av oppbevaringstiden for fingeravtrykk i utlendingsregisteret.

## **5.2 TELESEKTOREN**

### **5.2.1 Simonsensaken – fortsatt fildelingsjakt etter nemndas avgjørelse**

Simonsen Advokatfirma ble i 2006 gitt en tidsbegrenset konsesjon til å behandle personopplysninger som et ledd i bekjempelsen av ulovlig spredning av opphavsrettighetsbeskyttede åndsverk på Internett (ulovlig fildeling). Datatilsynet ga

advokatfirmaet tillatelse til å samle inn og registrere IP-adresser som er observert i aktivitet på ulike fildelingsnettverk, for å danne bevisgrunnlag for straffeforfølgelse og erstatningssøksmål for brudd på åndsverklovens bestemmelser.

Advokatfirmaets søknad om forlengelse av konsesjonen ble avslått ved Datatilsynets vedtak i juni 2009. Avslaget var begrunnet i at denne type virksomhet hadde så nære likhetstrekk med en politietterforskning at den i utgangspunktet burde foretas av politiet. Den tidligere konsesjon med senere forlengelser var gitt med tidsavgrensning i påvente av et lovarbeid som ikke skjedde innen tidsrammen for konsesjonen.

Klagen ble oversendt Personvernemnda for klagebehandling. I november 2010 gjorde nemnda om Datatilsynets vedtak, slik at konsesjonen skulle forlenges ut året. Personvernemnda fant at den aktuelle behandlingen av personopplysninger var nødvendig for at rettighetshaverne skal kunne gjøre gjeldende eller forsvare sitt rettskrav overfor personer som bedriver ulovlig fildeling. Personvernemnda stilte tydelige vilkår for forlengelsen, blant annet at informasjonen til de registrerte måtte forbedres.

Datatilsynet har løpende vurdert konsesjonen gitt til advokatfirmaet Simonsen. Tilsynet vurderer nå hvorvidt andre enn Simonsen bør være innehaver av konsesjonen. Som Personvernemnda peker på er det rettighetshaverne som eier det "krenkede" åndsverket og tilsynet antar at det er rettighetshaver som derfor bør være rette innehaver av konsesjonen. Advokatfirmaet Simonsen vil, hvis et slikt tankesett legges til grunn, fortsette det de gjør på vegne av rettighetshavere i henhold til en avtale dem i mellom. Dette er en vurderingsprosess som vil fortsette inn i kommende år.

### 5.2.2 Google Street View

I forbindelse med fotografering av nye områder for tjenesten *Google Street View*<sup>11</sup> ble det lastet ned og lagret, innholdsdata fra private trådløse nettverk. Selskapet ønsket, som et ledd i å styrke presisjonsnivået for lokalisering av mobile enheter (smarttelefoner m.v.), å stedfeste nettverkene. Dette gjøres ved at navn på nettverket (SSID), den trådløse nettverkets unike nummer (MAC-adresse til router) og GPS-informasjon sammenstilles. I april 2010 informerte selskapet tilsynet om at det i tillegg til tilsiktet fangst av data også hadde blitt lagret innholdsdata som ble kommunisert på nettverket. Selv om det kun var fragmenter av innholdsdata som var blitt lastet ned, ble det senere slått fast at disse dataene kunne inneholde informasjon som for eksempel brukernavn og passord for ulike netttjenester, slik som for eksempel Facebook. Da dette ble kjent stoppet Google umiddelbart enhver videre innhenting av data fra WiFi-nettverk ved bruk av sine street-view-biler.

Tilsvarende problemstilling har oppstått i mange Europeiske land. Flere personvernmyndigheter valgte å forfølge forholdet rettslig. Datatilsynet vurderte også tilsvarende reaksjon, men valgte i tråd med øvrige nordiske datatilsyn å kreve sletting av overskuddsinformasjonen. Slettingen har imidlertid blitt stilt i bero da materialet er påberopt

---

<sup>11</sup> Google Street View er en kartbasert tjeneste som tilbys av Google Inc.

som bevis i de nevnte rettslige prosesser i øvrige land. Datatilsynet arbeider fortsatt med å komme frem til en hensiktsmessig løsning.

Sommeren 2010 fortsatte Google Street View fotograferingen i Norge. I begynnelsen av desember 2010 ble det nye materialet publisert, og billedgrunnlaget er mer enn doblet siden forrige publisering. I Norge har det ikke vært særlige protester mot Google Street Views aktivitet. Datatilsynet har ikke sett behov for å iverksette tiltak overfor Google så identifiserende blir fjernet fra bildene. Selskapet raskt reagerer også raskt når brukere melder inn uønskede bilder. I Tyskland har forøvrig nesten 3% av husstandene ønsket å fjerne sitt hus fra Google Street View-tjenesten.

### **5.2.3 Tilsyn – Politiets innhenting av opplysninger fra teleselskapene**

Datatilsynet har ved tidligere tilsyn observert mulig uklare forhold med hensyn til utlevering av elektroniske spor fra telekommunikasjonsvirksomheter til politiet. Det var derfor ønskelig å gjennomføre tilsyn hos telekommunikasjonsvirksomhetene som forestår utleveringen til politiet.

Formålet med tilsynene var å kartlegge hvilke prosesser som utløser bruk av trafikkdata, samt å undersøke hvor tilgjengelig slike spor er for politiet. Videre ønsket tilsynet å kartlegge hvilke kriterier som må tilfredstilles før en utlevering kan finne sted. Datatilsynet gjennomførte tilsyn hos fire tilbydere av offentlige elektroniske kommunikasjonsnett eller offentlige teletjenester. I tillegg besøkte vi to politistasjoner og ble informert om deres prosedyrer opp mot teleselskapene. Det ble avdekket en noe varierende praksis med utlevering av nevnte data. Dette gikk både på det rettslige grunnlaget for utleveringen og omfanget. En stor del av utleveringen skjer ved at en mistenkt eller siktet gir sitt samtykke til politiet. Et sentralt spørsmål i denne sammenheng har vært om vilkårene for et frivillig, uttrykkelig og informert samtykke er til stede. Tilsynet avdekket for øvrig flere avvik med hensyn til manglende sletting av trafikkdata og/eller ip-adresser hos teleleverandørene.

Tilsynene er blitt fulgt opp med dialog med både Riksadvokaten og Post- og teletilsynet. Formålet har vært å drøfte avdekkede problemstillinger med disse aktørene før vedtak fattes ovenfor teleselskapene. Datatilsynet har i kraft av tilsynene fått større kjennskap til de prosesser politi og tilbydere har ved behandling av trafikkdata, og søker i det videre å få klarlagt overfor partene hvilke vilkår som må være oppfylt for at behandlingen skal være i tråd med personopplysningsloven.

### **5.2.4 Tilsyn – Nummeropplysningsvirksomheter**

Teleselskaper er etter lov om elektronisk kommunikasjon (ekomloven) pliktige til å levere ut kundeopplysninger til nummeropplysningsvirksomheter, med mindre det foreligger en reservasjon fra kundes side. Det er sterk konkurranse innen dette markedssegmentet. Flere av aktørene har tilført andre tilstøtende tjenester til sin nummeropplysningsvirksomhet, slik som kart, bursdager, horoskop og posisjonstjenester. Dette omtales som såkalte verdiøkende tjenester, det vil si tjenester hvor nummeropplysningsaktøren benytter andre



informasjonskilder for å berike opplysningene fra teleoperatøren, og/eller at opplysninger fra teleoperatøren brukes til å vaske andre databaser (som for eksempel markedsføringsinformasjon). Bakgrunnen for Datatilsynets tilsyn med sektoren var et ønske om å undersøke hvorvidt virksomhetene benytter kundeopplysningene fra teleselskapene til andre formål enn det som er opprinnelig forutsatt.

Datatilsynet gjennomførte fire tilsyn, to mot rene nummeropplysningsvirksomheter og to mot virksomheter som sammenstiller informasjon mottatt fra teleoperatører. De to sistnevnte virksomhetene tilbyr andre nummeropplysningsaktører tilgang til sine nummeropplysningsdatabaser.

Tilsynene har i hovedsak hatt fokus på forholdet mellom telekundens samtykke ovenfor teleoperatøren og videre bruk, samt verdiøkende tjenester. Gjennom tilsynene har Datatilsynet søkt å skaffe en oversikt over hvor opplysningene som vises hos nummeropplysningstjenestene kommer fra, hvordan informasjonen behandles hos nummeropplysningsvirksomheten (herunder også historiske data) og hvor opplysningene beveger seg videre. Bildet er adskillig mer komplekst enn at nummeropplysningsvirksomheter kun sammenstiller og viderefremidler informasjon fra teleoperatørene gjennom tradisjonelle nummeropplysning på telefon, Internett og sms.

Det er Post- og teletilsynet som forvalter ekomloven, og det er derfor naturlig å ha et samarbeid med dem ettersom nummeropplysningsbransjen har et skjæringspunkt mellom tilsynsmyndighetene med hensyn på lovverk og anvendelse av disse.

De nevnte tilsynene er nylig avsluttet og det er derfor vanskelig å komme med noen konklusjoner eller videre saksgang før dialogen med Post- og teletilsynet er avsluttet.

## **5.3 SOSIALE NETTSAMFUNN**

### **5.3.1 Prosjekt om sosiale nettsamfunn**

Datatilsynet har gjennomført et forprosjekt om sosiale medier med utgangspunkt i Facebook. Prosjektrapporten ble levert 1. desember 2010. Prosjektarbeidet har blant annet vist at profilinformasjonen som hver enkelt bruker frivillig gir fra seg, kun er en liten del av den samlede informasjonen som Facebook innhenter.

Forprosjektet viste også at Facebook samler inn informasjon om nettbrukere som ikke er medlem av Facebook. Via selskapets ulike informasjonsapplikasjoner (f.eks. "Liker") innhenter Facebook opplysninger om brukere av andre nettsteder som Facebook kan identifisere via for eksempel IP-adresse eller cookies. Som motytelse får nettsidene som implementerer Facebooks informasjonsapplikasjoner blant annet tilgang på statistikk.

Med i overkant av 500 millioner brukere over hele verden, og en stadig økende tilstedeværelse på nettet forøvrig, er Facebook i dag en stor aktør i det markedet hvor personopplysninger anvendes til kommersielle formål. I Norge ser man en utvikling hvor også bedrifter, organisasjoner og offentlige aktører velger å benytte seg av Facebook. Et av

forprosjektets konklusjoner er derfor at overnevnte problemstillinger ikke kan ignoreres i Datatilsynets videre arbeid, uavhengig av om norsk rett har jurisdiksjon over Facebook eller ikke.

Datatilsynet vil sende rapporten til personvernmyndighetene i andre europeiske land når den er ferdigstilt, med sikte på å samordne felles innsats/aksjoner på området.

### **5.3.2 Tilsyn – sosiale nettsamfunn**

Datatilsynet har mottatt gjentatte klager fra publikum på hvordan ulike sosiale nettsamfunn behandler personopplysningene til brukerne. Det ble med bakgrunn i dette gjennomført tilsyn med fire ulike nettsamfunn.

De gjennomførte tilsynene viste flere fellestrekk. Majoriteten av nettsamfunnene har ikke jobbet systematisk med utfordringer knyttet til personvern og hvordan de behandler personopplysninger. Det er et stort problem at flere av nettsamfunnene kopierer andre aktørers personvernpolicy, i stedet for å skreddersy retningslinjer tilpasset eget nettsted. Dette resulterer i lange og ofte uoversiktlige personvernpolicyer, preget av at de tilpasses utfordringer administratorene oppdager etter hvert.

En annen utfordring er videresalget av personopplysninger som flere nettsamfunn er engasjert i. Enkelte nettsamfunn informerer brukerne om at opplysningene vil kunne bli videreformidlet til samarbeidspartnere, men informerer sjelden om hvem disse er, hvordan opplysningene vil bli brukt og eventuelt om brukeren kan reservere seg mot dette.

Det ble videre avdekket at sikringen av personopplysningene ikke er tilstrekkelig utviklet hos nettsamfunnene. Løsningene er utviklet for at det skal være enkelt for brukerne å benytte nettstedet og for administratorene å administrere det. Etter Datatilsynets oppfatning er dette en bransje med store personvernutfordringer.

### **5.3.3 Klage på Facebook og Zinga fra Forbrukerrådet**

Datatilsynet mottok i meldingsåret en klage fra Forbrukerrådet angående Facebook og Zynga, som er en av applikasjonsleverandørene til Facebook-plattformen.

Forbrukerrådet fremmet en rekke innsigelser mot et utvalg av de databehandlinger som det mener Facebook eller Zynga er ansvarlig for. I hovedsak dreier det seg om forhold knyttet til innhenting, utveksling og utlevering av opplysninger om Facebook sine brukere.

Innsigelsene ledsages for øvrig av en generell oppfordring til Datatilsynet om å vurdere hvorvidt andre aspekter vedrørende Facebooks databehandlinger krever nærmere undersøkelse og oppfølging. Dette gjelder blant annet innsamling av personopplysninger som er definert som sensitive, og om brukernes samtykke kan sies å danne et godt nok rettslig grunnlag for behandlingen av disse. Forbrukerrådet ønsker dessuten en avklaring om hvorvidt personopplysningslovens krav til informasjonsplikt, relevans og saklighet er overholdt.

I klagen bes Datatilsynet om å ta stilling til om den norske personopplysningsloven kommer til anvendelse på de aktuelle databehandlingene. Spørsmålet byr på tvil, ettersom loven først og fremst gjelder virksomheter som er etablert i landet.

Det springende punktet er om hjelpemiddelkriteriet i lovens § 4 kan sies å være oppfylt, ettersom det innhentes informasjon ved hjelp av ”cookies” og lignende. Besvarelsen av dette spørsmålet utgjør derfor det grunnleggende premisset for Datatilsynets videre håndtering av klagen.

Selve klagesaken er fremdels under behandling, men henvendelsen fra Forbrukerrådet var med på å bidra til at Datatilsynet startet opp prosjektet om sosiale nettsamfunn høsten 2010.

## **5.4 SKOLE, BARN OG UNGE**

Barn og unge får registrert og lagret opplysninger om seg selv i langt større grad enn det som var tenkelig få tiår tilbake. Undervisningsinstitusjonene har i økende grad tatt i bruk elektroniske verktøy i sitt undervisningsopplegg. Læringsverktøy gir muligheter for kontroll av elevene, og til dels lærerne, i et omfang som tidligere ikke har vært mulig. Tilsyn i sektoren i året som gikk avdekket at behandlingsansvaret ikke er tilstrekkelig avklart når flere virksomheter samarbeider om en tjeneste.

### **5.4.1 Tilsyn – opptakssystemet for videregående opplæring (VIGO)**

Datatilsynet har gjennomført en rekke tilsyn mot utdanningssektoren de siste årene. Det er blant annet gjennomført tilsyn med individuelle opplæringsplaner og med håndtering av innrapportering i forbindelse med nasjonale prøver.

Våren 2010 ble det satt fokus på systemet for opptak til videregående utdanning – VIGO.

Det er gjennomført fem tilsyn med dette systemet. Tilsynene fordelte seg på henholdsvis to kommuner, to fylkeskommuner, VIGO Styre (eier av VIGO) og selskapet IST som er databehandler. Fokus ved tilsynene var på behandlingsansvar, behandlingsgrunnlag, databehandlerrelasjoner og ivaretagelsen av informasjonssikkerhet. Tilsynet så i tillegg på informasjonsutvekslingen mellom partene, informasjonsplikt, lagring og sletting.

For å sikre at alle elever bosatt i en fylkeskommune skal få oppfylt sin lovmessige rett til videregående opplæring innhenter fylkeskommunen en rekke elevopplysninger fra kommunene. Dette omfatter blant annet midlertidige karakterer og fraværsopplysninger. Elevopplysningene overføres i forkant av inntakene til de ulike skolene og studieretningene. Dette gjøres blant annet for å dimensjonere tilbudet til elevene, slik at flest mulig skal få sitt første ønske om videregående opplæring oppfylt. Fordi elevopplysningene innhentes før søknadsfristen, omfatter disse også elever som ikke søker seg til videregående opplæring. Fylkeskommunen har imidlertid et ansvar for å følge opp også disse elevene.

Datatilsynet avdekket manglende behandlingsgrunnlag for utlevering av elevopplysninger fra kommunen til fylkeskommunen. Informasjonsplikten er heller ikke tilstrekkelig oppfylt, da

verken eleven eller foresatte blir informert om at opplysninger om dem blir overført til fylkeskommunen.

VIGO styre, som ble etablert av Forum for fylkesutdanningsjefer, har lagt føringer for hvordan overføring av elevopplysninger skal skje og den videre bruken av disse opplysningene. Et problem i saken er at opplysningene kommer fra den enkelte kommune som skoleeier for grunnskolen. Datatilsynet mener at det ikke er klart at det finnes grunnlag for en slik utlevering av opplysninger om elever som VIGO styre legger opp til. VIGO styre har blant annet lagt til grunn at all elevinformasjon fra samtlige fylkeskommuner skal lagres i en sentral database. Dette er problematisk fordi VIGO styre ikke er en egen juridisk enhet, og derfor ikke har det juridiske ansvaret etter personopplysningsloven. Videre finnes ingen rutiner for sikkerhetskopiering, lagringstid eller sletting i den sentrale databasen. Tilsynet nevnte også utfordringer rundt utlevering av denne informasjonen til tredjepart for rapportering og opprettelse av brukerkontoer hos MinID.

Møte mellom Utdanningsdirektoratet, Kunnskapsdepartementet og Datatilsynet ble avholdt etter kontrollene for å orientere om funn og avklare videre prosess i saken. Det ble informert om at revisjon av opplæringslova er under arbeid, men at dette vil ta noe tid. Datatilsynet avventer en videre prosess.

#### **5.4.2 Tilsyn – elektroniske klassestyringsprogrammer**

Datatilsynet har mottatt klager og bekymringsmeldinger fra elever som føler seg overvåket av lærerne gjennom såkalte elektroniske klassestyringsprogrammer, både i og utenfor skoletiden. Et klassestyringsprogram er et program som gir læreren tilgang til å se hva eleven gjør på sin datamaskin i sanntid. Læreren har full kontroll over systemet, og kan blant annet begrense elevene sin tilgang til enkelte programmer og til Internett.

Datatilsynet har gjennomført tilsyn ved én videregående skole, og sett på hvordan de benytter klassestyringsprogrammet. Da det kun har vært gjennomført ett tilsyn har Datatilsynet liten erfaring med skolenes bruk av klassestyringsprogrammer generelt.

Tidligere gikk læreren fysisk rundt i klasserommet og kontrollerte elevenes arbeid. Nå kan denne kontrollen foretas elektronisk ved at læreren går inn og sjekker hver enkelt elevs arbeid på datamaskinen. Den opplevde overvåkingen fra lærerne er nok større enn den reelle, men elevene har ingen mulighet for å finne ut i hvor stor utstrekning læreren er inne og kontrollerer deres arbeid. Hvis skolen gir elevene mangelfull informasjon om dette, og de ikke forstår formålet med styringsverktøyet, skaper det bekymring fra elevenes side.

Løsningen er at skolene lager klare retningslinjer for bruken av klassestyringsprogrammene, slik at både elever og lærere er kjent med hvilke rammer programmet skal benyttes innenfor.

#### **5.4.3 Tilsyn – institusjoner som hjelper barn og ungdom**

Datatilsynet har prioritert tilsyn med virksomheter som arbeider med barn og ungdom. Erfaring tilsier at disse er sårbare grupper. I rapporteringsåret ble det blant annet foretatt tilsyn

ved Kompetanseteam mot tvangsekteskap, underlagt Integrerings- og mangfoldsdirektoratet, Senter for ungdomshelse, samliv og seksualitet, Atferdssenteret, Barnehuset i Oslo, Senter mot incest og seksuelle overgrep Sør-Trøndelag og to private skoler.

I enkelte tilfeller starter virksomheter som arbeider med ovennevnte grupper som et pilotprosjekt, hvor en konkret oppgave, et konkret problem eller utfordring skal løses. Prosjektene kan være finansiert av det offentlige, av ideelle organisasjoner eller en kombinasjon av disse. De kan også være et samarbeid mellom flere offentlig myndigheter. Datatilsynet erfarer at de rettslige rammer omkring behandlingen av personopplysninger ikke alltid er tilstrekkelig avklart. Det er også blitt avdekket en del andre utfordringer under kontrollene men Datatilsynet har opplevd en god prosess med de berørte aktører i ettertid. En ryddig behandling av personopplysningene, på en sikkerhetsmessig forsvarlig måte og med klare ansvarsforhold blant de involverte er blant de forhold som har stått mest sentralt i denne prosessen. Datatilsynet mener at slik ryddighet er viktig for aktørene selv, siden tilliten nettopp tuftes på en forsvarlig behandling av brukernes personopplysninger.

#### **5.4.4 Personvernskolen i regi av Universitetet i Oslo**

Personvernskolen er et nettsted som drives av Senter for rettsinformatikk ved Universitetet i Oslo. Nettstedet skal hjelpe til med fortolkning av personopplysningsloven og forskriften. Her kan man finne forklaringer til paragrafene i loven, samt spørsmål og svar relatert til behandling av personopplysninger.

Datatilsynet har sagt ja til å være høringsinstans på de svar som publiseres på siden. I forbindelse med personvernskolen har det kommet opp flere interessante personvernproblemstillinger knyttet til skole, forholdet skole – hjem og i brytningen mellom offentlig administrasjon og eleven som individ. Spørsmål om elever kan rustes i skolens regi, hvilke tilganger foreldre skal ha til elevers læringsplattformer, og når hjemmet skal ha kunnskap om fravær fra skolen, er temaer som har vært behandlet.

Deltakelsen har bidratt til økt kunnskap om hva elever og personer med tilknytning til skolen faktisk lurere på. Datatilsynet ser positivt på dette prosjektet, og anser det som et godt bidrag til å promotere personvern som et spørsmål som angår mange.

### **5.5 ARBEIDSLIV**

Datatilsynet får svært mange henvendelser med spørsmål om personvern i arbeidslivet. Det er et stort engasjement både fra arbeidstakersiden og arbeidsgiversiden. Datatilsynet opplever en klar vekst i detaljregistrering av personopplysninger. Opplysningene registreres for ulike formål. Dette kan blant annet være av sikkerhetshensyn (adgangskontrollsystem, kameraovervåking), bedriftsøkonomiske hensyn (flåtestyringssystem ved hjelp av GPS, elektroniske kjørebøker) eller for å ivareta lovpålagte krav (opptak av telefonsamtaler). Innsamlingen av opplysninger om ansatte gjøres som hovedregel ikke for å kontrollere ansatte, men det oppfattes allikevel ofte som et kontrolltiltak av de ansatte. Når dessuten

opplysningene først foreligger, opplever Datatilsynet ofte et ønske om å bruke disse til etterfølgende kontroll der arbeidsgiver har mistanke om at ansatte har opptrådt klanderverdig.

Det er videre en merkbar økning i spørsmål med internasjonal grenseflate, slik som overføring av personopplysninger om ansatte til utlandet, screening og utvidet lagringsplikt for e-post.

### **5.5.1 Innsyn i e-post**

Etter at nye regler om innsyn i e-post trådte i kraft i 2009, har Datatilsynet behandlet mange saker som omhandler dette. Hovedregelen etter de nye reglene er at arbeidsgiver bare har innsyn i ansattes e-post når det er nødvendig for å ivareta virksomhetens daglige drift eller andre berettigede interesser, eller når det er begrunnet mistanke om at arbeidstakeren bruker e-postkassen på en måte som innebærer grovt brudd på arbeidsforholdet.

Til tross for at regelverket har klargjort mange spørsmål, er bredden på problemstillingene som tas opp stor. Datatilsynet erfarer fortsatt at arbeidsgivers kjennskap til reglene om innsyn i e-post er sviktende, og at mange brudd på personopplysningsforskriften skyldes uvitenhet, samt manglende retningslinjer internt i virksomheten.

Som ledd i å gjøre regelverket bedre kjent har Datatilsynet avholdt foredrag for en rekke fagforeninger, og er i ferd med å ferdigstille en veileder om temaet.

Datatilsynet har i to saker som omhandlet grove brudd på bestemmelsene om innsyn i e-postkasse ilagt overtredelsesgebyr på henholdsvis 15 000 kroner og 75 000 kroner. I den ene saken opprettholdt arbeidsgiver den ansattes e-postkasse, videresendte all innkommet e-post til sin egen adresse, samt lagret kontoens innhold. I sak nummer to fikk en vikar tilgang til en sykmeldt arbeidstakers e-postkasse, slik at alt innhold ble tilgjengeliggjort over en lengre periode. Datatilsynet fastslo at virksomheten kunne ivaretatt bedriftens behov på en langt mer personvernvennlig måte. Vedtakene er ikke påklaget.

I 2010 har det videre vært enkelte rettssaker som angikk arbeidsgivers adgang til å foreta innsyn i arbeidstakers e-postkasse. Datatilsynet har vært inne i et par av disse sakene. I et tilfelle ble det tatt ut midlertidig forføyning som nedla et forbud mot å gjøre innsyn inntil saken var behandlet av Datatilsynet. Spørsmålet i saken handlet om adgangen til å foreta innsyn i e-postmeldinger og dokumenter knyttet til disse i arbeidstakernes private e-postkonti. Dette når kontoene befant seg på datamaskiner som ble stilt til arbeidstakernes disposisjon til bruk i arbeidet ved virksomheten. Datatilsynet kom til at det ikke kan gjøres innsyn i slike meldinger, da dette ville utgjøre et brudd på bestemmelsene i personopplysningsforskriften.

### **5.5.2 Tilsyn - innsyn i e-post**

Datatilsynet har gjennomført tilsyn hos flere mediehus hvor fokus har vært på virksomhetens plikt til å sørge for å etablere og etterleve regelverkets krav om innsyn i e-post og sletting av e-postkasse ved opphør av arbeidsforhold. Ingen av virksomhetene hadde foretatt innsyn i ansattes e-postkasser.

Det ble imidlertid fattet vedtak i alle tilsynene. Dette omfattet blant annet manglende etablering, implementering og etterlevelse av internkontroll i form av utarbeidelse av rutiner for innsyn i e-post og sletting av e-postkasser ved opphør av arbeidsforhold. Videre ble det konstatert avvik i forhold til etablering, implementering og etterlevelse av informasjonssikkerhet. Dette gjaldt spesifikt for gjennomføring og oppfølging av tiltak i henhold til risikovurdering samt gjennomføring og håndtering av avvik. Det ble også påvist mangler i forhold til etablering av databehandleravtaler med leverandører.

### **5.5.3 Tilsyn – Adgangskontrollsystem**

I meldingsåret gjennomførte Datatilsynet fem tilsyn med adgangskontroll som tema. Tilsynene var rettet mot de store aktørene innen oljesektoren (Total, Shell, Esso og Statoil). I tillegg ble det gjort tilsyn ved adgangskontrollsystemet i Oljedirektoratet. Tidligere var slike system konsesjonsbelagt, men etter Personopplysningsloven fra 2001 er bruk av adgangskontroll nå bare meldepliktig. Datatilsynet ønsket å se nærmere på om forholdene hadde endret seg vesentlig i denne perioden.

Det var systemsvikt hos de selskapene som ble kontrollert, da det manglet dokumenterte rutiner på flere vesentlige punkter, blant annet ved bruk av passeringslogg. Fire av foretakene hadde heller ikke overholdt meldeplikten overfor Datatilsynet. Et krav som Datatilsynet har påpekt både gjennom tidligere konsesjonsvilkår og senere tolkninger av regelverket, er at passeringslogg bare kan registreres ved samtidig bruk av PIN-kode (autentisering), og at denne loggen ikke kan oppbevares lenger enn tre måneder. To av tilsynsobjektene hadde lagret passeringsloggen langt utover disse tre månedene, og ett av foretakene hadde ikke slettet loggen siden 2002. Et foretak registrerte passeringslogg uten bruk av PIN-kode. Det var også dårlige rutiner for informasjon overfor nytilsatte om bruken av adgangskontrollanlegget.

På bakgrunn av de avvik og merknader som ble fastlagt ved tilsynene ble det utferdiget en ny veileder fra Datatilsynet om bruk av adgangskontrollsystem. Veilederen ble kommunisert til sikkerhetsbransjen.

### **5.5.4 Tilsyn – GPS-sporing**

Datatilsynet har de senere årene mottatt en rekke henvendelser som knytter seg til GPS-sporing i arbeidslivet. Årsaken til de mange henvendelsene er at flere og flere virksomheter bruker eller ønsker å bruke sporingsteknologi, og at regelverket som regulerer slik bruk har vært vanskelig tilgjengelige. Berørte aktører er ansatte, tillitsmannsapparatet, arbeidsgivere eller leverandørene/produsentene av GPS-enhetene.

På bakgrunn av de mange henvendelsene har tilsynet kontrollert flere virksomheter som har innført GPS-sporing i sine kjøretøy. Formålet med tilsynene har blant annet vært å kartlegge omfanget av bruken av sporingsteknologien, om regelverket blir fulgt i de tilfeller sporingsteknologi benyttes, og for å få kjenneskap til hvilket formål virksomhetene har for å innføre GPS-sporing.

Datatilsynet publiserte i 2010 veilederen «Bruk av sporingsteknologi i virksomheters kjøretøy» på egne nettsider. Tilsynet har i den forbindelse innhentet en uttalelse fra Skattedirektoratet om hvordan skattelovgivningen regulerer lagring av data, når GPS-enheten benyttes som en elektronisk kjørebok. Skattedirektoratet konkluderer med at det er 10 års lagringsplikt når den bokføringspliktige har valgt å oppfylle sin dokumentasjonsplikt ved å føre kjørebok.

### **5.5.5 ID-kort i byggebransjen**

Datatilsynet har hatt en lang prosess ovenfor Arbeids- og inkluderingsdepartementet i tilknytning til innføring av identitetskort på byggeplasser. I forbindelse med en kontroll som tilsynet gjennomførte i 2008 ble det reagert på en rekke forhold rundt nevnte ordning. Etter tilsynets oppfatning var det uklare rettslige rammer rundt utstedelse av slike kort. Tilsynet stilte seg også kritisk til kvaliteten i prosessen rundt utstedelse av kortene, samt at det ble samlet inn kopi av store mengder identitetsdokumenter. Sistnevnte kunne ifølge tilsynet kompromittere innehaver. På for eksempel bankkort er det informasjon om fødselsnummer, bankkonto, kredittkortnummer, utløpsdato og CCV2 kode.

Departementet valgte å foreslå justeringer i regelverket i stedet for å komme tilsynets bekymringer i møte. Datatilsynet gjentok sine bekymringer i høringsprosessen knyttet til forslaget til endringer i forskriften om id-kort for bygge- og anleggsbransjen. Forskriften er foreløpig ikke satt i kraft.

### **5.5.6 Telefonopptak i finanssektoren**

Datatilsynet har fått tallrike henvendelser i forbindelse med endring av regler om plikt til å foreta lydopptak i finanssektoren. Reglene gjelder all kommunikasjon i forbindelse med ytelse av investeringstjenester, og medfører en utstrakt plikt til opptak og lagring av telefonsamtaler, bruk av e-post, SMS, Bloomberg, Reuters Messenger og ulike andre chatte-kanaler på Internett. Endringene medfører utfordringer knyttet til personvernet til ansatte i de institusjonene som omfattes av forskriftens virkeområde, kunder av disse foretakene, samt tredjepersoner.

Datatilsynet var kritisk i høringsrunden, og etter at forslaget ble vedtatt har man sett et behov for avklaringer knyttet til blant annet omfanget av lagringsplikten. Tilsynet har fremhevet at personopplysningsloven stiller krav om at opplysninger som behandles skal være relevante for formålet med behandlingen, og at disse ikke lagres lenger enn det som er nødvendig for å oppnå formålet.

På bakgrunn av de mange henvendelsene har Datatilsynet sett et klart behov for en klargjøring av hvordan regelverket skal forstås, med særlig fokus på hvordan ivaretagelsen av personvernet til både ansatte, kunder og tredjepersoner skal sikres. Etter å ha hørt Finanstilsynet, Finansdepartementet og sentrale bransjeorganisasjoner har Datatilsynet utarbeidet en veileder som er tilgjengelig på tilsynets hjemmesider.

Ikrafttredelse av forskriftsendringene ventes 1. april 2011.



### **5.5.7 Tilsyn – kameraovervåking i arbeidslivet**

LOs sommerpatrulje har hatt kontakt med Datatilsynet, og sommeren 2010 ble noen av tipsene fra sommerpatruljen fulgt opp gjennom uanmeldte tilsyn. Fokuset på tilsynene var de ansattes personvern i forbindelse med kameraovervåking. De tre stedene som ble kontrollert var alle innenfor matserveringsbransjen.

Alle tilsynene avdekket kameraovervåking som gikk ut over hva regelverket tillater. På samtlige steder ble områder der de ansatte tilberedte maten overvåket. Dette anser Datatilsynet som et for stort inngrep i de ansattes personvern på jobb, og som en overvåking uten en tilstrekkelig sterk begrunnelse. Så fremt det ikke er nødvendig for ivaretagelse av liv eller helse, må arbeid med produksjon kunne skje uten overvåking. Det være seg på restaurantkjøkken eller ved et samleband i en fabrikk.

Kameraovervåking på arbeidsplassen har vært et sentralt tema også ved andre tilsyn i 2010. Under en uanmeldt tipskontroll fant Datatilsynet skjult kameraovervåking på et kontor. Kameraet var laget som en røykdetektor. Det var ingen varslingskilter der og de ansatte var heller ikke blitt informert på annet vis. De hadde derfor ingen grunn til å tro at rommet var overvåket. Opptak fra dette kameraet hadde skjedd over flere år. Datatilsynet anså den skjulte overvåkingen som et overtramp mot de ansattes personvern og som et tydelig og grovt brudd på regelverket.

### **5.5.8 Overføring av personlister til USA for terrorscreening**

Datatilsynet har jobbet med to saker som omhandler overføring av personopplysninger til utlandet/sammenkobling av data, med det formål å screene disse mot ulike svartelister/terrorlister. Dette for å hindre at et selskap inngår kontrakter eller foretar transaksjoner med gitte personer.

I den ene saken gjaldt det et norskregistrert utenlandsk foretak som var underlagt amerikansk lovgivning. Denne lovgivningen har forbud mot å inngå forretningsforbindelser, transaksjoner og lignende med såkalte "restricted /denied parties". På daværende tidspunkt ble ansatte, søkere til stillinger, avtaleparter, kunder og konsulenter sjekket opp mot rundt 40 lister utstedt i USA og flere andre land. Spørsmålet i saken dreide seg om adgangen til å påbegynne tilsvarende screening for disse gruppene i Norge.

Datatilsynet kom til at behandlingen av personopplysninger ville være av en slik karakter at det må oppstilles strenge krav til behandlingsgrunnlaget. Etter en konkret vurdering falt tilsynet ned på at det ikke forelå dekkende behandlingsgrunnlag. Saken er av stor prinsipiell betydning. Selv om tilsynet tilkjennega at selskapet har en berettiget interesse, ble det særlig lagt vekt på at man vanskelig kan kontrollere kvaliteten av de ulike listene personopplysningene skal sjekkes opp mot, samt rettssikkerheten til partene som berøres.

Saken er påklaget til Personvernemnda, som snarlig ventes å ferdigstille saken.

## **5.6 IDRETT**

### **5.6.1 Tilsyn – antidopingkontroller på treningsentre**

Datatilsynet har gjennomført tilsyn med seks treningsentre hvor tema var antidopingprogrammet til Antidoping Norge. Hensikten med tilsynene var å belyse hvordan dette arbeidet ble praktisert på det enkelte treningscenter. Virksomheten er konsesjonspliktig, og medlemmene må aktivt gi sitt samtykke på forhånd før det kan tas dopingprøve av vedkommende. Det er treningsentrene som er behandlingsansvarlig, og således er pliktsubjekt for Datatilsynets tilsyn, mens det er Antidoping Norge som legger til rette for antidopingarbeidet og fysisk utfører dopingtestene på det enkelte treningscenter.

Det ble konstatert at treningsentrene syntes det var problematisk å innhente et aktivt samtykke fra det enkelte medlem for å kunne ta en dopingprøve. Flere av treningsentrene påpekte at samtykke til å ta dopingprøve måtte være en del av avtalen medlemmet inngikk med treningscenteret for at ordningen skulle fungere. Dette har forbrukermyndighetene tidligere ikke godtatt, og etter personopplysningsloven er heller ikke en slik avtale et tilstrekkelig grunnlag for å behandle sensitive personopplysninger.

Enkelte av treningsentrene hadde også innlemmet sine ansatte i antidopingprogrammet. Fra tilsynets side ble det påpekt at arbeidsmiljølovens bestemmelser om kontrolltiltak overfor ansatte setter klare grenser for denne type tester, og at dette heller ikke var tillatt etter gjeldende konsesjonsvilkår.

Datatilsynet påpekte dessuten det urimelige i at et eventuelt positivt testresultat også skulle rapporteres inn til Norges Idrettsforbund så framtidig medlemmet også var medlem av en idrettsklubb under paraplyen til forbundet. Særlig syntes Datatilsynet dette ville være problematisk overfor såkalte støttemedlemmer, eller medlemmer som ikke driver som aktiv idrettsutøver.

Flere av treningsentrene oppbevarte treningshistorikk langt utover den perioden hvor dette ville være relevant. Lagringsperioden strakk seg fra to til syv år. Datatilsynet anbefalte at lagring av treningshistorikk ikke strakte seg utover to år.

Tilsynene resulterte i et samarbeid mellom Antidoping Norge og Datatilsynet for å se på alternative måter for anvendelse av antidopingprogrammet på treningsentre, og et samarbeid med Treningsforbundet for å komme fram til faste sletterutiner av treningshistorikk.

## **5.7 KAMERAOVERVÅKING**

Det har de siste årene vært en sterk økning i omfanget av kameraovervåking. Som følge av at overvåkingsteknologien er blitt rimeligere og lett tilgjengelig, tar stadig nye grupper kameraovervåking i bruk, gjerne til formål som ligger langt utenfor tungtveiende sikkerhetsformål. Tilsyn i sektoren viser at kameraovervåkingen brukes til andre formål enn det som er nedfelt, og at det benyttes av beleilighetsgrunner der andre, og mindre personverninngripende tiltak kunne ha vært benyttet.

### **5.7.1 Tilsyn – kjøpesentre**

Datatilsynet foretok i meldingsåret tilsyn ved tre store kjøpesentre i henholdsvis Oslo, Trondheim og Moss.

Datatilsynet har inntrykk av at de fleste kjøpesentre har kameraovervåking. Formålet med overvåkingen er et ønske om å forhindre og/ eller oppklare tyveri, innbrudd og hærverk.

Datatilsynets kontroller viste at overvåkingskameraene i ulik grad er integrert i det totale sikkerhetssystemet til kjøpesenteret. I et av kjøpesentrene var kameraovervåkingen direkte knyttet til alarmsystemet i butikkene. Ved de andre kjøpesentrene benyttet man dataene kun i etterkant av en tyveri- eller hærverksepisode.

Mange kunder tilbringer lang tid i kjøpesentrene uten å være klar over at det blir lagret bilder av hvordan de beveger og oppfører seg. Selv om Datatilsynets tilsyn viste at varslingen til kundene er blitt bedre, er det fortsatt et utbredt problem at varslingen har mangler eller er fraværende. Sentrene er stort sett klar over at de skal melde kameraovervåkingen til Datatilsynet, men dette blir ikke alltid fulgt opp ovenfor leietakerne i senteret. Leietakerne har et selvstendig ansvar for å melde sin egen kameraovervåking til Datatilsynet.

Tilsynene avdekket videre at kameraovervåkingen i enkelte tilfeller blir benyttet til andre formål enn det som er nedfelt. Eksempel på slik bruk er når sentrene benytter kameraene til å finne igjen personer som har feilparkert bilen. Slik bruk kan være innenfor regelverket hvis det er tydelig nedfelt og blir informert om.

### **5.7.2 Tilsyn – bruk av kameraovervåking ved parkeringskontroll**

Datatilsynet mottok i 2010 en rekke klager på et parkeringsbyrås bruk av kameraovervåking for parkeringskontroll og ileggelse av parkeringsbøter. Datatilsynet foretok med dette som bakgrunn et tilsyn hos virksomheten for å ta stilling til hvorvidt bruken av kameraovervåkingen falt innenfor personopplysningslovens bestemmelser.

I stedet for å benytte personell, har dette parkeringsbyrået valgt å utføre parkeringskontrollen ved å gjennomgå overvåkingsopptak for å identifisere feilparkeringer. Ved feilparkeringer ble bilde tatt ut fra overvåkingsopptakene og sendt sammen med parkeringsbot til bilens registrerte eier. For parkeringsbyrået var dette en enkel og kostnadseffektiv måte å ilegge kontrollgebyrer på. Ved at parkeringsboten sendes i ettertid per post, unngås også eventuelle diskusjoner mellom parkeringsvakten og den som blir ilagt gebyr.

Det ligger en klar personverninteresse i at det ikke samles inn unødvendige personopplysninger for å løse en oppgave, og at det velges metoder som griper minst mulig inn i den enkeltes personvern. Etter Datatilsynets vurdering medfører bruk av kameraovervåking betydelig større personvernulempet enn en tradisjonell kontroll, som representerer en mer rettet innsamling av personopplysninger og kun medfører lagring av opplysninger om feilparkeringene. Kameraovervåkingen fører på sin side til en masseinnsamling av personopplysninger om bevegelser i området rent generelt. Ved at

gebyret først kommer i ettertid, mister også bilføreren muligheten til å samle informasjon på stedet der og da for en eventuell klage.

Datatilsynet mener at dette kontrolltiltaket både kan og bør gjennomføres med mindre personverninnngripende virkemidler, og at bruk av kameraovervåking som metode for parkeringskontroll mangler et rettslig grunnlag. Det ble derfor gjort vedtak om at bruken av kameraovervåking for parkeringskontroll og ilegging av parkeringsbøter måtte opphøre.

### **5.7.3 Tilsyn – Akershus universitetssykehus**

På nyåret 2010 mottok Datatilsynet en henvendelse fra de tillitsvalgte og hovedvernombudet ved Akershus universitetssykehus der det ble stilt spørsmål ved lovligheten av den utstrakte bruken av overvåkingskameraer i sykehusets lokaler. Saken fremsto som kompleks, og på bakgrunn av de mottatte opplysningene ble det besluttet å gjennomføre et tilsyn ved sykehuset. Det ble lagt særlig vekt på at pasienter ved et sykehus ofte befinner seg i en sårbar situasjon, og at de ansatte opplevde at hele deres arbeidsdag ble fanget opp av kameraer.

Under tilsynet fikk Datatilsynet bekreftet at omfanget av kameraovervåking var betydelig, med over 200 installerte kameraer. Det kom frem at overvåkingskameraer ble benyttet til en rekke ulike formål og at det i liten grad var foretatt kritiske vurderinger av tiltakene i forkant.

Tilsynet resulterte i en rekke pålegg. Blant annet måtte overvåkingen av korridorer, heiser og andre fellesområder i all hovedsak avvikles.

Etter Datatilsynets vurdering er saken av prinsipiell betydning fordi det ble slått fast at brukere av sykehus har krav på et særlig vern mot at deres integritet og privatliv krenkes. Pasienter og deres pårørende bør av åpenbare grunner skånes mot at oppholdet på sykehuset blir underlagt overvåking, selv om hensiktene bak kameraene er aldri så gode.

## **5.8 SAMFERDSEL**

Datatilsynet har gjennom flere årsmeldinger påpekt tendensen til at de anonyme alternativene er under press. Dette er fortsatt en aktuell problemstilling, men Datatilsynet har notert seg enkelte positive utviklingstrekk i 2010 som går i retning av å styrke personvernet innen enkelte deler av sektoren.

For det første er det positivt at kollektivtransportbransjen har tatt initiativ til å utvikle en bransjenorm for mer personvernvennlige løsninger ved bruk av elektroniske billetteringssystemer. Datatilsynet er videre positive til det nye ITS-direktivet vedtatt av EU, som gir tydelige signaler om at det ved bruk av ITS skal tas tilstrekkelig hensyn til personvernet. Endelig ser tilsynet positivt på en studie utført av Statens vegvesen som skisserer en løsning der brukeren kan inngå en avtale med AutoPASS som gjør det mulig å foreta bomplasseringer anonymt.

Det er imidlertid fremdeles nok av utfordringer å ta tak i innenfor samferdselsektoren. I meldingsåret vil vi nevne utfordringene knytte til det europeiske Ecall-prosjektet spesielt.

### **5.8.1 Bransjenorm for betalingssystemer i kollektivtransporten**

I 2009 gjennomførte Datatilsynet flere tilsyn overfor kollektivtransportbransjen i forbindelse med bruk av nye elektroniske billetteringssystemer. I forbindelse med tilsynene fant Datatilsynet flere brudd på personopplysningsloven. De mest alvorlige funnene dreide som at det ble foretatt en betydelig innsamling av personopplysninger fra de reisende, samtidig som det ikke var rutiner for sletting av disse opplysningene. Datatilsynet fastslo etter tilsynene at kollektivtransportvirksomheter som benytter elektronisk billettering, ikke i nødvendig grad har tatt hensyn til personopplysningsloven ved utarbeidelse av systemene.

De vedtak som Datatilsynet utarbeidet etter kontrollene ble påklaget av tilsynsobjektene. Dermed gikk sakene til endelig behandling hos Personvernemnda.

Etter Datatilsynets kontroll med bruken av de nye elektroniske billetteringssystemene, tok Ruter initiativ til et møte med tilsynet for å avklare situasjonen. Ruter mente at det ville være formålstjenlig å utvikle en felles bransjenorm, hvor bransjen i samarbeid med Datatilsynet kunne fastsette mer personvernvennlige løsninger for bruk av de elektroniske billetteringssystemene.

Involverte parter i dette arbeidet er fylkeskommunene og deres respektive kollektivtransportselskap, Kollektivtransportforeningen, Interoperabilitetstjenester AS, Ruter, NSB, Vegdirektoratet, Samferdselsdepartementet og Datatilsynet. Mobiliseringsarbeidet startet høsten 2010 og Samferdselsdepartementet har stilt krav om at arbeidet med bransjenormen skal være ferdigstilt innen juni 2011.

I påvente av bransjenormen for elektronisk billettering har Rogaland kollektivtrafikk bedt Personvernemnda om at behandlingen av klagesaken i nemnda blir stilt i bero.

### **5.8.2 Samarbeid med Statens vegvesen**

Stortinget har i behandlingen av St.meld. nr. 17 (2006-2007) "Eit informasjonssamfunn for alle" lagt til grunn at det fremdeles skal gis tilbud om anonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg. Stortinget ønsker at det tilrettelegges for anonyme løsninger ved betaling i helautomatiske bomstasjoner slik at brukerne får mulighet til å ferdes anonymt også i fremtiden.

I de tradisjonelle bomstasjonene vil en bruker kunne være anonym ved å betale kontant til en betjent eller i en myntautomat. I de helautomatiske bomstasjonene er slik betaling ikke lenger mulig ettersom innkrevingen er basert enten på passering med AutoPASS-brikke, eller ved etterskuddsvis fakturering basert på opplysninger om kjøretøyets registreringsnummer (samlet inn i bomstasjonen) og kjøretøyets eier (samlet inn fra kjøretøyregisteret). Den siste betalingsmåten benyttes dersom AutoPASS-brikken ikke er lest eller kjøretøyet ikke har installert en AutoPASS-brikke. Det er i dag imidlertid mulig for brukere som inngår AutoPASS- avtale å velge at detaljerte passeringdata slettes etter at de er belastet avtalen. Da lagres i stedet bare aggregerte data som ikke forteller hvor og når passeringene fant sted.

Statens vegvesen har gjennomført en mulighetsstudie for å se på muligheter for anonym betaling i automatiske AutoPASS-anlegg. Mulighetsstudiet har kommet frem til en løsning der brukeren inngår en AutoPASS-avtale uten å registrere kundeopplysninger. Passeringsopplysningene kan således ikke kobles til person, og så lenge brukeren følger de betingelsene som er gitt i avtalen vil brukeren være anonym.

### **5.8.3 ITS-direktivet**

Europaparlamentet og Europarådet vedtok 7. juli 2010 et nytt EØS-relevant direktiv angående rammene for innføring av intelligente transportsystemer og tjenester (ITS) på veitransportområdet og for grenseområdene til andre transportformer (ITS-direktivet). ITS er en felles betegnelse på bruk av informasjons- og kommunikasjonsteknologi (IKT) i transportsektoren.

Datatilsynet ser det som positivt at personvernet er viet plass i ITS-direktivet som enda ikke er implementert i Norge. Artikkel 10 i direktivet er tilegnet regler for personvern, sikkerhet og gjenbruk av personopplysninger. Det blir slått fast at rettigheter og direktiver som omhandler personvern skal følges. Underpunktene i artikkelen presiserer ytterligere hva som er viktig å følge opp for å ivareta personvernet innen ITS.

Datatilsynet vil også bemerke at det er lagt viktige føringer i flere av punktene i grunnlagsteksten for direktivet. Viktigheten av å begrense formålet med innsamlingen av personopplysninger samt viktigheten av dataminimalisering presiseres. Viktigheten av anonymisering som et av prinsippene for å bedre individets personvern fremheves også. Datatilsynet er tilfreds med at kommisjonen skal konsultere den europeiske datatilsynsmannen og be om uttalelse fra Artikkel 29-gruppen der ITS-løsninger omfatter personopplysninger og sikkerhet for disse.

Det er uvisst om og/eller når direktivet blir innført i Norge. Ut fra et personvernståsted er det nyttig at det overfor ITS-aktørene blir presisert hvor viktig personvern er. Datatilsynet har sett at flere store satsninger i samferdselssektoren det siste tiåret har manglet ivaretagelse av personvernet. Dette gjelder for eksempel innen elektronisk billettering og elektronisk veifinansiering.

### **5.8.4 eCall**

eCall (emergency Call) er et felleseuropeisk prosjekt under EU-kommisjonen, som har til formål å forbedre mulighetene for hurtig hjelp etter trafikkulykker. I korthet innebærer dette at personbiler som typegodkjennes i fremtiden forutsettes å ha utstyr installert som ringer det felleseuropeiske nødnummeret 112 i situasjoner hvor det forventes å være behov for bistand fra nødetatene (brann/politi/helse). I forbindelse med oppringningen vil det oversendes data om kjøretøyet, for eksempel dets posisjon. Innføringen av eCall vil kunne få negative konsekvenser for personvernet dersom det ikke på forhånd legges til rette for å unngå disse.

eCall er i seg selv, dersom det blir implementert med kun nødvendig konfigurasjon, håndterbart med tanke på personvernet. Det forutsettes da at det er mulig å skru av systemet

når det skulle være ønskelig. Det er et klart dokumentert ønske fra datatilsynsmyndighetene i Europa at systemet er samtykkebasert ved at det kan skrues av. Når systemet er aktivert vil det kunne kommunisere, ikke bare ved hjelp av tekst, men også ved tale ettersom mikrofon og høyttaler i bilkupeen skal åpne for kommunikasjon med nødnummer 112.

Det er et sterkt ønske fra bilindustrien og forsikringsselskapene som deltar i standardiseringsarbeidet om å åpne for at nødkommunikasjonen ikke går direkte fra bilens eCall til 112, men via en tredjepartstjeneste. Denne skal kunne sette videre over til 112 med medlytt. Datatilsynet har vært motstander av en slik løsning, siden slik kommunikasjon er å anse som fortrolig og krever beskyttelse. Bilfabrikanter, forsikringsselskaper og andre kan ha økonomiske eller andre grunner til å foreta medlytt på en nødsamtale.

Datatilsynet har notert at eCall-systemet, med GPS og GSM-kommunikasjon, har trukket til seg flere interessepartnere som ser dette som en grunnkommunikasjonsenhet for et betydelig mer omfattende system. Når først eCall er etablert, vil man også kunne legge på en rekke andre tjenester, som opplysninger om værforhold, kø og så videre til multimediekommunikasjon i bilen. Det gis stadig indikasjoner på at industrien benytter et pålagt eCall-system som en mulighet for kommersielle tjenester. Det er derfor viktig for Datatilsynet at ordningen er samtykkebasert.

## **5.9 VELFERD, FORSKING OG HELSE**

Helsesektoren er i dag preget av høy grad av endringsvilje og evne – fra departement til institusjonsnivå. Særlig aktuelt i meldingsåret har vært modernisering av helseregisterområdet. Flere viktige høringer har vært til behandling i tilsynet. Datatilsynet hadde i 2010 fokus på den sentrale forvaltningen av helseopplysninger og foretok flere tilsyn i sektoren.

### **5.9.1 Tilsyn – Folkehelseinstituttet**

Datatilsynet gjennomførte en serie tilsyn ved Nasjonalt Folkehelseinstitutt (FHI) i 2010. Tilsynene omfattet FHI generelt, Tvillingregisteret, Den norske Mor og Barn-undersøkelsen, og helseforskning etter helseforskningsloven. Tilsynene var en naturlig del av Datatilsynets fokus på helseforskning og sentral forvaltning av helseopplysninger.

Med inntreden av helseforskningsloven i 2009 var Datatilsynet interessert i å se hvordan praksis etter ny lov virket, om vilkår stilt av Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK) ivaretas, og hvordan grensen mellom helseregisterloven og helseforskningsloven håndheves i praksis. Ved innføringen av helseforskningsloven er forhåndskontrollen av prosjekter som faller inn under denne loven, flyttet til REK. Datatilsynet skal imidlertid føre tilsyn med at loven følges.

FHI er en sentral aktør når det gjelder helseforskning og helseforvaltning. Datatilsynet og FHI har i flere tilfeller hatt ulike synspunkter rundt helseforskning og registerforvaltning. Datatilsynet opplever imidlertid at samarbeidet med instituttet er konstruktivt, og at instituttet ivaretar sine oppgaver på en tilfredsstillende måte.

Tilsynene viste at Folkehelseinstituttet har kommet langt når det gjelder internkontroll, og at det er etablert en støttefunksjon for igangsetting av forskningsprosjekter. Samtlige prosjekter går gjennom støttefunksjonen før de oversendes for godkjenning hos REK. Avvik ble imidlertid konstatert knyttet til kontroll med oppbevaring av helseopplysninger, forståelse av regelverkets definisjoner av anonyme og aidentifiserte helseopplysninger, og ivaretagelse av informasjonsplikten.

Tilsynet påpekte at instituttet må styrke sine vurderinger av om det foreligger en informasjonsplikt til de registrerte for forskningsprosjekter som ikke er basert på samtykke. Datatilsynet har grunn til å tro at problemstillingen som ble påpekt også har relevans i forhold til andre forskningsinstitutter og vil derfor følge dette opp videre.

I tilknytning til godkjenninger gitt av REK noterte Datatilsynet seg at REK kan ha gitt tillatelser til prosjekter som faller utenfor helseforskningsloven. Hvis denne observasjonen er korrekt, vil en slik tillatelse i så fall ligge utenfor REKs kompetanseområde. Datatilsynet er imidlertid usikker på hva som fremstår som korrekt formell håndtering av slike situasjoner.

Datatilsynet har oversendt funnene til godkjennings- og myndighetsaktørene innen helseforskningsområdet som grunnlag for videre vurderinger. Avklaring av regelverkets virkeområde og REKs kompetanse berører forhold utenfor Folkehelseinstituttets kontroll. Likevel vil det kunne ha konsekvenser for instituttet da det berører det rettslige grunnlaget for instituttets forskningsprosjekter.

Med bakgrunn i funnene og avklaringene vil Datatilsynet ha videre dialog med REK og Den nasjonale forskningsetiske komité for medisin og helsefag (NEM). Tilsynet ser det som viktig at slike problemstillinger bringes opp tidlig mens praksis etter helseforskningsloven formes. I annen dialog med REK har det også kommet frem at det er behov for at Datatilsynet bidrar med veiledning. Dette gjelder særlig med hensyn til informasjonssikkerhet, både til REK og til plikthaverne etter helseforskningsloven.

### **5.9.2 Tilsyn – Kreftregisteret**

I oktober 2009 gjennomførte Datatilsynet et tilsyn hos Kreftregisteret. I den foreløpige rapporten konkluderes det med at Kreftregisteret mangler samtykke fra de undersøkte med negative funn vedrørende livmorhalskreft. Forskriften som regulerer dette stiller krav til Kreftregisteret om at de skal hente inn samtykke fra den registrerte hvor det ikke er funnet kreft eller forstadier til kreft. Kreftregisteret kan ha data fra alle undersøkelser, også negative funn, men ikke over tid uten at de har spurt først.

Datatilsynet fattet vedtak i 2010 om at det må hentes inn samtykke fra de registrerte for å beholde og bruke de lagrede opplysninger – opplysninger om ca 1,6 millioner kvinner.

Kreftregisteret har klaget på Datatilsynets vedtak. Tilsynet er ved årets slutt i dialog med Kreftregisteret, for å finne en ordning hvor de registrertes personvern ivaretas uten at opplysningene slettes.



### **5.9.3 Tilsyn – Norsk pasientskadeerstatning**

Datatilsynet gjennomførte tilsyn ved Norsk pasientskadeerstatning (NPE) våren 2010. Statistikken deres viser at erstatningskrav etter skade i forbindelse med helsebehandling øker. Økningen i antall saker som meldes inn til NPE fører naturlig med seg at mengden personopplysninger som behandles av NPE også har tiltatt i omfang. Temaet for tilsynene var å få oppdatert kunnskap om denne delen av forvaltningen og analysere hvordan pasientenes personvern ivaretas.

Det er ikke utarbeidet endelig kontrollrapport for tilsynet hos NPE i meldingsåret. Datatilsynet har imidlertid utarbeidet en foreløpig kontrollrapport. Der har det blitt konstatert flere avvik både på krav til internkontroll og informasjonssikkerhet.

NPE har i tilsvar kommet med flere innvendinger til Datatilsynets foreløpige vurderinger. Dette gjelder blant annet Datatilsynets vurdering av at samtykkeerklæringen NPE bruker for innhenting av opplysninger om pasienter ikke anses tilfredsstillende i henhold til kravene til et gyldig samtykke.

### **5.9.4 Tilsyn - helseregistre**

Datatilsynet gjennomførte tilsyn hos Forsvarsdepartementet, Folkehelseinstituttet, Krefregistret og Helsedirektoratet. Disse er ansvarlige for de i alt åtte sentrale helseregistrene hvor det er et krav om intern kryptering av identifiserende opplysninger. Tilsynene var en naturlig oppfølging av den offentlige debatten rundt etableringen av et nasjonalt hjerte- og karregister. I debatten fremgikk at de allerede etablerte sentrale helseregistrene hadde kommet kort i implementeringen av kravet om intern kryptering av identitet.

Datatilsynet vurderte det slik at kravet om intern kryptering var ivaretatt i kun to av de åtte registrene; Norsk pasientregister og Norsk vaksinasjonsregister. Fremdriftsplanene som ble fremlagt indikerte en tidshorisont for implementering på to til tre år. Det forutsetter blant annet overgang fra papirbaserte meldinger til elektroniske meldinger.

En spesiell problemstilling reiste seg da Helse- og omsorgsdepartementet sendte ut en tolkning av hvordan kravet om intern kryptering av identitet skulle forstås mens kontrollene pågikk. Datatilsynet tolkning av regelverket divergerte fra departementets tolkning. Tilsynet mente at egen tolkning lå tettere opp til de forventningene Stortinget hadde da kravet ble innført.

Stortingets kontroll- og konstitusjonskomité opprettet en kontrollsak om implementeringen, og Datatilsynet deltok i en kontrollhøring. I Stortingets behandling av innstillingen fra Kontroll- og konstitusjonskomiteen orienterte helse- og omsorgsministeren om at lovforståelsen vil fremlegges for Stortinget.

Det bemerkes at Datatilsynet og departementet ikke synes å ha ulikt syn på hvordan registrene i fremtiden skal utformes, men om hvordan kravet i regelverket skal forstås.

Saken om intern kryptering må også ses i sammenheng med det offentlige ordskiftet rundt strategien for modernisering av Helseregisterområdet (Gode Helseregistre – Bedre helse) og stortingsbehandlingen av det nye sentrale helseregisteret for hjerte- og karlidelser.

### **5.9.5 Tilsyn – NTNU**

Datatilsynet gjennomførte tilsyn ved NTNU i september 2009. Tilsynet avdekket at pasientjournaler for mer enn 116 000 pasienter var stilt til disposisjon for deler av forskningsmiljøet på Norsk senter for elektroniske pasientjournaler ved NTNU. Tilsynet avdekket en rekke kritikkverdige forhold i nevnte sak. Blant annet ble det reist kraftig kritikk for det tilsynet mente var ulovlig erverv av elektroniske pasientjournaler, mangelfull informasjon til berørte pasienter, manglende rettslig grunnlag, mangelfull sikring av helseopplysninger, manglende tillatelser og mangelfull internkontroll.

Datatilsynet påla NTNU en informasjonsplikt ovenfor berørte pasienter, en styrking av sitt internkontrollsystem og tilhørende avvikssystem. Dette for å unngå at lignende tilfeller oppstår i fremtiden.

Tilsynet mener at opplysningene har tilflytt NTNU gjennom brudd på helsepersonells taushetsplikt, og oversendte derfor saken til Helsetilsynet.

Helsetilsynet fant at lovbruddene var så graverende at helsepersonellet ble politianmeldt for brudd på taushetsplikten. Saken var ikke ferdig behandlet fra politiets side ved utgangen av 2010.

### **5.9.6 Avslag på søknad om konsesjon for forskningsprosjekt i regi av NOVA**

Datatilsynet ga delvis avslag på søknad om konsesjon i forbindelse med Norsk institutt for forskning om oppvekst, velferd og aldring (NOVA) sitt forskningsprosjekt ”Nordisk omfangs undersøkelse - Ung i Norden 2009”. Prosjektet var tilrådd av Nasjonal forskningsetisk komité for humanoria og samfunnsfag (NESH).

Datatilsynet vurderte for det første at barn fra 14-15 år ikke har selvstendig samtykkekompetanse for å delta i et forskningsprosjekt av denne art. Konsesjonen ble derfor gitt under forutsetning av at det ble innhentet samtykke fra barnas foreldre.

Vurderingen av barnas samtykkekompetanse berodde på en konkret vurdering. Datatilsynet la blant annet vekt på at undersøkelsen innebærer en omfattende og detaljert kartlegging av det enkelte barns liv. Det skal registreres over hundre spørsmål av svært inngående og sensitiv karakter. Videre la Datatilsynet vekt på tidligere praksis som har vært at barn fra 14- 15 år ikke har selvstendig samtykkekompetanse for deltakelse i slike typer forskningsprosjekter.

Datatilsynet har i sin vurdering også funnet det naturlig å se hen på myndighetsalderen for deltakelse i helseforskningsprosjekter. Dette fordi forskning på helseopplysninger etter helseforskningsloven og denne type forskning på sensitive personopplysninger kan være nokså likartede. Myndighetsalderen etter helseforskningsloven er 16 år. Et tilsvarende helseforskningsprosjekt måtte derfor vært basert på samtykke fra barnas foreldre. Det påpekes

at helseforskningsloven har åpnet opp for at departementet i forskrift kan gjøre et begrenset unntak fra myndighetsalderen på 16 år for spesielle typer forskningsprosjekter.

Odelstingsdebatten viser at unntaket var omdiskutert. Departementet har på nåværende tidspunkt ikke gitt en slik forskrift.

Datatilsynet vurderte også informasjonssikkerheten til ikke å være tilfredsstillende ivaretatt ved gjennomføring av prosjektet. Konklusjonen ble derfor at opplysningene ikke kunne innhentes på omsøkt måte.

Saken er klaget inn for Personvernemnda. Nemndas avgjørelse i saken vil kunne få prinsipiell betydning for vurdering av barns samtykkekompetanse.

### **5.9.7 Høring – tilgang på tvers**

Datatilsynet ga høsten 2010 sin uttalelse til forskriftsforslaget om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.

Forskriften skal blant annet fastsette kravene som må oppfylles for at virksomheter skal kunne få tilgang til helseopplysninger i hverandres journalssystemer. Adgangen for slik tilgang ble gitt ved endring av helseregisterloven i 2009.

Tilsynet var positive til at det i forskriften var implementert en rekke av Stortingets forutsetninger for tilgang på tvers ved lovendringen i 2009. Det ble imidlertid understreket at det er behov for nærmere klargjøringer av hvordan man skal sikre at det etableres systemer som faktisk gjør det mulig å oppfylle regelverkets krav. Herunder å ivareta forutsetningen om at det bare er nødvendige, relevante og strukturerte opplysninger det gis tilgang til. Lovforarbeidene har også oppstilt klare krav til strukturering av pasientjournaler.

Datatilsynet ser det som hensiktsmessig at systemkrav for tilgang og strukturingskrav til journalene presiseres nærmere for å sikre at reglene etterleveres i praksis. Presiseringene kan for eksempel gis i form av rundskriv.

Videre mener Datatilsynet at tilgang til helseopplysninger mellom virksomheter bør ses i sammenheng med arbeidet omkring nasjonal- og regional kjernejournal. Tilsynet ser behovet for bedre samhandlingsløsninger og er positive til en samtykkebasert kjernejournal. Denne kan både ivareta behovet for tilfredsstillende informasjonsdeling og samtidig sikre pasientens rett til selvbestemmelse.

Datatilsynet ser på det som viktig og ønskelig å få bistå i det videre arbeidet med kravene til systemer for tilgang på tvers og arbeidet med kjernejournal.

Forskriften løser ikke problemstillingen i primærhelsetjenesten med formaliserte kontorfellesskap mellom ulike virksomheter. Datatilsynet har her over lang tid påpekt en ubalanse i sektorens alminnelige organisering, hvor for eksempel et legekantor som består av flere enkeltpersonforetak må forholde seg til et regelverk som ikke har tillatt tilgang på tvers. Etter tilsynets forståelse har departementet startet en forskriftsprosess på dette området.

### **5.9.8 Høring – strategi for Norsk Helsenett**

Statsforetaket Norsk Helsenett sendte i 2010 sin strategi på høring. Etter den første høringsrunden ble en revidert versjon av strategien sendt på ny høring.

Datatilsynet pekte i sine høringsuttalelser på den sentrale rollen Norsk Helsenett har med å legge til rette for sikker kommunikasjon og etterlevelse av Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren. Her er det viktig at Norsk Helsenett i sin strategi legger til rette for dette, og selv forplikter seg til å etterleve normen. Videre har Datatilsynet pekt på behovet for at Norsk Helsenett i strategien ser på hvordan de skal håndtere sine ulike roller som nettverksleverandør, databehandler og eventuelt databehandlingsansvarlig.

Norsk Helsenett har gjennom utkastene til strategien uttrykt et mål om å ta rollen som en nasjonal enhet for forvaltning av helseregistre. Datatilsynet er i utgangspunktet negativ til at én aktør skal gis en slik sentral rolle. Dette henger sammen med at en så stor samling av sensitive personopplysninger vil kunne øke risikoen utover hva tekniske tiltak alene kan kompensere.

### **5.9.9 Høring – Drap i Norge**

Helse- og omsorgsdepartementet sendte i meldingsåret NOU 2010:3 ”Drap i Norge i perioden 2004-2009” på høring. Datatilsynet ga utvalget honnør for grundig arbeid, men poengterte at enkelte av forslagene reiser personvernmessige utfordringer. Dette gjaldt blant annet forslaget om å vurdere endringer av aktuelle bestemmelser i helsepersonelloven og politiloven vedrørende taushetsplikt, samt forslaget om etablering av permanent ordning for forskning på drap.

Utvalget anbefaler at det gjennomføres systematiske studier på hvordan taushetspliktbestemmelsene faktisk praktiseres mellom samarbeidende etater. Det er uvisst om det er regelverket eller andre forhold som forhindrer nødvendig informasjonsutveksling og samarbeid mellom etater. Datatilsynet støtter et slikt utredningsarbeid.

Utvalget foreslår også etablering av en permanent forskningsbasert ordning for gjennomgang av samtlige drap i Norge. Datatilsynet forstår behovet for å øke kunnskapen om drap i Norge, men savner en nærmere konkretisering av hva utvalget har ment med en permanent forskningsbasert ordning. Det er en rekke avklaringer av personvernmessig og forskningsetisk karakter som må gjøres i forkant av slik forskning. Særlig kravet til samtykke, informasjonsplikt, graden av personidentifikasjon og sletting er viktig å nevne i denne sammenhengen.

### **5.9.10 NAV**

NAV er en storforbruker av personopplysninger, og Datatilsynet mottar mange henvendelser vedrørende NAV.

Datatilsynet har blant annet mottatt flere henvendelser som gjelder ønske om innsyn i logg i NAVs systemer. Dette for å avdekke eventuell ”snoking”. I de sakene som tilsynet har

behandlet har tilsynet konkludert med at de registrerte ikke har rett til innsyn i NAVs logger, men at hensynene bak tilsvarende rett etter helselovgivningen i noe grad er ivaretatt gjennom NAVs interne saksbehandling i disse sakene. Retten til innsyn i hva NAV har av opplysninger om den enkelte er i behold.

Det har også kommet henvendelser vedrørende NAVs brudd på personvernregelverket i forbindelse med at personopplysninger har kommet på avveie, at de har blitt sendt til feil mottakere, og andre brudd på personvernlovgivningen. Tilsynet har i flere saker veiledet NAV-brukere om muligheten til å kreve erstatning, også for ikke-økonomisk tap, som følge av brudd på regelverket.

Et vedtak gjort av Datatilsynet om informasjonsplikt ved NAVs innhenting av pasientjournaler i forbindelse med etterkontroll, ble klaget inn for Personvernemnda. Nemnda kom til samme resultat som Datatilsynet; at det foreligger informasjonsplikt ved innhenting av pasientjournaler i kontrolløyemed.

Datatilsynet gjennomførte høsten 2010 et tilsyn med Arbeids- og velferdsdirektoratet (NAV-direktorat) med fokus på tilgangsstyring og logging i de statlige fagapplikasjonene generelt. Videre ble en del av tilsynet gjennomført ved kontaktsenteret i Bodø. I sammenheng med tilsynene hentet Datatilsynet inn informasjon fra seks NAV-kontor om hvor mange som hadde tilgang til de ulike fagapplikasjonene.

Ved innføringen av NAV-reformen ble det lagt som et premiss at personvernet skulle ivaretas når de tidligere uavhengige tjenesten ble slått sammen, blant annet gjennom modernisering av IT-løsninger.

Datatilsynet fant at NAV ikke har oppnådd denne sentrale forutsetningen i reformen. Flere fagsystemer hadde mangler i loggfunksjonalitet. NAV var generelt ute av stand til å avdekke uautorisert lesing fordi loggene ikke ble benyttet eller ikke var tilgjengelige. Dette fremstår som svært uheldig, også siden reformen medfører at svært mange får tilgang til personopplysninger som angår et stort antall personer.

Videre hadde Datatilsynet kommentarer til organiseringen av sikkerhetsarbeidet i NAV, og til NAVs internkontroll.

### **5.9.11 Velferdsteknologi**

Datatilsynet mottar en økende mengde henvendelser vedrørende såkalt velferdsteknologi. Også media har i 2010 hatt fokus på 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 medisinerer eller automatisk tilkalling ved akutt hjelp. Helsetjenesten kan slik gi bedre og mer målrettet omsorg

til de som trenger det mest. I forhold til personvernet kan imidlertid teknologien innebære en betydelig økning i registrering av personopplysninger.

Datatilsynet ser utfordringer i forhold til personopplysningslovens 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 hvis de motsetter seg dette. Dersom det ikke kan innhentes samtykke til bruk av teknologien, må det foreligge annet behandlingsgrunnlag.

Hovedutfordringen på dette området er imidlertid hjemmelsproblematikken når det gjelder bruk av slike tiltak i helsetjenesten, og slik hjemmel må søkes i helselovgivningen.

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

Datatilsynet har også i 2010 deltatt i en referansegruppe nedsatt av Helsedirektoratet. Gruppen har til formål å utarbeide en veileder for bruk av sporingsteknologi overfor demente og andre med kognitiv svikt.

## **5.10 FINANS OG FORSIKRING**

Datatilsynet har i 2010 hatt fokus på nye konsesjoner innen finanssektoren. Ny konsesjon til banksektoren ble ferdigstilt etter samarbeid med bransjen. Videre ble arbeidet med ny konsesjon for kredittopplysningsvirksomhetene tatt opp igjen. Arbeidet med nye konsesjoner innen sektoren vil fortsette i 2011.

### **5.10.1 Kredittopplysningsvirksomheten**

Datatilsynet fikk i 2010 en rekke henvendelser fra enkeltpersoner som enten ikke skjønner hvorfor de har blitt kredittvurdert, eller de er uenig i at vilkårene for slik vurdering er tilstede. I hovedsak går henvendelsene ut på at de mener kredittvurderingen er usaklig; de har ikke vært i kontakt med den som har bedt om kredittvurderingen eller de har ikke blitt informert om at det vil bli foretatt en slik vurdering som ledd i inngåelse av en avtale. Tilsynet har også mottatt henvendelser med påstander om at kredittvurderingen er foretatt i sjikanehensikt. Datatilsynet leser ut fra henvendelsene at økonomiske forhold oppfattes som følsomme og er beskyttelsesverdige, selv om slike opplysninger ikke er definert som sensitive i personopplysningslovens forstand.

I tillegg mottar Datatilsynet henvendelser fra personer som oppfatter at parametrene som benyttes i kredittvurderingen er usaklige. For eksempel kan alder, kjønn, bostedsadresse samt flyttehistorikk få negative utslag i kredittvurderingen. Slik bruk av opplysningene oppfattes som urettferdig for personer som aldri har misligholdt en betalingsfrist.

Datatilsynet utarbeidet i 2009 utkast til ny konsesjon til kredittopplysningsbyråene. Arbeidet med konsesjonen ble tatt opp igjen i 2010. Forholdene nevnt ovenfor vil stå sentralt i vurderingen av konsesjonen. I tillegg har Personvernemnda truffet enkelte avgjørelser som må nedfelles i den nye konsesjonen. Arbeidet med konsesjonen vil bli videreført i 2011.

### **5.10.2 Tilsyn – BBS og eFaktura**

Datatilsynet var i 2010 på tilsyn hos daværende Bankenes Betalingsentral AS (BBS) – nå Nets Norway AS – og en større bank for å kontrollere bankenes behandling av personopplysninger, særlig i forbindelse med eFaktura. eFaktura er en fellestjeneste som gjør at nettbankkunder kan betale sine regninger elektronisk. Tjenesten er tilgjengelig for alle norske banker.

Kundene inngår en avtale med banken om å benytte eFaktura fra en virksomhet (for eksempel sin strømleverandør). Etter inngåelse av avtalen er eFakturaen tilgjengelig i alle nettbanker hvor kunden har relasjoner, og fakturaen kan derfor betales i hvilken som helst av disse bankene. Problemet er at andre banker ikke vil være juridisk ansvarlig overfor kunden ved behandling av personopplysninger i eFakturasystemet. Skjer det en uautorisert utlevering av personopplysninger vil ansvarsforholdet og straffeansvaret etter personopplysningsloven være svært vanskelig å avklare bankene i mellom.

Behandling av personopplysninger for eFaktura involverer flere parter, herunder ulike eFakturautstedere, ulike eFakturahotell, Nets Norway og bankene. I hovedsak var forholdet mellom partene regulert i standardavtaler, men forholdet til personopplysningsloven var ikke eksplisitt omtalt.

Etter Datatilsynets vurdering vil Nets Norway være databehandler for den enkelte bank, men vil også ha eget ansvar for koblingsregisteret som gjør fakturaen tilgjengelig i andre banker. De ulike ansvarsforholdene må etter Datatilsynets vurdering avklares og nedfelles i avtalene mellom partene. I tillegg må informasjonen om eFaktura bedres overfor kundene.

### **5.10.3 Tilsyn – utlevering av personopplysninger til land utenfor EØS-sonen**

Datatilsynet fikk tidlig i 2009 varsel om at enkelte bankers IKT-oppgaver ble flyttet til lavkostland, land hvor personvernlovgivningen står svakt eller er ikke-eksisterende. Høsten 2009 foretok Datatilsynet kontroll med en sparebank (behandlingsansvarlig) og EDB Business Partner ASA (databehandler) i forbindelse med håndtering av personopplysninger innen banksektoren. EDB Business Partner ASA hadde utplassert noe av håndteringen av bankens personopplysninger til land utenfor EØS-sonen.

Et av hovedspørsmålene under tilsynet var om det faktisk ble behandlet personopplysninger i Ukraina, og videre hvorvidt den eventuelle behandlingen ble omfattet av personopplysningslovens bestemmelser om overføring til utlandet.

Tilsynet ble avsluttet i forbindelse med at ny databehandleravtale ble etablert og Datatilsynet viste til Finanstilsynets rundskriv av 31. mai 2010 om utflytting av bankenes IKT-oppgaver.

Finanstilsynet er av den oppfatning at utkontrahering av sentrale driftsrelaterte IKT-oppgaver til land med høy risiko innebærer en kritisk risiko for driftsstabiliteten i norske banker og i betalingssystemene. Finanstilsynet nevner for eksempel at kundeopplysninger er blant de funksjonsområder hvor risikoen blir for stor og at slike IKT-oppgaver ikke kan utkontrakteres til landområder med høy risiko. Datatilsynet støtter Finanstilsynets vurdering.

## **5.11 PERSONVERN I KOMMUNESEKTOREN**

Kommuneprosjektet startet opp i februar 2009. Bakgrunnen for prosjektet var at kommunene behandler store mengder personopplysninger om innbyggere og ansatte. Mange av opplysningene som behandles er sensitive og krever vurdering av nødvendige sikkerhetstiltak.

Gjennom flere år har resultater fra Datatilsynets kontroller vist at mange kommuner ikke har tilfredsstillende rutiner for behandling av personopplysninger. I 2003 fikk over halvparten av 31 undersøkte kommuner påvist mangler. Gjennom prosjektet ville Datatilsynet igjen fokusere på kommunenes etterlevelse av personopplysningsloven.

### **5.11.1 Tilsyn med kommuner**

Gjennom prosjektet har Datatilsynet til sammen gjennomført 11 tilsyn med kommuner med tema internkontroll, informasjonssikkerhet og ledelsesforankring i henhold til kravene i personopplysningsloven med forskrift. Følgende fylker har hatt tilsyn i 2009-2010: Vestfold, Rogaland, Oppland og Akershus.

Det ble påvist avvik fra regelverkets krav hos samtlige kontrollerte kommuner. Flertallet av kommunene manglet et tilstrekkelig dokumentert system for internkontroll og informasjonssikkerhet. Videre hadde flere kommuner mangelfulle rutiner for publisering på Internett og mangelfull oversikt over hvilke personopplysninger som ble behandlet i kommunen.

### **5.11.2 Dagsseminarer og oppdatert veileder**

I samarbeid med KINS (Kommunal Informasjonssikkerhet) og NorSIS (Norsk senter for informasjonssikring) ble det i prosjektperioden gjennomført en rekke gratis dagsseminarer om internkontroll og informasjonssikkerhet i byene Bergen, Trondheim, Stavanger, Drammen, Tromsø, Kristiansand, Hamar, Ålesund, Bodø, Kristiansund og Moss.

Rådmenn og andre fra ledelsen, samt sikkerhetsansvarlige og ansatte med ansvar og interesse for internkontroll og informasjonssikkerhet i kommunen, ble oppfordret til å delta.

Seminarene vektla formidling av praktiske tips til hvordan kommunene bør jobbe med internkontroll og informasjonssikkerhet for å lykkes. Målet var at kommunene skulle sitte igjen med konkrete og praktiske råd til hvordan regelverket skal etterleves. Dette ble gjort ved å representere funn fra kontroller i kommunene samt å orientere om hva et tilsyn innebærer. I tillegg har representanter for enkelte kommuner fortalt om sine erfaringer og utfordringer fra arbeidet med internkontroll og informasjonssikkerhet og bidratt med råd om iverksettelse og



løsninger knyttet til temaet. Våren 2010 var det mer en 300 påmeldte til syv gjennomførte seminarer. Høsten 2010 var det 96 påmeldte til de fire resterende seminarene.

I løpet av prosjektperioden er dessuten Datatilsynets veileder i internkontroll og informasjonssikkerhet fra 2007 blitt oppdatert, redesignet og trykket på nytt. Veilederen er utarbeidet for å hjelpe blant annet kommuner og fylkeskommuner med å komme i gang med arbeidet med å få på plass et dokumentert system for internkontroll.

### **5.11.3 Kartlegging av status for arbeid med personvern**

Prosjektet har i løpet av sommeren og høsten 2010 gjennomført en kartlegging av hvor langt kommunene og fylkeskommunene har kommet i arbeidet med å implementere et system for internkontroll og informasjonssikkerhet. Kartleggingen ble gjennomført etter at alle kommuner hadde mottatt veilederen med følgebrev og tilbud om å delta på Datatilsynets gratis seminar om temaet. Etter til sammen tre purrerunder har 429 av 449 kommuner og fylkeskommuner svart på redegjørelsen.

Det umiddelbare resultatet viser at nesten halvparten av alle kommuner og fylkeskommuner oppgir at de ikke har et dokumentert system for internkontroll og informasjonssikkerhet slik loven krever.

Datatilsynet vil i 2011 foreta en nærmere analyse av materialet og vurdere en fortsatt oppfølging av kommunesektoren.

## **5.12 PERSONVERNOMBUD**

Ved utgangen av meldingsåret har Datatilsynet registrert 173 personvernombud som til sammen representerer over 350 virksomheter innenfor ulike bransjer over hele landet. Dette utgjør 20 prosent økning i antall ombud fra 2009.

Som følge av bevilgninger fra FAD i forbindelse med prosjektet ”Internkontroll, informasjonssikkerhet og personvernombud” ble personvernombudsordningen styrket med en prosjektleder i full stilling. Samlede ressurser knyttet til ordningen har i 2010 vært i overkant av to årsverk.

Fokus har vært å styrke ordningen generelt, gjennom utvikling av veiledningsmateriell, økt kurstilbud, og utarbeiding av en langsiktig strategi for ordningen. Formålet har vært å etablere virkemidler som vil styrke bevisstheten omkring internkontroll, informasjonssikkerhet og personvernspørsmål i norske virksomheter, for dermed å bedre regelverksetterlevelsen.

Som del av utviklingsarbeidet er det gjennomført evaluering av ordningen; først gjennom en spørreundersøkelse rettet mot alle ombudsvirksomhetene på vårparten, dernest gjennom en nærstudie av utvalgte virksomheters ombudspraksis. Resultatene vil danne bakgrunn for vurdering av eksisterende tiltak og eventuelle behov for oppfølging, samt vurdering av ombudsordningens effekt.

Høsten 2010 ble det avsatt en øremerket pott til nettverkstiltak for personvernombudene. Midlene var tilgjengelig for ombudene gjennom åpen søknad. To aktører, som til sammen representerer 25 kommuner i henholdsvis Østfold og Nordland fikk innvilget tilskudd.

Datatilsynet arrangerte i løpet av året seks kurs for ombudene; grunnkurs, informasjonssikkerhet I og II, samt juridisk påbygningskurs. I mai ble Datatilsynets årlige ombudskonferanse avholdt. Konferansen besto av en fellesdel med interne og eksterne forelesere, etterfulgt av bransjeinndelte parallellsesjoner for bank/finans, kommune/utdanning og helse, samt en sesjon med bransjeuavhengige tema. For statlig sektor ble det i juni arrangert et eget seminar om personvern- og sikkerhetsutfordringer i offentlig sektor.

I regi av ombudsordningen ble det avholdt personverndag i forbindelse med Sikkerhets- og sårbarhetskonferansen i Trondheim i mai, og et samarbeidsseminar med Difi og Sintef i Kristiansand i oktober om aktuelle sikkerhets- og personvernutfordringer for norske virksomheter.

Ombudsordningen har også blitt promotert gjennom deltagelse og foredrag på andre relevante arenaer.

Etter føringer fra FAD vil personvernombudsordningen utgå fra prosjektsatsingen, og vil fra 2011 bli lagt under ordinært driftsbudsjett. De bevilgede prosjektmidlene vil videreføres i prosjektet ”Internkontroll og informasjonssikkerhet”.



***Datatilsynet***

*Gateadresse: Tollbugata 3, Oslo*

*Postadresse: postboks 8177 Dep, 0034 Oslo*

*E-post: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no)*

*Telefon: 22 39 69 00 - Faks: 22 42 23 50*