

# Årsmeldingen for 2012

Manus til stortingsmeldingen om Datatilsynets virksomhet, jf. personopplysningsloven § 42.  
Oversendt Fornyings-, administrasjons- og kirkedepartementet, februar 2013.



## Forord

Året 2012 var et godt år for Datatilsynet. I 2011 la vi grunnlaget for vårt strategiske arbeid for flere år fremover ved å lansere en ny overordnet strategi og en egen strategi for helseområdet. I meldingsåret har vi fortsatt arbeidet med å utarbeide strategier for både justissektoren og vårt internasjonale engasjement, og vi har rettet større oppmerksomhet mot hvordan vi gjennomfører vårt tilsynsarbeid og saksbehandlingen. Debatten rundt personvern har også vært god.

I 2012 har vi økt antallet tilsyn med 20 prosent, vi har fått bedre struktur på behandlingen av enkeltsaker og vi har profesjonalisert veiledningsarbeidet ytterligere. Vi ser også at det strategiske arbeidet fra 2011 gir resultater. Det er enklere å prioritere riktig med en god strategi som bunnplanke.

Teddy Roosevelt sa en gang: *“Speak softly and carry a big stick, and we will go far.”* Dette sitatet kjennertegner vår måte å jobbe på. Vi opplever at omverdenen ser på Datatilsynet som en attraktiv, strategisk samarbeidspartner. Samtidig viser vår forvaltningspraksis at vi bruker strenge sanksjoner når det er riktig, og vi legger stor vekt på å utøve ombudsrollen vår. Kritikken av flere av Justisdepartementets forslag til lovendringer har vært hard og berettiget, og vi har påpekt at vi ikke må miste hodet etter de tragiske hendelsene 22. juli 2011. Det har også vært viktig å kommunisere utad at Datatilsynet ønsker å spille på lag med og ligge i forkant av den teknologiske utviklingen. Og vi beskyldes sjeldnere og sjeldnere for å ha skyld i at pasientjournaler fortsatt kjøres i taxi, eller sendes med telefaks.

En viktig strategisk satsing er å sette den enkelte borger i stand til å ivareta sitt eget personvern og gjøre de som registrerer og bruker personopplysninger så gode at folk ikke trenger å klage til oss. Våre nye nettsider ble lansert i januar 2012. De er bygd opp nettopp med dette for øye; selvhjelp og god informasjon til borgere og behandlingsansvarlige. Vi legger stor vekt på vårt veiledningsarbeid, men mener samtidig at nettsidene i mange tilfeller er en vel så god kilde til informasjon. Det er derfor positivt at vi ser en nedgang i antall henvendelser på telefon og e-post, og vi tolker dette som et signal på at vårt digitale førstevalg virker.

På tampen av 2012 la regjeringen fram en stortingsmelding om personvern. Den gir en god gjennomgang av personverntilstanden i ulike sektorer, og det er vårt håp at den vil lede til en bred debatt om personvernets kår i dagens samfunn. Dette er påkrevet. Den største trusselen mot personvernet er de mange små inngrep, registreringer og overvåkingstiltak som til sist kan ende med at vi mister den friheten vi setter så høyt; frihet til å reise hvor vi vil, til å bruke penger på hva vi vil og til å kommunisere med hvem vi vil, uten frykt for at noen ser oss i kortene.

Bjørn Erik Thon  
Direktør

## Innhold

1. Datatilsynet i en teknologisk tid .....	4
2. Tema.....	7
Et sporbart arbeidsliv.....	7
Kunsten ikke å miste hodet etter 22. juli .....	11
3. Nærmere om utvalgte områder.....	13
Internett og telekommunikasjon.....	13
Helse og velferd .....	18
Justissektoren.....	24
Offentlig sektor.....	28
Internasjonalt samarbeid.....	31
4. Om Datatilsynet - organisasjon og ressursbruk.....	36
Tilsynsverksemnda .....	36
Juridisk saksbehandling .....	39
Personvernombod .....	47
Deltagelse i offentlige råd og utvalg .....	48
Kommunikasjonsvirksomheten .....	50
Budsjett, organisasjon og administrasjon .....	56
5. Vedlegg.....	58
Vedlegg A. Gjennomførte tilsyn .....	58
Vedlegg B. Høringer .....	60
Vedlegg C. Saker oversendt til Personvernemnda .....	64

## 1. Datatilsynet i en teknologisk tid

*At dagens teknologiutvikling går i rasende fart er ingen overdrivelse. Vi konsumerer og bruker data i et voldsomt tempo. Hele 90 prosent av dagens digitale data er generert bare i løpet av de to siste årene og datamengden er antatt å øke med 40 prosent per år framover. I løpet av det minuttet det har tatt å bla seg fram til denne artikkelen og lese det som er skrevet til nå er det lastet ned 47 000 apper, lagt ut 30 timer video på YouTube, sendt 204 millioner e-poster og gjort to millioner søk på Google.*

Denne utviklingen treffer i aller høyeste grad Datatilsynet. Det pågår knapt en politisk diskusjon uten at det har en side til personvernet. Bompenger, elektroniske billetter, GPS i arbeidslivet, helsejournaler og helseregistre, sosiale medier, søkemotorer, terrortrusler, digitalisering av offentlig sektor, kameraovervåking og betalingskort; alt har en personvernmessig konsekvens.

### Om Datatilsynet

Personvern er et begrep med mange nyanser og ulike forståelser. Det finnes derfor ikke én presis og god definisjon på hva personvern er, men enkelt sagt handler personvern om retten til et privatliv og retten til å bestemme over egne personopplysninger. Personvern er ikke bare en viktig menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet og privatliv. Personvern er også viktig for å sikre felles goder i et demokratisk samfunn. Et dårlig ivaretatt personvern vil sette demokratiet i fare ved at borgerne begrenser sin deltakelse i åpen meningsutveksling og politisk aktivitet. Den enkelte kan frykte at opplysninger om personlige forhold kan bli trukket frem og gjort til allmenn oppmerksomhet. Man kan også sette begrensninger på seg selv, fordi man frykter at myndighetene registrerer og lagrer opplysninger om ens ferdsel, interesser, uttrykk for holdninger eller kommunikasjon med andre.

Datatilsynets rolle er å passe på at personvernet ivaretas. Vi skal ivareta enkeltpersoner som mener at deres personvern er krenket, og vi skal passe på at de som har plikter etter personopplysningsloven følger disse.

Datatilsynet manøvrerer i et krevende landskap. Tilsynet består av drøye førti kloke hoder som er veldig bevisste på at vi sammen, og ved å jobbe riktig, kan få til mye godt personvern for norske borgere, samt sørge for at regelverket etterleves bedre enn i dag. Med begrensede ressurser er det imidlertid viktig at Datatilsynet har en god strategi for sitt arbeid. Vi har grovt sett fire virkemidler til disposisjon; behandling av enkeltsaker, kontroller/tilsyn, veiledning av publikum og de som behandler personopplysninger, samt informasjon og bruk av ombudsrollen for å skape debatt og påpeke utfordringer for personvernet. Det er viktig å bruke de ulike virkemidlene riktig. På enkelte områder er utstrakt tilsynsvirksomhet sentralt, på andre områder er veiledning det viktigste, mens det på atter andre områder er viktig å drive informasjonsarbeid.

### Prioriterte områder

Datatilsynet må være veldig tydelig på hva som prioriteres. I meldingsåret har følgende områder vært høyest prioritert: Justissektoren, arbeidsliv, økonomi og finans, helse og omsorg, Internett og sosiale medier, samt samferdsel. Grunnen til dette er ganske enkelt at vi ut fra en risikovurdering fant at det

er i disse sektorene personvernet er under størst press. Det er de samme prioriteringene som i 2011, og etter vår vurdering har det vært viktig å beholde de samme områdene over minst to år. Samtidig har prioriteringer en negativ side. Viktige områder som for eksempel skole- og utdanningssektoren, registrering av personopplysninger ved bruk av fordelskort og personvern i idretten har for eksempel ikke vært prioritert i 2012.

Datatilsynet har i meldingsåret jobbet for å få opp antallet gjennomførte tilsyn. 2011 var preget av utredningsarbeid og ny strategi, og det var nødvendig å prioritere dette på bekostning av antall tilsyn. I 2012 har antallet derimot økt igjen. Vi er imidlertid mer opptatt av å gjennomføre de *riktige* tilsynene i de riktige sektorene framfor et visst antall tilsyn. Litt forenklet sagt kan Datatilsynet lett gjennomføre 50 tilsyn på en uke dersom vi ville se nærmere på merkingen av kameraovervåking i de største byene våre, men dette er neppe den beste måten å bruke ressursene på. Et riktig gjennomført tilsyn gir positive ringvirkninger i bransjen og gir bedre regeletterlevelse totalt.

### Internasjonalt arbeid

Internasjonalt arbeid er viktig for tilsynet. I januar 2012 la EU-kommisjonen fram et forslag til ny personvernforordning som, når den blir vedtatt, blir til norsk lov. En av hovedhensiktene med forslaget er at håndhevingen av regelverket på tvers av de enkelte nasjonene skal bli bedre. For å lede og koordinere dette arbeidet foreslås det opprettet et eget organ, European Data Protection Board. Det er fortsatt uklart om Norge får en plass i dette organet, og vi har forsøkt å gjøre det politiske miljøet og forvaltningen oppmerksom på hvor viktig det er å jobbe for at Datatilsynet blir med. Den nordiske kanalen er viktig i dette arbeidet. Men mest av alt er det viktig at politikere på alle nivåer og i alle partier bruker sitt internasjonale nettverk for å gi Datatilsynet en plass rundt det bordet hvor beslutninger tas.

### Mest kompetente på personvern

Vi i Datatilsynet må til enhver tid sørge for å ha god nok kompetanse til å matche kompetansen hos næringsdrivende, offentlige etater og andre vi fører tilsyn med. En av våre målsetninger er å være Norges mest kompetente fagmiljø på personvern. Andre virksomheters kompetanse på personvern blir stadig bedre, og de fleste store bedrifter, organisasjoner og offentlige etater har i dag ansatt personvernekspert. Dette ser vi først og fremst på som en fordel fordi det er lettere å skape forståelse hos folk med kompetanse på området.

Vi har også som målsetning å gjøre andre gode personvern. I dette ligger en enkel realitet, nemlig at førti mennesker alene ikke klarer å gjøre jobben med å sørge for at lovverket etterlevs. Manglende etterlevelse av lovverket skyldes oftere mangel på kunnskap enn manglende vilje, og bedre kunnskap hos eksterne parter fører til bedre etterlevelse av regelverket. En viktig del av denne satsingen er å ha proaktiv kontakt med eksterne aktører. Vi gjennomfører årlig en rekke kontaktmøter og dialogmøter for å fremme personverntanken, lære av andre og finne sammen i godt samarbeid.

Ikke minst er det viktig å ha god kontakt med forsknings- og utviklingsmiljøene. For to år siden pekte vi ut dette som en strategisk satsing, og det har gitt resultater. Vi har bygd ut kontaktnettet med sentrale forsknings- og utdanningsinstitusjoner, vi har vært veiledere på studentoppgaver og vi ser at interessen for å skrive om personvern både på master- og doktornivå er økende.

Men, kompetanse har også en side til det vi startet dette kapitlet med, nemlig teknologi. Datatilsynets ansatte må være godt skolert på teknologi. Vi må fange opp teknologitrender tidlig og ha tett dialog med de sentrale teknologidriverne nasjonalt og ikke minst internasjonalt. Teknologi går inn i alt vi gjør, innen alle sektorer. Her må Datatilsynet ligge i forkant. Og vi må sørge for at teknologien tas i bruk for å fremme personvernet. I denne sammenhengen blir innebygd personvern viktig. Ved å bygge personvernet inn i de teknologiske løsningene fra starten av, oppstår det en vinn-vinn-situasjon for alle parter; brukerne får personvernavennlige løsninger, mens virksomhetene slipper kostnadene ved å måtte bake inn gode løsninger i etterkant.

## 2. Tema

### Et sporbart arbeidsliv

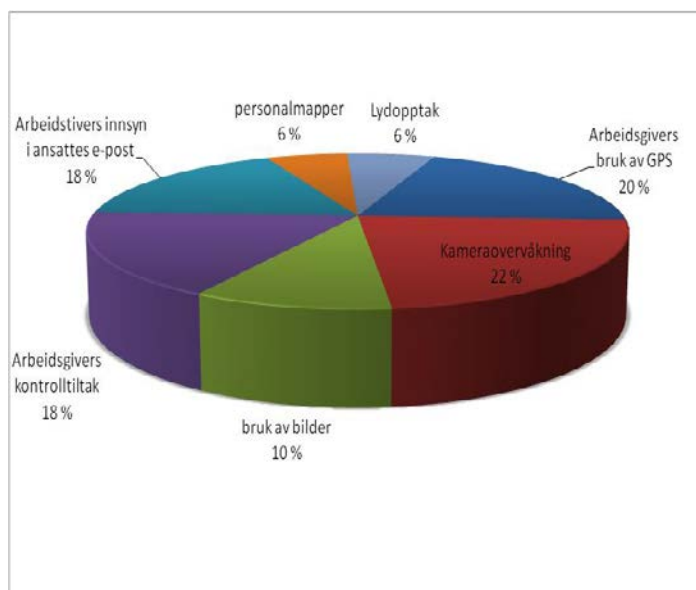
*Fra du kommer på jobb til du går for dagen legger du igjen spor. Du fanges opp av overvåkingskameraer utenfor jobben, du drar adgangskortet for å komme inn hoveddøra eller for å bevege deg innad i bygget, du stempler deg inn i timeregistreringssystemet, det loggføres hva du gjør i saksbehandlersystemet og du drar kantinekortet når du kjøper lunsj. Det registreres opplysninger om hvor du er, hvem du har ringt, hvem du har skrevet e-post til og hva som blir skrevet. Listen er lang.*

Datatilsynet erfarer en økning i bruk av personopplysninger i arbeidslivet. Opplysningene registreres til mange ulike formål, og bruksområdet utvides. Registreringen kan begrunnes i behovet for å planlegge arbeidet, effektivisering, ressursfordeling, ulike krav til dokumentasjon, samt hensynet til helse, sikkerhet og miljø. I praksis er det ofte slik at ett og samme sett av opplysninger er velegnet for flere formål. Hensikten med kameraovervåking kan for eksempel være å trygge sikkerheten til de ansatte. Opplysninger fra det samme kameraet kan imidlertid også benyttes av arbeidsgiveren for å kontrollere om noen av de ansatte tar for lange pauser eller gjør noe annet som arbeidsgiveren finner grunn til å holde et årvåkent øye med.

Økningen i omfanget av registreringer henger også sammen med utviklingen og bruken av ny teknologi som har endret organiseringen av arbeidet og arbeidsoppgavene. Ny informasjonsteknologi har lagt til rette for en mer fleksibel arbeidshverdag og mer selvstendige og autonome arbeidstakere. Samtidig medfører innføringen av systemer med en økt detaljregistrering at det er forholdsvis enkelt å systematisere, sammenstille og analysere opplysninger om arbeidstakerne. Utviklingen har slik åpnet for teknologi som muliggjør overvåking og kontroll av ansatte i et helt annet omfang enn tidligere. Eksempler på slik teknologi er smarttelefoner, håndholdte datamaskiner (PDA-er), geografiske sporingssystemer (GPS) og ulike digitale prestasjonsmålingsverktøy.

#### *Mange henvendelser fra publikum*

Spørsmål relatert til arbeidsliv utgjør den største andelen av publikumshenvendelsene til Datatilsynet. I 2012 utgjorde arbeidslivsspørsmål 15 prosent av den totale mengden e-posthenvendelser til tilsynet. Henvendelsene var hovedsaklig konsentrert omkring bruk av kameraovervåking, GPS, lydopptak, kontrolltiltak og bilder, innsyn i e-post og personalmapper.



### Arbeidshverdagens elektroniske spor

I 2012 utarbeidet Datatilsynet rapporten "*En vanlig dag på jobb – arbeidshverdagens elektroniske spor*". Hensikten med rapporten har vært å illustrere hvordan registreringstrykket i deler av yrkeslivet ser ut, samt å gi økt kunnskap om og skape bevissthet rundt hvordan personopplysninger om arbeidstakere samles inn og benyttes generelt i Norge i dag. I rapporten så vi nærmere på arbeidshverdagen til tre ulike yrkesgrupper; bussjåfører, hjemmesykepleiere og saksbehandlere. Vi gjennomførte intervjuer med representanter for ledelsen og de ansatte (som også var tillitsvalgte) ved to arbeidsplasser innenfor hver av de tre valgte yrkesgruppene.

Målet med undersøkelsen var å få en mest mulig *fullstendig* oversikt over *alle typer spor* som den ansatte legger igjen i løpet av en vanlig arbeidsdag. Eksempler på slike spor kan være lokasjonsdata om hvor en ansatt har vært, logger etter bruk av adgangskort eller opptak fra kameraovervåkingen.

Med utgangspunkt i beskrivelsen av seks vanlige arbeidsdager er det noen observasjoner som peker seg ut. Vi ønsker å trekke frem enkelte av disse.

### Vanskelig å holde oversikt

Intervjuene viste klart at det er vanskelig for de ansatte å holde oversikt over hvilke personopplysninger som behandles om dem. En mulig grunn til dette er at det ofte er et betydelig antall ulike systemer som registrerer opplysninger. Et annet viktig moment er at det for mange av systemene slett ikke er opplagt *hva* som registreres eller *om* det registreres noe i det hele tatt. Et eksempel på dette er når man drar adgangskortet eller surfer på Internett. Loggingen av denne typen elektroniske spor er ikke noe den ansatte selv kan se. Det kan da være vanskelig å få oversikt over *hvilke opplysninger* som registreres *til hvilke formål*, og *hvem* som har tilgang til opplysningene.

Usikkerheten i intervjuene kan tyde på at de ansatte ikke har fått god nok informasjon om systemene. Det stilles krav i både arbeidsmiljøloven og personopplysningsloven om at arbeidstakerne skal ha dekkende informasjon om hvilke personopplysninger som behandles, og hva de skal brukes til. For å kunne være sikre på hva som skjer, er de ansatte avhengige av dekkende informasjon og tillit til arbeidsgiveren.

Det kan være krevende for både arbeidsgiveren og arbeidstakeren å gi, samt få, fullgod informasjon. Mengden opplysninger gjør dette spesielt utfordrende. Retten til informasjon er imidlertid avgjørende for at den enkelte skal kunne gjøres i stand til å ivareta egne rettigheter etter loven. Dette gjør seg særlig gjeldende når det er lite intuitivt hva som faktisk skjer i de ulike prosessene som etterlater elektroniske spor.

I tillegg til at det er vanskelig å ha oversikt over hvilke opplysninger som lagres, er det også lite intuitivt *hvor lenge* opplysningene blir lagret. Intervjuene avdekket stor usikkerhet blant både tillitsvalgte og ledere knyttet til hvor lenge opplysningene faktisk blir lagret i de ulike systemene.

### En loggført arbeidsdag

I løpet av en arbeidsdag legger arbeidstakeren igjen en lang rekke spor. Sporene finnes i flere forskjellige systemer og de gir ulike former for informasjon. Inntrykket etter intervjuene er at en arbeidsdag i stor grad lar seg rekonstruere i ettertid. Hvor langt tilbake det er mulig å rekonstruere,



er mer usikkert. Noen elektroniske spor slettes etter kort tid, andre blir liggende lenge, og noen opplysninger er ikke tenkt slettet i det hele tatt.

Av de tre yrkesgruppene vi så nærmere på i forbindelse med rapporten, er det bussjåførene som legger igjen den største mengden elektroniske spor. Med innføring av sanntidssystem og kjøretøycomputere i bussen kan arbeidsgiveren følge med på om sjåførene følger oppsatte rutetider og om de kjører bussene på en forsvarlig og ønskelig måte. Rutebusselskapene opererer i et anbudsmarked hvor marginene for å vinne neste anbudsrunde er små. Flåtestyring er påkrevd for å delta i anbudskonkurranser om busstilbudet. Tidsplanene er til dels svært strikte og forsinkelser på ruta genererer bøter fra oppdragsgiveren til busselskapet. Bussjåførene mente systemet bidro til å gi en stressende arbeidshverdag. Samtidig så de også positive sider ved systemet. I forbindelse med klager fra for eksempel kunder kunne det oppleves som en trygghet at man kan benytte loggdata fra kjøretøycomputeren eller sanntidssystemet for å tilbakevise urettmessige klager. Sjåførene mente også at systemene kunne bidra til å dokumentere ovenfor arbeidsgiveren og oppdragsgiveren at de estimerte rutetidene ikke er mulige å overholde.

Bruk av flåtestyring har endret arbeidshverdagen i mange yrkesgrupper, ikke bare i transportbransjen, men også innenfor blant annet kommunal hjemmehjelp, logistikk, renhold og elektrotjenester. Arbeidstakere som før utførte sine arbeidsoppgaver relativt fritt "ute i felten", kan nå bli fulgt i detalj av arbeidsgiveren på lang avstand.

#### *Bruk av opplysningene til nye formål*

Manglende sletting og gjenbruk av opplysninger til nye formål, skaper utfordringer for personvernet. Datatilsynet har i et stort antall saker avdekket systematiske brudd på regelverkets krav om sletting. Opplysninger beholdes i mange tilfeller på ubestemt tid og slettes kun når praktiske hensyn tilsier det. Lagring av data har blitt billigere og billigere, noe som fører til at det ofte er dyrere og mer ressurskrevende for virksomheten å etablere tilfredsstillende sletterutiner, enn å lagre opplysningene videre.

Et grunnleggende prinsipp i personvernlovgivningen er at personopplysninger ikke skal lagres lenger enn nødvendig for å gjennomføre formålet med behandlingen. Når formålet er oppfylt skal opplysningene slettes. Ofte argumenteres det med at man ønsker å oppbevare opplysningene fordi de kan komme til nytte senere, uten at man nødvendigvis har klart for seg hva man senere skal benytte opplysningene til. Prinsippet om formålsbestemt bruk av personopplysninger stilles da på prøve. I tillegg til at manglende sletting som regel vil være et brudd på personopplysningsloven, øker det også faren for at opplysningene senere kan brukes til andre formål som er uforenlig med det opprinnelige.

#### *Viktig å bevare tillitt*

Et annet trekk ved dagens arbeidsliv er at det finnes store mengder opplysninger som er egnet til regelrett overvåking av de ansatte. Det kan komme nye muligheter for å sammenstille opplysninger, eller det kan oppstå konkrete situasjoner hvor arbeidsgiveren ønsker å gjennomgå det som er registrert om den ansatte. I tillegg viser det seg også at mange tiltak ikke begrunnes konkret, eventuelt har vage begrunnelser. Det blir derfor i liten grad forutsigbart hva opplysningene skal kunne brukes til. Det forekommer også at tiltak innføres med skjult begrunnelse.

Arbeidsgiveren trenger de ansattes aksept eller forståelse for systemer, rutiner og valg. Men, det er også viktig for de ansatte at de forutsetninger og begrensninger som finnes blir knyttet til formål og at den forespeilede bruken blir overholdt. Hvis de ansatte får negative erfaringer, brytes tilliten ned. Bruk av opplysninger til nye formål uten at de ansatte er involvert, eller anerkjenner behovet, kan føre til at tillitsforholdet bryter sammen.

Arbeidsgiveren kan med utgangspunkt i styringsretten bestemme hvordan arbeidet skal utføres og hvilke hjelpemidler som skal benyttes for å utføre arbeidsoppgavene, innenfor rammene av regelverket. Selv om mange av systemene ikke innføres for å føre kontroll med den enkelte, *muliggjør* systemene ofte en nitidig kontroll. Vi er derfor avhengige av tillitt mellom partene for at arbeidslivet skal fungere. Slik tillitt er betinget av at arbeidsgiveren informerer, men også av at arbeidstakerne tar seg umaken ved å sette seg inn i hvilke systemer som finnes på en arbeidsplass og hva de brukes til.

Det mest sentrale er likevel å komme bort fra den enkle forestillingen som har dominert store deler av arbeidslivet til nå; at informasjonsteknologien tillater et stadig friere arbeidsliv og at kontrollsystemene bare brukes til å forhindre uvedkommende på kontoret. Vi skal ikke male fanden på veggen og si at vi nærmer oss Orwells dystopi hvor storebror alltid ser deg, men vi er allerede farlig nær en situasjon hvor arbeidsgiveren stadig ser deg. Det bør gi grunn til en mer kritisk debatt – kanskje særlig nå som manglende trygghet og manglende sikkerhetssystemer får all oppmerksomhet. All sikkerhet er ikke bare til det gode, og sikkerhetshensyn må hele tiden avveies mot grunnleggende rettigheter.

## Kunsten ikke å miste hodet etter 22. juli

Etter 22. juli var det bred politisk enighet om at terror skulle bekjempes med mer åpenhet og mer demokrati. Dette var et godt signal for alle som er opptatt av personvern. En slik hendelse utløste allikevel, naturlig nok, en debatt om politiets fullmakter og endringer i straffeloven. Særlig politiet og deres foreninger har vært aktive på forslagsfronten. Det har blant annet blitt fremmet forslag om utvidelse av lagringsplikten i ekomloven (som implementerer datalagringsdirektivet) til også å gjelde internettkafeer, hoteller, biblioteker og andre områder med trådløse nett. Politiets sikkerhetstjeneste (PST) har krevd mer utveksling av informasjon fra offentlige etater til PST, samt en styrket plikt for helsepersonell til å melde fra til PST om mistenkelige personer.

Flere av forslagene har blitt fulgt opp politisk. Sommeren 2012 sendte regjeringen et forslag om ytterligere kriminalisering av solokriminalitet på høring. Forslaget var i det vesentlige bygd på et forslag fra PST. Datatilsynet og flere andre høringsinstanser uttalte seg kritisk til forslaget, og da særlig til at forslagene var for dårlig utredet. Det var heller ikke foretatt vurderinger av forslaget opp mot for eksempel Menneskerettighetskonvensjonens beskyttelse av privatlivets fred.

Datatilsynet fant også grunn til å minne om at det er et grunnleggende prinsipp i en demokratisk rettsstat at det er lovgiver som skal sette grenser for politiets inngrep overfor borgerne. Dette gjelder selv om politiet har de beste intensjoner og utfører en samfunnsnyttig oppgave. Det er uheldig når svært inngripende forslag baseres nokså ukritisk på politiets ønsker, slik forslaget om å kriminalisere forberedelse til soloterrorisme gjorde.

Inngrep i personvernet må alltid ha et rettslig grunnlag. På justisfeltet må det rettslige grunnlaget være hjemmel i lov. Det er svært viktig at Stortinget ikke overlater til den enkelte borger å måtte definere grenser for politiets virksomhet. Dette er grunnen til vi stiller oss kritiske til at straffelovens bestemmelser om frivillig DNA-testing anvendes overfor andre personer enn de som har en lovlig tilknytning til åstedet eller bevismaterialet. Såkalt DNA-screening er en stadig mer brukt metode ettersom kostnaden ved å ta DNA-prøver er redusert og at det med dagens teknologi er mulig for politiet å finne ut hvem som har vært i et område.

Med ikrafttredelsen av datalagringsdirektivet vil borgerne i enda større grad bli lokalisert, og det er grunn til å tro at denne etterforskningsmetoden vil bli enda mer brukt. Den tar imidlertid ikke høyde for at ikke alle har nødvendige forutsetninger for å kunne ivareta sine egne rettigheter når politiet henvender seg for å be om DNA-prøver. Det kan også stilles spørsmål ved om det i det hele tatt er mulig å hente inn et samtykke som er reelt frivillig i slike saker. De samme bekymringene gjør seg gjeldende i forbindelse med frivillige narkotikarazziaer mot skoleelever. I disse og lignende saker er det viktig at Stortinget tar en endelig beslutning på borgernes vegne.

Politiet, og særlig PST, underbygger sine ønsker om utvidede fullmakter med at det ellers er vanskelig å innfri samfunnets forventninger om at de skal beskytte oss mot terrorisme og annen alvorlig kriminalitet. Kanskje handler dette også om at Stortinget må justere egne og befolkningens forventninger til hvilken beskyttelse staten kan garantere, uten at det kommer i konflikt med et felles ønske om mer demokrati og mer åpenhet. Det er viktig å kommunisere at den absolutte trygghet ikke er mulig å oppnå innenfor et åpent, demokratisk samfunn som vårt. Tiltakene som innføres for å

etterkomme ønsket om trygghet kan faktisk føre til at tilliten til staten undergraves, og dermed forutsetningen for ivaretagelse av tryggheten.

Datatilsynet mener det er viktig at det stilles kritiske spørsmål når politiet ber om utvidede fullmakter og om at stadig mer av borgernes handlinger belegges med et potensielt straffeansvar. I en tid og i et land hvor verken teknologien eller ressursene setter faktiske grenser for hvilke tiltak som kan iverksettes overfor borgerne, må Stortinget basere grensesettingen på en konkret og prinsipiell avveining av ulike samfunnsinteresser. Det er viktig å etterspørre dokumentasjon på at inngripende tiltak faktisk er effektive, og at det identifiserer og tar på alvor de mothensyn som gjør seg gjeldende, *før* politiets fullmakter utvides på bekostning av borgernes frihet.

Debatten i kjølvannet av voldtektsbølgen i Oslo høsten 2011 er illustrerende. Mange tok til orde for at flere overvåkingskameraer var veien å gå. Datatilsynet var en ganske ensom stemme som advarte mot flere kameraer og vi stilte spørsmålsteget ved om effekten av tiltaket sto i forhold til det inngrepet dette var i borgernes personvern. Sentrale politikere pekte på København som en foregangsby. Nå skrinlegger danskene planen om flere kameraer. Politiinspektør Svend Foldager fra Københavns Politis Efterforskningsenhet sier at *"det er ekstremt omkostningstungt både at få data ind og opbevare dem, og så må vi koldt og kynisk se på udbyttet. Det har ikke nogen præventiv virkning. Vi kan bruge det til opklaring af tilfældige ting, og det er selvfølgelig godt, men det er ikke sådan, at videoovervågningen reelt gør en forskel"*.

Det er også viktig at personverninngripende tiltak evalueres slik tilfellet var med kameraovervåkingen i København. Det må føres en *løpende* debatt, også i Stortinget, om nivået på det totale overvåkingsnivået i samfunnet. Selv om hvert enkelt tiltak i seg selv ikke er inngripende er det grunn til å advare dersom totaliteten blir for stor. Dersom et inngrep for eksempel ikke har noen dokumenterbar effekt på kriminalitetsbekjempelsen må det oppheves.

Personvern handler om respekt for det enkelte individ, om klare lovhjemler og forutberegnelighet, om åpenhet, om grundige forhåndsvurderinger og om evaluering. Dersom Stortinget vedtar lover bygd på disse prinsippene, og politiet bygger sitt arbeid på de samme prinsippene, har vi alle sjanser til å lykkes i å bevare det tillitsbaserte samfunn. Da kan vi også klare kunsten ikke å miste hodet etter 22. juli.

### 3. Nærmere om utvalgte områder

#### Internett og telekommunikasjon

Internett har revolusjonert måten vi kommuniserer på. Fra å være et sted hvor man først og fremst mottok informasjon, har nettet utviklet seg til å bli et sted hvor man også aktivt deler og sprer informasjon. Denne utviklingen har utvilsomt hatt en økt demokratiserende effekt på samfunnet, men den har også gitt nye, store utfordringer. I sosiale nettsamfunn lagres det i dag personopplysninger i et voldsomt, og stadig økende, omfang. Våre bevegelser og søk på nett kan kartlegges og danne svært detaljerte mønstre om hvordan vi opptrer. Dette benyttes blant annet – ofte uten vår viten – til å skreddersy reklame. Personopplysninger er blitt en handelsvare med stor økonomisk verdi.

Vi ser også en økende grad av kobling mellom produkt og tjeneste. Dette synliggjøres for eksempel ved valg av smarttelefon, der enten Google, Apple eller Microsoft leverer operativsystemet. Kundene tvinges så mer eller mindre inn i leverandørens utvalg av tjenester og må godta deres personvernvilkår. Forskjellige løsninger komplementerer hverandre og skaper allianser der utvekslingen av personopplysninger blir vanskelig å holde styr på for forbrukeren. Smarttelefoner har blitt allemannseie, og antall programmer og applikasjoner som tilbys til smarttelefonene er stadig økende. Kompleksiteten fører til at et stort flertall av brukerne trolig vil basere seg på produsentens forhåndsinnstillinger. Dette er slett ikke alltid et godt valg for personvernet.

Markedet preges dessuten av noen få store aktører. Foruten å være en av verdens største søkemotorer, står for eksempel Google også bak populære tjenester som Gmail, Google Maps, Google Apps, Blogger, Chrome, Android, YouTube, Google Analytics og Google+. Dette gjør Google til en av verdens aller største tjenesteleverandører på nett, og gir Google tilgang på enorme mengder personlig informasjon. Er forbrukerne egentlig oppmerksomme på dette, og hvilke utfordringer skaper det?

Enkelte virksomheter velger å la eksterne leverandører drifte sine IKT-løsninger, noe som egentlig ikke er noe nytt. Markedet og teknologien har imidlertid utviklet seg enormt med inntreden av nettskyen, hvor man utnytter et globalt kommunikasjons- og datakraftmarked. Bruk av nettskyen kan skape utfordringer når det gjelder kontroll over personopplysninger og informasjonssikkerhet. Det er imidlertid både Datatilsynets og andre internasjonale personvernmyndigheters utgangspunkt at det er mulig å oppnå godt personvern også ved bruk av nettskytjenester.

Stortinget vedtok i 2011 å implementere datalagringsdirektivet i norsk rett. Datatilsynet vil få en rekke nye oppgaver i tilknytning til direktivet, blant annet tilsynsoppgaver og utarbeidelse av konsesjoner. Ved inngangen til 2013 er det fremdeles usikkert når lovendringen trer i kraft.

I meldingsåret mottok Datatilsynet en god del henvendelser som gjaldt nettsidene [www.minlarer.no](http://www.minlarer.no) og [www.legelisten.no](http://www.legelisten.no). Dette er nettsider der elever og pasienter kan gå inn og vurdere fastlegen sin og egne lærere, men problemstillingen er generell for alle typer forum og blogger på nett.

Spørsmålet er hvor grensene går for hva slags personopplysninger som kan legges ut. Hvor langt strekker ytringsfriheten seg i slike tilfeller? Dette er nok en utfordring vi bare vil se mer til fremover.

Det ligger i sakens natur at Internett og telekommunikasjon et felt der det som rører seg internasjonalt er av særlig stor betydning for Datatilsynets arbeid. Vi har derfor et utstrakt samarbeid med andre land og internasjonale aktører, noe som omtales nærmere under *Internasjonalt samarbeid*.

## Hva er gjort på området?

### Nettskytjenester

Det har vært mye oppmerksomhet og debatt rundt bruk av nettskytjenester, og mange har uttrykt usikkerhet om hvordan personvern og informasjonssikkerhet kan håndteres på en tilfredsstillende måte i slike tjenester.

Datatilsynet gjennomførte i 2012 en gjennomgang av Narvik kommunes bruk av nettskytjenesten Google Apps. Bakgrunnen for dette var at tilsynet i 2011 mottok en klage på kommunens bruk av tjenesten, og etter en vurdering av kommunens redegjørelse varslet tilsynet et vedtak om at deres bruk av tjenesten måtte opphøre.

Datatilsynet ble også kontaktet av Moss kommune som selv tok kontakt og ba om veiledning i bruk av Microsoft Office 365. På grunn av mange likhetstrekk med Narvik-saken, ble en gjennomgang av disse sakene gjort parallelt.

I forbindelse med begge sakene ble det avholdt flere konstruktive dialogmøter med kommunene og tjenesteleverandørene. Det førte blant annet til at leverandørene endret på sine standard databehandleravtaler. Dette er en avtale som partene må inngå når en virksomhet setter ut hele eller deler av sin behandling av personopplysninger til en annen virksomhet. Datatilsynet definerte dessuten noen forutsetninger som må være oppfylt for at bruk av nettskytjenester kan finne sted. Virksomheten må blant annet gjennomføre sikkerhets- og sårbarhetsanalyser i forkant, og en tilfredsstillende databehandleravtale må være på plass. Det er også viktig å revidere bruken av tjenesten jevnlig.

Datatilsynet konkluderte med at Narvik kommune kan bruke Google Apps og at Moss kommune kan ta i bruk Microsoft Office 365, så fremt forutsetningene i rapportene er på plass.

### Sak om bryting av kryptering

Datatilsynet behandlet i 2011 og 2012 en sak om bruk av sikkerhetsteknologi som bryter kryptert kommunikasjon.

Kryptert trafikk inn i virksomheters nettverk representerer en trussel for informasjonssikkerheten ved at slik trafikk ikke lar seg inspisere mot skadelig programvare og virus. Det er derfor utviklet sikkerhetstiltak som bryter krypteringen og gjennomfører kontroll mot uønsket innhold, før trafikken krypteres på nytt og sendes til brukeren, tilsynelatende uten at kommunikasjonen er brutt. Teknologien forutsetter at virksomheten har en grad av kontroll over brukerens utstyr.

For brukeren (normalt ansatt i virksomheten) og parten brukeren kommuniserer med, innebærer dette at den antatt sikre kommunikasjon ikke lenger er sikker. Dette kan være nettbasert e-post eller nettkommunikasjon med for eksempel fastlegen. Man kan også betrakte problemstillingen slik at krypteringen ikke er god nok siden den lar seg bryte.

Datatilsynet fattet først vedtak om opphør av praksisen med bryting av kryptering. Vedtaket ble senere omgjort. Forutsetningene for at praksisen vurderes som akseptabel, er at trafikk fra antatte sikre kilder utelates fra brytingen. Det må også etableres sikre rammer for behandling av dekryptert trafikk og at det blir gitt god informasjon til de ansatte om at privat kryptert kommunikasjon kan bli innsisert.

Saken viser at sikkerhetstiltak i én sammenheng kan representere en trussel mot personvernet og informasjonssikkerhet i en annen sammenheng. Det var viktig for tilsynet å sette virksomheten, som den ansvarlige for behandlingen, i stand til å ivareta sine forpliktelser etter personopplysningsloven, ved å ha kontroll over eget informasjonssystem og ivareta personvern og informasjonssikkerhet.

### *DLD-konsesjonen*

Stortinget har som kjent vedtatt at EUs datalagringsdirektiv (direktiv 2006/24/EF) skal innføres i norsk rett. Datatilsynet fikk i den sammenheng i oppdrag å lage en standardkonsesjon for å behandle de lagringspliktige personopplysningene. I 2011 ble det innledet samtaler med blant annet Samferdselsdepartementet, Post- og teletilsynet samt representanter fra tele- og internetttilbyderne om hvilke utfordringer de ulike involverte instansene og virksomhetene står overfor. På bakgrunn av dette ble det i desember 2011 sendt et utkast til konsesjon på høring.

Vårt mandat er å stille konsesjonsvilkår som på best mulig måte ivaretar de registrertes personvern og underlegger de lagrede dataene tilfredsstillende sikkerhetskrav. Samtidig er det av stor betydning å skape et praktisk gjennomførbart regime som ikke undergraver formålet med implementeringen av direktivet. En tett dialog med de virksomhetene som vil bli underlagt lagringsplikt, samt representanter fra Politiet og Post- og teletilsynet, var derfor av sentral betydning.

Datatilsynet mottok konstruktive hørings svar og kunne i mai 2012 sende ut en endelig konsesjon til de sentrale aktørene. Det er imidlertid tatt forbehold om at det ennå hersker noe usikkerhet om de rettslige premissene for implementeringen.

### *Høringsuttalelse – datalagringsforskriften*

I sitt forslag til datalagringsforskrift slår Post- og teletilsynet fast at det ikke er aktuelt å pålegge leverandører av innholdstjenester lagringsplikt. Datatilsynet støtter selvsagt dette. Konsekvensene av innholdslagring ville være uoverskuelige og svært inngripende.

Innholdslagring ble fullstendig avvist av Stortinget da direktivet ble vedtatt implementert i norsk rett, og dette er nå nedfelt i forslaget til datalagringsforskrift. Dersom leverandører av diskusjonsforum skulle pålegges lagringsplikt slik noen har antydnet, ville det medført betydelige personvernkonsekvenser. Det vil bli umulig å unngå å lagre opplysninger om selve innholdet i kommunikasjonen om det skulle vedtas. Datatilsynet mener videre at det er rimelig at staten dekker de totale, eller deler av, tilbydernes investeringskostnader.

### *Overtredelsesgebyr til Google*

I september ble Google ilagt et overtredelsesgebyr på 250 000 kroner av Datatilsynet for brudd på personopplysningsloven. Google måtte også slette personlig informasjon innsamlet av deres Street View-biler i Norge.

Bakgrunnen var at Datatilsynet i 2010 ble informert av Google om at deres Street View-biler hadde samlet inn nytteedata (payload-data) i forbindelse med sin kartlegging av gater og veier i Norge. Nyttedata vil si kommunikasjon på private trådløse nettverk, og kan blant annet omfatte brukernavn, passord og innhold i e-poster. Datatilsynet ba i 2011 Google om å slette alle disse dataene, og fikk en bekreftelse på at dette var gjennomført. I meldingsåret kom det derimot frem at alle disse dataene ikke var slettet likevel, noe tilsynet så svært alvorlig på.

Google manglet et rettslig grunnlag for å innhente den aktuelle typen informasjon, det var ikke bedt om samtykke fra enkeltpersonene dette omfattet, opplysningene var lagret utover det som er nødvendig og opplysningene var ikke slettet etter anmodning fra Datatilsynet. Dette omfattet dessuten en forholdsvis stor gruppe intetanende enkeltindivider. Tilsynet tok hensyn til at det var Google selv som varslet om innsamlingen. Det ville vært vanskelig for Datatilsynet alene å oppdage denne type avvik.

### *Oppfølgingen av Facebook*

Facebook har sitt europeiske hovedkontor i Irland, og det er de irske personvernmyndighetene som fører tilsyn med virksomheten. Det norske Datatilsynet har imidlertid også ført en aktiv dialog med Facebook i meldingsåret, og det har vært avholdt to møter der Facebook har stilt med representanter på høyt europeisk nivå. Blant temaene som har vært diskutert er ansiktsgjenkjenning og Facebooks skanning av brukernes innhold. Facebook er også oppfordret til å utarbeide offentlige rapporter over hvor mange henvendelser de får fra politiet om innsyn i brukernes konti. Videre har vi løpende gitt innspill til de irske personvernmyndighetene direkte og gjennom Technology Subgroup, som er en internasjonal arbeidsgruppe for personvernmyndigheter.

Det utstrakte europeiske samarbeidet omkring oppfølgingen av Facebook kan det leses mer om under *Internasjonalt samarbeid*.

### *Personvernemnda – Nettby*

Datatilsynet vedtok i 2011 at personopplysninger som stammer fra det nedlagte nettsamfunnet Nettby (eid av VG) skulle slettes. VG klagde på vedtaket og saken endte hos Personvernemnda. Nemnda kom i meldingsåret til at det foreligger en avleveringsplikt for de dokumentene VG ønsker å lagre i denne saken, det vil si innholdet i de åpne fora/områdene som var åpne for indeksering i søkemotorer. Det gjelder også for de delene som ikke var åpne for indeksering, men som var tilgjengelige for samtlige borgere av Nettby. Avleveringsplikten må oppfylles før materialet slettes av VG.

Avgjørelsen er viktig med tanke på at mange personer i dag benytter sosiale nettsamfunn. De tenker antakelig i liten grad på at de ikke selv bestemmer hvor lenge opplysningene skal lagres, og hvem som skal ha tilgang til disse, både i nåtid og i ettertiden. Nemnda legger til grunn at også de som stiller en plattform til rådighet for enkeltpersoner har plikter overfor det offentlige ved Nasjonalbiblioteket, i form av en avleveringsplikt. Konsekvensen av en slik forståelse vil ha betydning



langt utover denne saken med tanke på de mange aktører som gjør som VG – stiller en plattform eller et forum til rådighet for en stor gruppe personer.

## Funn fra tilsyn

### *Google Analytics – behandling av IP-adresser*

Størsteparten av norske virksomheter bruker Google Analytics til å analysere brukeratferd på sine nettsider. I 2011 ble det gjennomført kontroller hos Skatteetaten og Lånekassen da dette er store virksomheter som de fleste borgere er nødt å forholde seg til. Kontrollene avdekket enkelte uklarheter når det gjelder analyseverktøyets behandling av IP-adresser i forbindelse med besøk på nettsidene. Bruk av Google Analytics berører også det felleseuropeiske regelverket om forhåndssamtykke ved bruk av informasjonskapsler, direktiv 2009/136/EF, et direktiv som for øvrig ikke er innført i Norge enda.

I 2012 varslet Datatilsynet at det vurderte å fatte vedtak om at etatene må dokumentere at IP-adressene som samles inn ved hjelp av analyseverktøyet blir anonymisert uten opphold. Det ble også varslet vedtak om at etatene må dokumentere at personopplysningene ikke benyttes til andre formål etter at de er samlet inn.

Skattedirektoratets og Lånekassens tilbakemeldinger på varselet kom i oktober, og der kom det fremt frem at IP-adressene anonymiseres i minnet *før* adressene blir lagret hos Google. De viser også til at anonymiseringen er reell, det vil si av en slik art at den ikke er reverserbar. Google har dessuten oversendt en skriftlig bekreftelse på at opplysningene ikke brukes til andre formål enn de som er oppgitt.

En endelig vurdering av etatenes tilbakemeldinger foreligger i 2013.

### *Mobilapplikasjoner*

Datatilsynet gjennomførte våren 2012 tilsyn med tre virksomheter som sto ansvarlig for applikasjoner (apper) til smartmobiler. De tre tilsynsobjektene DnB Eiendom, NSB og Wimp ble valgt blant annet på grunn av størrelse og antall kunder.

Under tilsynene var det spesielt interessant å få belyst tre forhold; hvem som var behandlingsansvarlig, hvilke opplysninger som ble innhentet og behandlet, samt hvilken informasjon som ble gitt til kundene. De tre leverandørene ga klare svar på spørsmålet om behandlingsansvar. I tillegg var det minimalt med personopplysninger som ble innhentet i forbindelse med de aktuelle appene.

Brukerne skal informeres om hvordan en app benytter personopplysninger, slik som telefonens posisjon eller informasjon fra telefonens kontaktbok. Informasjon kan gis der appen kjøpes, inne i appen, eller på nettstedet til den behandlingsansvarlige. Det sentrale er at brukeren blir gitt informasjon *før* bruken tar til. De kontrollerte virksomhetene hadde lagt til rette for informasjon om behandlingen av personopplysninger i appene. Datatilsynet pekte likevel på enkelte forbedringsområder når det gjaldt hvordan informasjonen ble gitt.

## Helse og velferd

Helse og velferd involverer samtlige innbyggere i Norge, i alle stadier av livet. Opplysningene som behandles i sektoren er blant de mest sensitive personopplysningene som finnes. Samtidig må folk gi fra seg svært mange opplysninger i "bytte" mot helsehjelp. Enkeltpersoner har begrenset kontroll med spredningen av opplysningene og trolig også liten kjennskap til hvordan opplysninger benyttes og videreformidles.

Sektoren er preget av en relativt høy grad av endringsvilje og -evne, fra departement til institusjonsnivå, samtidig som sektoren har hatt utfordringer over lang tid med å løse god samhandling, samt sikre helseopplysninger mot uautorisert innsyn.

Regjeringen la i november 2012 frem stortingsmeldingen "*Én innbygger – én journal – Digitale tjenester i helse og omsorgssektoren*" (Meld. St. 9 2012-2013). Her legges kursen for den videre digitaliseringen av helsesektoren mot målet om én innbygger – én journal. I meldingen legges det opp til videre satsning på igangsatte aktiviteter slik som styrket samhandling gjennom meldingsutveksling, kjernejournal og tilrettelegging for tilgang på tvers.

Helsesektoren har et stort kunnskapsbehov, og det finnes en rekke helseregistre som gir grunnlag for å styre, kvalitetssikre og forske på helseopplysninger. Ivaretagelse av personvernet avhenger av registerform og hva som registreres, varighet av registreringen og i hvilken grad personen selv kan velge sin deltakelse. En sentral prosess her er modernisering av helseregisterfeltet.

Vi vil i årene som kommer se økt interesse for og bruk av teknologi innen omsorgssektoren, gjerne kalt velferdsteknologi. Velferdsteknologi er mangeartet og kan benyttes i mange ulike former; varslings- og lokaliseringsteknologi, slik som fallalarmer og komfyrvakt, mobilteknologi i oppfølging av pasienter, digitale kanaler for sosial kontakt og lignende. Noen løsninger lagrer helse- og personopplysninger, og noen gjør det ikke.

Velferdsteknologi kan ivareta pasientenes helsemessige behov på en god måte samtidig som personvernet ivaretas. Mange vil for eksempel oppleve det som mindre integritetskrenkende å avlegge en urinprøve hjemme og sende svaret elektronisk enn å gjøre det på et legekontor. Samtidig som teknologien gir mange muligheter kan den imidlertid også innebære utfordringer for personvernet. Noen former for velferdsteknologi innebærer en overvåking og kontroll som krenker den enkeltes personlige integritet. Datatilsynet har prioritert å delta i prosessene rundt utviklingen av velferdsteknologi for sikre at det etableres løsninger som både støtter gode tjenester og ivaretar personvernet. Området er velegnet for å arbeide etter prinsippene for innebygd personvern ved at man allerede i innovasjons- og utviklingsfasen tar hensyn til personvernet.

## Hva er gjort på området?

### *Genteknologi*

Datatilsynet har i meldingsåret jobbet med en kartlegging av sentrale personvernutfordringer i helsesektoren og i helseforskning, knyttet til gjennomføring av genetiske undersøkelser, samt bruk av genetiske opplysninger og biologiske materiale.

Et viktig element i personvernet er at personer i utgangspunktet skal kunne bestemme over bruken av egne genetiske opplysninger og biologisk materiale. Det er særlig hensynet til overordnede helseformål, samfunnsinteresser og forskningsinteresser som utfordrer den enkeltes rett og mulighet til selv å bestemme over disse opplysningene. Det utleveres genetiske opplysninger fra behandlingsrettede helseregistre til flere sentrale helseregistre.

På grunn av rutinekontroller og masseundersøkelser kan det antas at det per i dag finnes minst én prøve (biologisk materiale) av de aller fleste personer i Norge lagret i en biobank. Per 1. januar 2008 var det anslått at det totalt forelå prøver fra i overkant av 12 millioner pasienter over fire til fem generasjoner. Det sentrale formålet for oppbevaring av materialet er i første omgang helsehjelpsformål. Oppbevaringen av materialet utover dette formålet skjer for å ivareta andre interesser, slik som samfunns- og forskningsinteresser. Kommersielle interesser er også relevant i denne sammenhengen.

En sentral personvernutfordring er at det er lav kunnskap i befolkningen om det omfattende materialet som er lagret i landets biobanker. Datatilsynet mener en viktig årsak til dette kan spores til svakheter ved dagens regelverk. For det første er det en utfordring at et stilltiende samtykke til helsehjelp også er et tilstrekkelig rettslig grunnlag for lagring av materialet for senere bruk til samfunns- og forskningsformål. For det andre har det vist seg at informasjonsplikten om retten til å reservere seg mot bruk av biologisk materiale i forskning ikke fungerer i praksis.

Samtidig som dagens regelverk har svakheter, utredes mulighetene for å utnytte biologisk materiale bedre i forsknings- og kommersielt øyemed. Det er tatt til orde for å etablere en felles nasjonal forskningsbiobank for forskningsformål og å utnytte biobankmateriale for kommersielle formål.

Rapporten foreslår tiltak for å styrke personvernet på området. Rapporten har også identifisert uklarheter, mangelfull etterlevelse og mangler ved dagens regelverk.

### *Velferdsteknologi*

Per i dag mangler det et rettslig grunnlag for å ta i bruk varslings- og lokaliseringsteknologi i den offentlige helse- og omsorgstjenesten hvis man ikke har samtykke fra pasienten. Et forslag til en lovbestemmelse som gir en begrenset adgang til bruk av slik teknologi overfor personer som ikke er samtykkekompetente var på høring i 2012. Datatilsynet ga sin støtte til dette arbeidet.

Datatilsynet har arbeidet aktivt med dette området for å sikre at innbygget personvern skal være en del av de velferdsteknologiske løsningene som utvikles. Hjelpemiddelet som tas i bruk må være minst mulig integritetskrekkende. For eksempel bør det ved bruk av lokaliseringsteknologi ikke lagres opplysninger utover den tiden det tar å lokalisere brukeren, alarmer bør utløses av pasienten selv i

de tilfellene det er tilstrekkelig og såkalte "geofences" – virtuelle elektroniske gjerdar – bør benyttes fremfor kontinuerlig overvåking.

Datatilsynet har gjennomført flere aktiviteter for å bidra til ivaretagelse av personvernet når velferdsteknologi tas i bruk:

- Kontakt med forsknings- og utviklingsmiljøer, samt kommuner som bruker velferdsteknologi.
- Deltakelse i den offentlige debatten omkring bruk av GPS på personer med demens. Tilsynet har også gitt tilslutning til at GPS-sporing av demente kan innebære mer frihet, verdighet og trygghet for den enkelte under forutsetning av at personvern hensyn blir ivare tatt allerede ved utviklingen av løsningene.
- Deltakelse i en arbeidsgruppe hos Helsedirektoratet. Gruppen har jobbet med en fagrapport om bruk av varslings- og lokaliseringsteknologi i den kommunale helse- og omsorgstjenesten.
- Deltakelse i arbeidet med å få på plass et rettslig grunnlag for bruk av varslings- og lokaliseringsteknologi.

### *Samhandlingsutfordringer*

Datatilsynet har vært i dialog med helsemyndighetene om etableringen av helseportal og kjernejournal. For tilsynet er det sentralt at slike løsninger etableres etter prinsippene for innebygd personvern, og vil derfor videreføre denne dialogen.

Datatilsynet har over tid kommunisert til helse- og omsorgssektoren at det har vært en utfordring knyttet til bruk av felles journalsystemer mellom virksomheter i primærhelsetjenesten. Dette har nå blitt løst med en forskrift som kom i november om virksomhetsovergrepene pasientjournal i formalisert arbeidsfellesskap. Forskriften er ikke begrenset til primærhelsetjenesten. Datatilsynet har i høringsrunden gitt omfattende innspill, blant annet for å sikre at forskriften ivaretar ulike samhandlingsformer, slik som samhandling mellom kommunen og spesialisthelsetjenesten. Den vedtatte forskriften er relativt generell og løser godt utfordringen med felles journalsystem i primærhelsetjenesten. For øvrige samarbeidsløsninger er ikke rammene like tydelige.

Helseinformasjonssikkerhetsforskriften ble vedtatt i juni 2011, men er ikke trådt i kraft enda. Forskriften setter klarere rammer for informasjonssikkerhet, og stiller krav som må oppfylles for at virksomheter kan utøve tilgang til hverandres journalsystemer. Datatilsynet imøteser de klagerte kravene til informasjonssikkerhet. For tilgang til hverandres systemer er det viktig at fagsystemene blir modernisert slik at det kan skje på en trygg måte. Datatilsynet har dialog med sektoren om dette gjennom standardiseringsarbeid og gjennom *Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren* (Normen).

### *Sikre pasientjournaler – snoking og tilgangsstyring*

Datatilsynet har lenge pekt på utfordringen ved manglende konfidensialitetssikring i pasientjournalene. Mangelfulle løsninger for tilgangsstyring i kombinasjon med enten mangelfull logging eller manglende funksjonalitet for loggkontroll, gjør at det er store muligheter for å gjøre uautoriserte oppslag i pasientjournaler. Det er samtidig små muligheter for å avdekke slik snoking.

Ved endring av helseregisterloven i 2008 ble det gjort klart at det er forbudt å gjøre uautorisert oppslag i journalene.

I meldingsåret har Datatilsynet fulgt sektorens arbeid med løsninger for logganalyse, og da spesielt et forprosjekt i regi av Oslo Universitetssykehus. Det overordnede formålet med logganalyse er å etablere løsninger som gjør det mulig å avdekke uautorisert bruk. Etter det vi forstår er funnene i forprosjektet positive.

Av avviksmeldinger og kontakt med sektoren observerer vi at snoking i journalsystemer følges mer profesjonelt opp av sektoren, både arbeidsrettslig, gjennom melding til Datatilsynet, gjennom kontakt med Helsetilsynet og i noen tilfeller gjennom politianmeldelse. Det fremstår som om loggene nærmer seg et nivå hvor de er tilstrekkelige til å bekrefte mistanke om snoking, selv om de ikke blir analysert i tilstrekkelig grad for å avdekke snoking. I et tilfelle ble en politianmeldt sak henlagt selv om snoking ble dokumentert gjennom logger. Årsaken var, etter det Datatilsynet kjenner til, at autentiseringen bare besto av brukernavn og passord, såkalt svak autentisering, og at det ikke kunne bevises at det var det aktuelle helsepersonellet som hadde brukt sin egen brukertilgang. Datatilsynet ser det som nødvendig at det arbeides mot sterkere autentiseringsløsninger i sektoren.

I arbeidet med tilgangsstyring håper tilsynet at det pågående arbeidet med standardisering av helsefagsystemer i regi av Helsedirektoratet kan bidra til at systemene får nødvendig funksjonalitet. Datatilsynet følger med på dette arbeidet.

Det har ikke vært gjennomført tilsyn med denne tematikken i meldingsåret, men det er klart at tilstanden ikke er tilfredsstillende. Datatilsynet opplever at helsemyndighetene slutter seg til dette, at de gjennomfører tiltak, blant annet ved at helseinformasjonssikkerhetsforskriften er vedtatt, og ved at det arbeides med standardisering, som nevnt ovenfor.

#### *GE-sakene – uautorisert utlevering av helseopplysninger*

Datatilsynet fikk i mars 2012 kjennskap til uautorisert utlevering av helseopplysninger fra flere virksomheter til leverandøren GE Healthcare Systems (GE) i USA. Opplysninger om et betydelig antall pasienter var hentet ut og overført, og omfattet blant annet pasienters navn, ID-nummer, fødselsdato og helseopplysninger. Avviket gjaldt elleve virksomheter i Norge. Det ble opprinnelig meldt til tilsynet at det var snakk om 126 344 pasienter, men dette tallet er noe usikkert.

Bakgrunnen for saken er at virksomhetene har hatt en tilknytning til leverandøren GE som skal drive vedlikehold og overvåking av medisinteknisk utstyr. Tilknytningen har vært satt opp på en slik måte at GE har kunnet hente ut helseopplysninger uten tekniske hindre. Datatilsynet mener at opplysningene ikke har vært godt nok sikret.

Datatilsynet fattet vedtak med flere pålegg i saken, blant annet om at virksomhetene må etablere tilfredsstillende sikkerhetstiltak når det gjelder konfidensialitet for leverandørtilknytninger mot medisinteknisk utstyr. Det ble også fattet vedtak om at de berørte identifiserte pasientene må informeres om hendelsen.

Pålegget om informasjon til pasientene er påklaget fra nesten samtlige virksomheter. Ved årsskiftet var klagen til vurdering hos Datatilsynet.

### *Personvernemnda – reseptregisteret*

Folkehelseinstituttet har ønsket å hente et begrenset antall variabler for et utvalg inneliggende pasienter, for deretter å importere informasjonen til reseptregisterets database. Det ble derfor søkt om å få utrede en løsning for innsamling av informasjon om legemiddelbruk for pasienter i institusjon. Datatilsynet ga avslag på denne søknaden og saken endte hos Personvernemnda. Nemnda kom, i likhet med Datatilsynet, frem til at reseptregisteret bare kan inneholde opplysninger som direkte eller indirekte fremkommer av reseptene og rekvisisjonene. Denne testingen ville derfor innebære en utvidelse som ikke kan gjennomføres med mindre reseptregisterforskriften endres.

Avgjørelsen viser at reseptregisteret som et pseudonymt register, skal være beskyttet for utvidelser eller sidebruk utover det som står i forskriften. Dette er godt personvern og styrker tilliten til registeret og forutberegneligheten for reseptinnehavere. Avgjørelsen støtter også opp under at Datatilsynets fullmakter ikke skal være et middel for å utvide eller innføre tillegg til eksisterende grenser angitt i lov eller forskrift.

### *Personvernemnda – opplysninger fra politirapporter til forskning*

I en konkret sak var det spørsmål om en rettsmedisinsk studentoppgave, der det ble hentet opplysninger fra politirapporter, hadde behandlingsgrunnlag. Behandlingsgrunnlaget for en slik bruk av personopplysninger må finnes i personopplysningsloven, og Datatilsynet mente at man måtte ha et samtykke for denne type forskning. Nemnda kom derimot til at samfunnsinteressen, og verdien av forskningen, måtte veie tyngre enn personvernet.

Avgjørelsen føyer seg inn i en rekke saker hvor temaet er interesseavveiningen mellom personvern for den enkelte og andre interesser. Avgjørelsen er viktig for tilsynet i det videre arbeidet hvor denne typen avveining er en avgjørende del av vår saksbehandling.

### *Personvernemnda – SUSS-saken*

Datatilsynet gjennomførte høsten 2010 et tilsyn med Senteret for ungdomshelse, samliv og seksualitet (SUSS). Stiftelsen arbeider for å sikre ungdom hjelp til å oppnå bedre helse, spesielt ved å forebygge uønsket graviditet, abort og seksuelt overførbare sykdommer.

SUSS gir råd og veiledning til ungdommer via telefon, SMS og e-post. Kontrollen avdekket at SUSS lagret telefonnummeret til de som kontaktet dem, og i tillegg ble det registrert hva problemstillingen eller spørsmålet var, samt hvilke råd eller veiledning som ble gitt. Samtlige av virksomhetens henvendelser ble journalført, noe som var i strid med informasjonen på deres nettsider. På deres egen nettside ble det på kontrolltidspunktet opplyst at man var helt anonym. Datatilsynet innhentet en lovtolkning fra Helsedirektoratet og Helse- og omsorgsdepartementet for å få avklart om SUSS sin veiledning kom inn under begrepet helsehjelp.

På bakgrunn av avklaringen fattet tilsynet pålegg om at SUSS måtte slette personopplysninger som ble lagret i forbindelse med virksomhetens veiledning, med mindre det kunne påvises et gyldig rettslig grunnlag for behandlingen, alternativt kunne opplysningene anonymiseres. Virksomheten ble videre pålagt å oppfylle sin informasjonsplikt overfor brukerne.

Datatilsynets pålegg ble klaget inn for Personvernemnda, som støttet tilsynet. SUSS må etter nemndas avgjørelse rydde opp i de registrerte opplysningene. Virksomheten må enten anonymisere

eller slette alle personopplysninger som er registrert når SUSS har gitt veiledning eller råd til personer som ønsker å være anonyme. SUSS må videre endre informasjonen på nettsidene, og begrep som anonym kan ikke benyttes dersom dette er misvisende overfor brukerne. Informasjonen på SUSS sin nettside må være klar, tydelig og lettfattelig.

### *Høringsuttalelse – kreftscreening*

Helse- og omsorgsdepartementet har foreslått å endre kreftregisterforskriftens regler om behandling av opplysninger om personer som har deltatt i program for tidlig diagnose eller kontroll for konkret kreftsykdom (kreftscreening). Departementet ønsker å oppheve reglene om at pasienter må gi uttrykkelig samtykke for at negative funn i screeningprogrammer skal kunne oppbevares permanent. I stedet foreslår de å etablere en ordning der pasienter må reservere seg mot lagring.

Endringen omfatter de to store screeningsprogrammene som foregår i regi av Kreftregisteret i dag; Mammografiprogrammet og Livmorhalskreftprogrammet. Datatilsynet var tidligere (2009) gjort kjent med at samtykke ikke var innhentet for denne kategorien registrerte, og fattet derfor vedtak om at slikt samtykke skulle innhentes.

Datatilsynet ga i sin høringsuttalelse uttrykk for at forholdene i utgangpunktet ligger godt til rette for innhenting av samtykke til permanent lagring av opplysninger om negative funn. Vi mener at departementet burde ha vurdert om dagens ordning med samtykke kunne vært videreført tilfredsstillende gjennom å endre rutiner hos helsepersonellet. Datatilsynet oppfordrer også departementet om å pålegge informasjonsplikt i tilknytning til prøvetakingen, slik at den enkelte får en reell mulighet til å ivareta sine egne interesser.

Etter at denne høringsuttalelsen ble avgitt i mars 2012, kom det i desember nok et forslag til endring i kreftregisterforskriften, hvor det ble foreslått at regelen om reservasjon skal gis tilbakevirkende kraft. Målet er en så fullstendig oversikt over prøver med negativt resultat som mulig. Departementet fremstiller endringen fra samtykke til denne tilbakevirkende reservasjonsretten som kun "av praktisk karakter".

Datatilsynet er svært skeptiske til dette forslaget, da det i praksis vil oppheve vedtaket om innhenting av samtykke etter gjeldende forskrift, et vedtak som også er stadfestet av Personvernemnda. Det kan stilles spørsmål ved om dette er et brudd på Datatilsynets uavhengighet, ved at tilsynet i realiteten styres politisk.

## Justissektoren

Den enkeltes rett til å bestemme over egne personopplysninger er ikke absolutt. Hensynet til samfunnets interesser vil i mange tilfeller veie tyngre enn hensynet til den enkeltes personvern. Dette er særlig tydelig innen nettopp justissektoren. Her står den enkeltes individuelle interesser i sterk konflikt med svært tunge samfunnsinteresser, som for eksempel kriminalitetsbekjempelse og samfunnssikkerhet. Det er et gjennomgående trekk ved sektoren at borgeren har minimalt med autonomi og har begrenset kunnskap om hvilke opplysninger som samles inn til hva. Dette er utfordrende fra et personvernståsted, særlig fordi sektoren har hjemmel til å bruke tvangsmidler.

Innen justissektoren virker personvernet som en rettsverngaranti som setter grenser for statens maktbruk overfor sine borgere. Ettersom selvbestemmelsesretten er begrenset innen sektoren, er det ekstra viktig at de andre personvernprinsippene ivaretas. Det gjelder særlig kravene om at behandlingen skal ha et rettslig grunnlag, at de registrerte skal ha informasjon og at nytten av tiltaket skal stå i forhold til inngrepet.

Datatilsynet er særlig opptatt av at de mest inngripende tiltakene må ha hjemmel i lov, fastsatt i Stortinget. Det er nødvendig både for å sikre forutberegnlighet for borgerne og for å sikre at forholdsmessigheten i tiltaket er belyst og vurdert i en bred, demokratisk lovprosess. Siden behandlingene av personopplysninger innen sektoren for en stor del er lovhjemlet, blir legalitetskontrollen et helt sentralt element i vår oppfølging av sektoren.

I tillegg er Datatilsynets mål å søke å bevare det tillitsbaserte samfunnet, hvor iverksettelse av kontrolltiltak overfor den enkelte borger må begrunnes særskilt, og hvor informasjon og åpenhet omkring offentlig myndighetsutøvelse er en selvfølge.

## Hva er gjort på området?

### *Strategi for et godt personvern i justissektoren*

I meldingsåret utarbeidet Datatilsynet en egen strategi for godt personvern i justissektoren. Her beskrives de særlige utfordringene som oppstår for personvernet innen denne sektoren mer inngående. Tilsynet gjør også rede for sine overordnede mål for sektoren, sine posisjoner i enkeltspørsmål og sine strategiske valg.

Datatilsynet mål for denne sektoren, og som strategien utdyper, er blant annet å bevare det tillitsbaserte samfunnet, der iverksettelse av kontrolltiltak overfor den enkelte borger må begrunnes særskilt. Tilsynet vil også jobbe for at det gjennomføres demokratiske prosesser *før* inngripende tiltak settes i verk. Videre må det sikres at offentlig myndighetsutøvelse skjer innenfor rammene av de fullmaktene Stortinget har gitt, samt sørge for informasjon og åpenhet omkring offentlig myndighet.

Strategien skal ligge til grunn for vår egen virksomhet, men er også ment å gi et budskap til omverdenen om våre posisjoner. Strategien er derfor presentert for sentrale aktører innen sektoren; både politiske myndigheter og forvaltningsorganer. Den er også gjort tilgjengelig på Datatilsynets hjemmeside.



### DNA-screening

I forbindelse med alvorlige straffesaker har politiet i stadig større utstrekning benyttet seg av såkalt DNA-screening. Det er en etterforskningsmetode som medfører at et stort antall personer blir kalt inn til politiet med status som vitner, inkludert en anmodning om å avgi frivillig DNA-prøve. Det er ikke grunnlag for mistanke mot de personene som kalles inn. Innkallingen er gjerne basert på teleoperatørens trafikkdata som indikerer hvilke personer som var i nærheten av åstedet på det aktuelle tidspunktet. Statusen som vitne skulle tilsa at den enkelte antas å kunne bidra til oppklaring av saken, men det å avgi en DNA-prøve for eventuelt å bli sjekket ut av en straffesak er etter vår oppfatning ikke en del av vitneplikten. Enkeltpersoner blir slik satt i en situasjon der deres status vil kunne oppfattes nærmere som *mistenkt* enn som et vitne.

Datatilsynet har mottatt flere henvendelser fra enkeltpersoner som har blitt kalt inn til frivillig DNA-testing. De beskriver at det oppleves som tvang da de frykter at manglende fremmøte gjør at man får et mistankens lys på seg.

Datatilsynet er skeptisk til denne metodebruken. Spørsmålet om lovligheten reguleres imidlertid av straffeprosessloven, og faller dermed utenfor tilsynets forvaltningskompetanse. Tilsynet har derfor henvendt seg til Justisdepartementet for å be dem vurdere om en slik praksis er i tråd med straffeprosessloven.

Tilsynet problematiserte særlig om et samtykke til DNA-testing i forbindelse med en screening kan være reelt frivillig. Den enkeltes egne personlige forutsetninger i møte med politiet vil være avgjørende for om samtykket er gyldig, og dermed om det foreligger et rettslig grunnlag for undersøkelsen. Datatilsynet mener dette er uholdbart. Hvis det rettslige grunnlaget mangler vil politiets virksomhet i det enkelte tilfellet være i strid med menneskerettighetene og statens internasjonale forpliktelser. Tilsynet mener derfor at det er Stortinget som skal fastsette grensene for politiets etterforskningsvirksomhet. Det kan ikke overlates til den enkelte borger å måtte forholde seg til.

Datatilsynet har blitt orientert om at ressursituasjonen i Justisdepartementet foreløpig ikke har tillatt en realitetsbehandling av henvendelsen.

### Nødnettet

Datatilsynet mottok i 2012 en henvendelse fra Motorola Solutions som drifter nødnettet i henhold til en avtale med Direktoratet for nødkommunikasjon. Virksomheten stilte Datatilsynet spørsmål om sin rolle ved behandling av personopplysninger i nødnettet, for eksempel om det er adgang til sentral lagring av lydlogg.

Med bakgrunn i den påfølgende korrespondansen mellom virksomheten, Datatilsynet og Direktoratet for nødkommunikasjon, kom Datatilsynet til at det var et behov for å avklare roller og ansvarsforhold rundt behandlingen av personopplysninger i nødnettet. Tilsynet er av den oppfatningen at behandlingsansvaret for kommunikasjonssinnholdet hviler på den enkelte brukeren av nødnettet, for eksempel politiet, helsetjenesten, brann- og redningsetaten og frivillige organisasjoner. Det innebærer at Motorola Solutions kun vil være en databehandler og må forholde seg til de instruksene som blir gitt av den enkelte behandlingsansvarlige. Tilsynet mener at dette er en uheldig løsning med tanke på behandlingens karakter og antall behandlingsansvarlige.

Datatilsynet har i dialog med Justisdepartementet anbefalt at det etableres en egen lovgivning for å sikre tilfredsstillende og oversiktlige ansvarsforhold rundt behandlingen. Tilsynet har derfor tatt til orde for at tjenesteleverandøren bør pålegges et selvstendig ansvar som sådan. I den forbindelse kan det være aktuelt å se på ansvaret teleleverandørene har etter ekomlovgivningen.

### Høringsarbeid

Meldingsåret har naturlig nok vært preget av at regjeringen ønsker å iverksette tiltak etter hendelsene 22. juli 2011. Det har vært fremsatt lovendringsforslag som også medfører utvidet kriminalisering og utvidede fullmakter til både politiet og ulike forvaltningsorganer. Dette er tiltak som kan få store konsekvenser for den enkeltes personvern.

#### *Kriminalisering av terrorforberedelser*

Tilsynet vil særlig nevne regjeringens forslag om ytterligere kriminalisering av forberedelse til terrorhandlinger. Forslaget innebar blant annet å straffelegge hverdagslige handlinger dersom det kunne bevises at handlingene skjedde med et terrorforsett.

Datatilsynet uttalte at departementet var farlig nær å foreslå kriminalisering av borgernes tanker, noe som medfører et behov for meget inngripende etterforskningsmetoder. Tilsynet kritiserte at utredningen var mangelfull og ensidig. Siden utredningen i all hovedsak fremstod som å være en ukritisk videreformidling av PSTs synspunkter og påstander, understreket tilsynet at det ikke må overlates til politiet selv å definere sine fullmakter. Vi etterlyste en mer grundig utredning og en klarere begrunnelse for forslaget. Tilsvarende synspunkter ble også fremmet av en rekke andre høringsinstanser, noe vi er godt fornøyde med.

#### *Endringer i statsborgerloven og statsborgerforskriften*

Regjeringen foreslår å gi statsborgermyndighetene hjemmel i lov til å hente inn og behandle opplysninger fra andre offentlige organer i saksbehandlingsøyemed, uten hinder av taushetsplikt.

I denne høringsaken ble Datatilsynet også invitert til dialog. Barne-, likestillings- og inkluderingsdepartementet ønsket en nærmere redegjørelse for tilsynets skepsis til forslaget. Tilsynet mente forslaget utfordret retten til å ha kontroll med egne personopplysninger ved at opplysningene skulle hentes inn av forvaltningen uten søkerens medvirkning. Tilsynet mente også forslaget brøt med grunnleggende personvernprinsipper som formålsbestemthet, forholdsmessighet og nødvendighetskravet; nytten må stå i forhold til inngrepet. Departementet på sin side ønsket å informere om bakgrunnen for forslaget ut over det som fremgikk av høringsnotatet. Etter møtet ble Datatilsynet anmodet om å revurdere den avgitte høringsuttalelsen og eventuelt frafalle den, noe vi ikke fant grunn til. Forslaget fremstod også etter departementets redegjørelse som et stort inngrep i den enkeltes personvern.

Datatilsynet ser generelt svært positivt på at vi kan være aktive deltakere i regelverksutviklingen i samfunnet og på den måten sikre at personvernet ivaretas på et tidlig tidspunkt i prosessen. Vi mener det er bedre for det endelige resultatet at personverninteressen integreres i arbeidet i motsetning til at det "legges på til slutt". Erfaringsmessig gir et slikt etterarbeid mindre gode og mer kompliserte løsninger.

## Funn fra tilsyn

### *NAVs kontrollvirksomhet*

Datatilsynet gjennomførte i 2012 et tilsyn hos NAV Kontroll. Formålet var å vurdere om NAV gjennomfører kontroll av borgerne i tråd med Stortingets fullmakter, slik de er definert i folketrygdloven og personopplysningsloven med forskrift. NAVs kontrollvirksomhet omfatter en ustrakt behandling av tildels svært sensitive personopplysninger. Opplysningene kan knyttes både til stønadsmottakerne og andre, og hentes inn fra en stor krets personer, virksomheter og offentlige myndigheter. Det ble vurdert som viktig å se på opplysninger om andre enn stønadsmottakerne, i og med at de i liten grad er del av kommunikasjonen med NAV i forbindelse med søknad om stønad eller annen ytelse.

Funnene førte til at Datatilsynet ba Arbeidsdepartementet om å revidere folketrygdlovens bestemmelser, eller å utdype dem gjennom et forskriftsverk. Datatilsynet mente at gjeldende regelverk er for vidtrekkende og skjønnsmessig, og at det ikke tilfredsstillende angir klare rammer for NAVs kontrollvirksomhet.

Det ble også avdekket at NAVs interne rutiner ikke ga tilfredsstillende grenser for den enkelte saksbehandlerens kontrollhandlinger. Dette gir en uakseptabel risiko for at det blir iverksatt tiltak som er i strid med gjeldende regelverk og internasjonale forpliktelser.

Videre ble det avdekket at NAV ikke gir informasjon til de registrerte i tråd med personopplysningslovens bestemmelser. Dette innebærer at personer som har vært underlagt en svært inngripende kontroll, med innhenting og spredning av personopplysninger, aldri har fått informasjon om dette. Det undergraver den enkeltes rett til kunnskap og mulighet til å utøve rettigheter som registrert, blant annet ved å kunne få opplysninger rettet.

Det viste seg også at informasjonssikkerheten rundt de aktuelle opplysningene var svært mangelfull. Det var for mange ansatte i enheten som hadde tilgang til for mange saker. Det var heller ikke etablert tilfredsstillende tiltak for å hindre uautorisert utlevering av opplysninger ut av enheten og etaten.

Datatilsynet fattet en rekke pålegg overfor NAV Kontroll. Ingen av dem er påklaget.

### *Politiets innhenting av opplysninger fra førerkortregisteret og passregisteret*

Politidirektoratet og Statens vegvesen har i lang tid levert ut opplysninger fra passregisteret og førerkortregisteret til politiets etterforskning, typisk fotografier i forbindelse med automatisk trafikkontroll. Datatilsynet har ved flere anledninger kritisert etatene for å ha levert ut opplysningene uten å ha forsikret seg om at straffeprosesslovens vilkår for utlevering var oppfylt.

Datatilsynet valgte å følge opp praksisen i etatene, noe som endte med varsel om vedtak i begge tilfellene. Som en følge av dette besluttet både Politidirektoratet og Statens vegvesen selv å endre sine rundskriv og interne rutiner for utlevering av personopplysninger til politiet i forbindelse med etterforskning av enkeltsaker. Datatilsynet avsluttet derfor tilsynssakene uten å fatte vedtak.

## Offentlig sektor

Det offentlige er den sektoren i Norge som behandler størst mengde personlig informasjon. Mange av statens og kommunenes oppgaver tar utgangspunkt i rettigheter eller plikter for borgeren, noe som forutsetter en utstrakt bruk av personopplysninger.

Gjennom flere år har resultater fra Datatilsynets aktiviteter overfor kommuner og fylkeskommuner vist store utfordringer knyttet til kravene i personopplysningsloven om internkontroll og informasjonssikkerhet. Kommunene har gjennomgående hatt for dårlig oversikt over hvilke personopplysninger de behandler og hvilket regelverk som gjelder for behandlingen av dem. Dette underbygges også av erfaringene fra Datatilsynets klagesaksbehandling og tilsynsvirksomhet. Jevnlige avdekkes det svikt i offentlig sektors behandling av personopplysninger, for eksempel ved at sensitive opplysninger havner i postjournalen.

Offentlig sektor er helt avhengig av borgernes tillit. Et viktig bidrag til å bygge tillit er at det gis god informasjon om *hva som benyttes og til hva*, at konfidensialiteten sikres og at regelverket følges når denne sektoren behandler personopplysninger.

Regjeringens digitaliseringsprogram "*På nett med innbyggerne*" slår fast at regjeringens ambisjon er at Norge skal ligge i front internasjonalt når det gjelder å utvikle en digital forvaltning. En videre digitalisering av offentlig sektor fremstår som naturlig, men reiser også utfordringer for personvernet. Sentrale tema i den sammenhengen er sammenstilling og gjenbruk av informasjon, forvaltning av digitale identiteter, elektronisk kommunikasjon med borgeren og etablering av felles tjenester.

Ved økt digitalisering av statlig sektor øker farene for at offentlig informasjon benyttes til ID-tyveri og at statlige tjenester utsettes for ID-svindel. Sikre offentlige nettløsninger, og en god offentlig ID-forvaltning, er vesentlig i denne sammenhengen. Datatilsynet mener at et viktig tiltak vil være at det offentlige sikrer at kvalifiserte digitale ID-er tas i bruk ved samhandling med publikum.

## Hva er gjort på området?

### *Digitalisering av offentlig sektor*

Datatilsynet satte i 2012 i gang arbeidet med å lage en egen strategi for hvordan vi skal forholde oss til regjeringens digitaliseringsprogram "*På nett med innbyggerne*", med hensyn til en best mulig ivaretagelse av personvernet. I strategien skal det nedfelles hvordan vi skal jobbe opp mot programmet og hvordan vi skal prioritere våre ressurser. I denne strategien vil vi også avklare hvordan vi skal jobbe med temaene fellesløsninger, gjenbruk og effektivisering. Strategien lanseres i 2013.

Digitaliseringsprogrammet er preget av at det både er prosesser og aktiviteter som har gått over lang tid (for eksempel Altinn), og av prosesser og aktiviteter som er i støpeskjeen.

Det viktigste for Datatilsynet knyttet til digitaliseringsprogrammet er at vi har et tett og godt samarbeid med de sentrale aktørene i digitaliseringsprosessene både på departements- og etatsnivå,

samt med Kommunenes interesseorganisasjon (KS) når det gjelder norske kommuner. For Datatilsynet er det viktig å gjøre alle aktørene gode på personvern, informasjonssikkerhet og innebygd personvern. Deltakelse sikrer også at Datatilsynet har tilstrekkelig kunnskap om utviklingen. På dette området er dessuten kontakt med og rådgiving til leverandørbransjen en viktig aktivitet. Datatilsynet har i meldingsåret hatt kontaktmøter med flere av de sentrale aktørene i gjennomføringen av digitaliseringsprogrammet.

### *Automatiserte avgjørelser*

Det er en utfordring at offentlig forvaltning i økende grad tar i bruk automatiserte avgjørelser, noe som vil si at vedtak kan treffes uten at en saksbehandler har sett på saken. Dette er for eksempel aktuelt ved beregning av støtteordninger. Mange vedtak i forvaltningen er basert på slike automatiserte prosesser hvor plikter og krav følger av profiler som stat eller kommune har om borgeren.

I meldingsåret ble det i samarbeid med Senter for rettsinformatikk (SERI) ved Universitetet i Oslo gjennomført et prosjekt for en videre analyse og undersøkelse av den enkeltes personvern når det fattes automatiserte avgjørelser i forvaltningen. Elleve offentlige virksomheter ble undersøkt, deriblant NAV, Lånkassen og Husbanken.

Ved automatiserte avgjørelser hentes det opplysninger fra både interne og eksterne registre. Skatteetatens folkeregister benyttes i de fleste systemene. Flesteparten av de spurte forvaltningsorganene forventer mer automatisering innen sitt forvaltningsområde i tiden fremover. Dette vil være i samsvar med forvaltningspolitikken og digitaliseringsprogrammet. Resultatene av undersøkelsen viser at systemer som er etablert før år 2000 vil erstattes av nye og mer automatiserte systemer.

Rettigheter som innsyn, informasjonsplikt, kvalitet på opplysningene og retten til å kreve manuell behandling peker seg ut som særdeles viktige når det gjelder automatisert saksbehandling. Når det gjelder forvaltningens enkeltsaksbehandling er det svært sjelden saker om feil i automatiserte avgjørelser blir tatt opp for domstolene. Dermed kan rettssikkerhetskrav som at vedtak er korrekte og forutsigbare, være vanskelige å etterprøve.

For å kunne ivareta sine rettigheter etter loven er det nødvendig at den registrerte har kunnskap om de automatiserte prosessene i forvaltningen. Slik kunnskap kan skje gjennom aktiv bruk av egen innsynsrett, eller gjennom pålagt informasjonsplikt for det enkelte forvaltningsorgan. Personopplysningsloven pålegger en slik plikt, men med det viktige unntaket at den registrerte ikke har krav på slik informasjon når behandlingen skjer med uttrykkelig hjemmel i lov. Og bruk av automatiserte avgjørelser skjer som regel ikke uten at dette er fastsatt i lov. Den registrerte er dermed fratatt nødvendig informasjon for å kunne etterprøve denne type forvaltningsvedtak.

Rapporten synliggjør at mer bruk av automatiserte avgjørelser betyr dårligere rettigheter for de som er registrert. Dette kunne forvaltningsorganene ha løst for eksempel gjennom aktiv informasjon på sine nettsider.

## Funn fra tilsyn

### *Oppfølging av kommuneundersøkelsen*

I kommuneundersøkelsen 2010/2011 avdekket Datatilsynet at kommunal sektor har utfordringer når det gjelder etterlevelse av personopplysningsloven. Med bakgrunn i undersøkelsen ble det gjennomført tilsyn med fem kommuner i Troms. Tilsynene viste generelle mangler med internkontroll og informasjonssikkerhet for samtlige av de kontrollerte kommunene.

I tillegg har Datatilsynet fulgt opp kommuner som ikke besvarte kommuneundersøkelsen, eller som svarte at de ikke hadde etablert internkontroll og heller ikke hadde en plan om dette. Oppfølgingen endte med at Datatilsynet fattet vedtak om tvangsmulkt for seks kommuner knyttet til implementering av internkontroll.

### *Tilsyn med statlige virksomheter*

Høsten 2012 gjennomførte Datatilsynet fem tilsyn rettet mot statlige virksomheter under temaet internkontroll og informasjonssikkerhet. Følgende fem virksomheter ble kontrollert: Utdanningsdirektoratet, Utlendingsnemnda, Havarikommisjonen, Direktoratet for arbeidstilsynet og Direktoratet for naturforvaltning.

Det var stor variasjon i virksomhetenes natur; fra Utlendingsnemnda som har store databaser med personopplysninger og til for eksempel Havarikommisjon som ønsker å registrere færrest mulig personopplysninger. Tilsynene viste store forskjeller i kunnskapen om personvernregelverket.

Av de fem virksomhetene hadde to stykker gode og dokumenterte rutiner for internkontroll og informasjonssikkerhet. De andre manglet rutiner for internkontroll.

Når det gjaldt informasjonssikkerheten hadde enkelte mangel på ledelsesforankring. Andre igjen hadde mangelfulle sikkerhetstiltak, for eksempel ved bruk av usikre kommunikasjonskanaler slik som usikret e-post. Flere var dårlige på etablering av databehandleravtaler og hadde mangelfull gjennomføring og oppfølging av risikovurderinger.

## Internasjonalt samarbeid

Utviklingen på personvernområdet er sterkt påvirket av den internasjonale utviklingen og av regelverk fastsatt utenfor Norge. I 2012 utarbeidet Datatilsynet en strategi for sitt internasjonale arbeid. I strategien er det uttalt at vi skal fortsette å være aktive på den internasjonale arenaen for å påvirke rettsutviklingen og for å få kunnskap om endringer og utviklingstrekk som vil kunne utfordre oss i fremtiden.

Regelverket Datatilsynet forvalter er basert på et EU-direktiv. Direktivet er igjen tuftet på europeiske og globale menneskerettigheter. Datatilsynets forvaltning må, i tillegg til de føringene som lovgiver har gitt, i rimelig grad forholde oss til forvaltningspraksis hos øvrige personvernmyndigheter. Mange av virksomhetene som behandler personopplysninger er multinasjonale selskaper, og personopplysninger utveksles i stadig større omfang utover landegrensene. Mye av det internasjonale arbeidet tar nettopp utgangspunkt i et ønske om en enhetlig forvaltning av direktivet, samt det å utveksle synspunkter og erfaringer.

Ettersom Norge ikke er medlem av EU er Datatilsynets påvirkning av EU-prosessene dels avhengig av egen aktivitet og dels av andres. Dette gjør det særlig viktig med et tett og forpliktende samarbeid mellom de nordiske landene.

Datatilsynets deltagelse i ulike internasjonale fora er nødvendig for å sikre et godt personvern i Norge, og det pågår en rekke prosesser tilsynet kan delta i, både i Europa og globalt. Det er imidlertid viktig å være målrettet og ha klare prioriteringer på vårt arbeid. Dette bør styres *av hvor vi kan påvirke og hvor vi kan lære*.

Vi ser at teknologitrender treffer Norge og Datatilsynet umiddelbart. Mange av disse trendene kommer fra andre deler av verden, men Norge ligger i forkant når det gjelder å ta i bruk ny teknologi og når det gjelder deltagelse på nye sosiale plattformer. Politisk sett er EU mest sentralt for vårt arbeid, men USA er den store driveren i teknologiutviklingen, og en stor del av selskapene som utfordrer norske borgeres personvern er lokalisert utenfor både Norge og EU. Det er derfor helt sentralt at vi i Datatilsynet holder oss informert om den internasjonale utviklingen og har god kompetanse både om internasjonale prosesser og utviklingen generelt. Dette gjør det også viktig å jobbe aktivt overfor store internasjonale aktører direkte, slik det blant annet har blitt gjort med Facebook.

### EU-kommisjonens forslag til nye personvernregler

I januar la EU-kommisjonen frem et forslag om å erstatte dagens personverndirektiv med en ny personvernforordning (lov). Kommisjonens formål er todelt; man ønsker et regelverk som er mer tilpasset vår digitale nåtid og fremtid enn det gjeldende direktivet fra 1995, og det er et ønske om økt harmonisering på personvernområdet i Europa. I dag er det store nasjonale variasjoner i hvordan personverndirektivet er implementert, og særlig for virksomheter som opererer i flere land er dette tungvint.

Forslaget er svært omfattende, og det er vanskelig fullt ut å se konsekvensene av det som er foreslått. Siden den norske personopplysningsloven er bygget på dagens personverndirektiv vil det få konsekvenser også i Norge dersom dette forslaget blir vedtatt. Selv om det samarbeides godt mellom

personvernmyndighetene i Europa på stadig flere områder, er det en utfordring at det gjeldende personvernregelverket er tolket ulikt i de forskjellige land, i tillegg til at det ikke legger føringer på *hva* det skal samarbeides om og *hvordan*.

#### *Nytt, overordnet personvernorgan*

Kommisjonen har kommet med et forslag om å gjøre samarbeidet mindre tilfeldig ved å opprette et nytt, overordnet personvernorgan; European Data Protection Board (EDPB). Det er et godt forslag, men Datatilsynet frykter at det bare er tilsynsmyndighetene i medlemslandene som skal være representert i EDPB. Det norske Datatilsynet risikerer da å havne helt på sidelinjen i det felleseuropeiske personvernarbeidet, og kan risikere å bli bundet av beslutninger som vi ikke har kunnet påvirke. Et norsk krav bør derfor være at så lenge EUs nye personvernlovgivning blir gjeldende rett i Norge, må Norge være representert med fulle rettigheter i EDPB.

#### *Enhetlig praktisering av loven*

I forslaget foreslås egne regler som skal sikre at loven praktiseres likt i de ulike EU-landene. Dette er en viktig forutsetning for at forordningen skal fungere etter hensikten. EDPB vil spille en sentral rolle som koordinator og pådriver for å oppnå enhetlig praktisering. Prosessen som foreslås er imidlertid svært omfattende og byråkratisk. Datatilsynet frykter at dette vil forsinke prosessene og at de ulike medlemslandene vil forsøke å unngå å bruke prosessreglene forordningen legger opp til. Vi har derfor tatt initiativ til et nordisk samarbeid for å legge fram et alternativt forslag til en prosess for enhetlig praktisering av loven.

#### *For mye makt til kommisjonen*

Datatilsynet reagerer dessuten på at kommisjonen gis forskriftskompetanse på nesten en tredjedel av forordningsforslagets innhold, inkludert innhold som er av stor materiell betydning. Som ikke-medlem har Norge langt færre muligheter til å påvirke forskriftsarbeid enn det medlemsland har. I tillegg gis kommisjonen mulighet til å overstyre nasjonale personvernmyndigheter i enkeltsaker for å sikre harmonisering og konsistens. Dette truer personvernmyndighetenes uavhengighet.

#### **Artikkel 29-gruppen (Art. 29 Data Protection Working Party – WP 29)**

Denne gruppen er den øverste rådgivende forsamlingen for EU-kommisjonen i spørsmål om personvern og informasjonssikkerhet, og avgir uttalelser om tolkning av personverndirektivet. Norge er observatør i denne gruppen, som består av lederne hos personvernmyndighetene i EU- og EØS-land. Observatørstatusen kommer av at Norge ikke er medlemsland, og gjør at vi ikke har stemmerett. I 2012 har det vært avholdt fem møter i gruppen.

Tidlig i meldingsåret informerte Datatilsynet artikkel 29-gruppen om det nordiske initiativet overfor Facebook, og det ble vist til rapporten vi hadde skrevet i 2011 om sosiale medier. Det er mange andre lands myndigheter som har tilsvarende utfordringer med store internasjonale aktører, og inntrykket er at det er interesse for hva vårt initiativ kommer til å resultere i.

Mye av arbeidet i undergruppene til artikkel 29-gruppen var i meldingsåret preget av forventningen til det nye forslaget til forordning som var varslet fra EU. Det ble i løpet av året produsert en rekke uttalelser om sentrale personverntemaer, slik som hva som skal regnes som sensitive data, underretning til den registrerte, bruk av biometri, samtykkeinstituttet og om tilsynsmyndighetenes



fremtidige rolle på en internasjonal arena. Innen helseområdet er et arbeid med en europeisk kjernejournal i gang, og det er satt ned en egen undergruppe som skal se på dette.

I tillegg har artikkel 29-gruppen rettet en god del oppmerksomhet mot utfordringer knyttet til Internett. Norge er fullverdig medlem i **Technology Subgroup**, en undergruppe av artikkel 29-gruppen, og er slik sentralt plassert i arbeidet som foregår der. Gruppen er meget aktiv innenfor teknologispørsmål og representerer en viktig del av tilsynets internasjonale nettverk. I gruppen deler tilsynet sine oppfatninger, men får også god innsikt i øvrige lands vurderinger i teknologispørsmål. Eksempler på hva som har vært behandlet i 2012 er spørsmål knyttet til adferdsstyrt reklame, lokaliseringstjenester på mobiltelefoner knyttet til Internett (særlig Apples lagring av slike opplysninger), Google Street View, Facebook og andre sosiale nettsamfunn, lekkasjen fra / hackingen av Sony sine servere, samt sporing på nett.

### *Sporing på Internett – Do Not Track-standarden*

Vi blir alle sporet når vi surfer på Internett, og det er mulig for bedrifter å spore enhver bevegelse vi gjør på deres nettsider. Dette har internasjonal interesse, og Datatilsynet deltar i drøftingen rundt dette gjennom sin representasjon i Technology Subgroup.

En såkalt Do Not Track-standard vil fungere ved at det gis beskjed fra brukerens utstyr eller nettleser om hvilke preferanser brukeren har når det gjelder sporing, for eksempel om brukeren ønsker å gi fra seg opplysninger for å få relevant reklame. Do Not Track-standarden vil også bestemme hvordan tilbydere må forholde seg til brukerens valg.

I begynnelsen av 2012 var det et stort håp, blant annet hos EU-kommisjonen, om at man skulle greie å etablere en tilfredsstillende Do Not Track-standard. I oktober ble det lagt frem et utkast til standard, men standarden var etter EU-kommisjonens syn for svak. Prinsippet skulle være at man skulle slippe unna sporing, noe som ennå ikke var tilstrekkelig ivaretatt. Det er også fremdeles bekymring for at Do Not Track ikke blir satt som et standardvalg i nettleserne, og for at unntakene som er foreslått fra standarden blir for omfattende. Det kan dermed fremdeles være langt frem til vi får en tilstrekkelig god Do Not Track-standard.

Noen aktører har allerede lagt ned arbeid for å muliggjøre at brukerne ikke blir sporet, og Do Not Track er et av standardvalgene i Microsofts Internet Explorer 10 på Windows 8. Dette har møtt kritikk fra markedsføringsselskaper som hevder at bruk av Do Not Track må være et valg gjort av brukeren og ikke et standardvalg.

Problematikken rundt sporing på Internett har lenge vært en utfordring, og reglene om personvern og databeskyttelse på nett ble styrket i forbindelse med endringen i ekomdirektivet i 2009: Internettbrukerne skulle bli bedre informert om informasjonskapsler (cookies) og om hva som skjer med deres personlige data, og de skulle lettere kunne utøve kontroll over opplysninger om seg selv.

Artikkel 29-gruppen laget i meldingsåret en egen opinion om håndteringen av informasjonskapsler i de tilfellene der samtykke ikke er nødvendig. Artikkel 29-gruppens arbeid rundt hvordan informasjonskapsler kan benyttes og en Do Not Track-standard vil fortsette i 2013.

### Personvernvilkår på nettjenester

Artikkel 29-gruppen har i 2012 koordinert et arbeid der det har blitt sett nærmere på om personvernvilkårene til Facebook, Google og Microsoft er i samsvar med EUs personverndirektiv. Datatilsynet har gitt innspill til dette arbeidet gjennom sin deltagelse i Technology Subgroup.

Facebook, Google og Microsoft har hver for seg etablert en rekke tjenester. Spørsmålet er blant annet om personopplysninger gitt til én tjeneste, blir brukt for å bedre eller gjennomføre andre tjenester. Dette skjer muligens uten at det blir innhentet et logisk og klart samtykke eller uten at det finnes hjemmel for slik bruk av personopplysningene.

Overfor Google har artikkel 29-gruppen vært kritisk til at selskapets nye personvernvilkår åpner for utveksling av personopplysninger mellom de ulike Google-tjenestene. Artikkel 29-gruppens arbeid med å se nærmere på Googles personvernvilkår blir koordinert av personvernmyndighetene i Frankrike, Commission nationale de l'informatique et des libertés (CNIL).

Microsoft har endret sine personvernvilkår betydelig etter sommeren. For Europa har Microsoft utgangspunkt i Luxembourg, det er dermed dette landets personvernlovgivning som vil gjelde for Microsofts personvernvilkår.

Dette er et område som også vil få oppmerksomhet i 2013.

### Oppfølging av Facebook

I desember 2011 publiserte de irske personvernmyndighetene sin tilsynsrapport for Facebook Irland. Rapporten inneholdt en detaljert kravliste over anbefalte løsninger for Facebook. Det ble lagt opp til en gjennomgang av implementeringen i juli 2012, og det ble konkludert med at de fleste anbefalingene hadde blitt tilfredsstillende implementert hos Facebook. Dette gjelder spesielt områdene for bedre åpenhet overfor brukerne, bedre kontroll over innstillinger, klare lagringstider for sletting av personopplysninger og en utvidet mulighet for brukerne til å slette elementer, samt brukernes tilgang til egne personopplysninger. I noen tilfeller har Facebook gått lenger enn de kravene som i utgangspunktet var blitt satt for å kunne imøtekomme kravene også fra andre lands personvernmyndigheter.

Gjennomgåelsen av Facebook var kun en vurdering på et gitt tidspunkt. Endringer og utvikling av Facebooks tjenester overfor brukerne og bruk av personopplysninger for reklamevirksomhet vil fortsette å utfordre personvernet. Dette medfører et behov for en fremtidig kontinuerlig involvering og arbeid for de irske personvernmyndighetene.

Det norske Datatilsynet har i løpet av meldingsåret også hatt aktiv dialog med Facebook, dette er omtalt nærmere under *Internett og telekommunikasjon*.

### Berlin-gruppen

Datatilsynet er fullverdig medlem i denne globale gruppen som arbeider med personvernproblemstillinger knyttet til teknologi. Det er bred deltakelse fra alle deler av verden. Deltakelsen i denne gruppen bidrar til at vi får kunnskap om aktuelle problemstillinger på et tidlig stadium. Gruppen utøver også påvirkning på prosesser i EU, og den er et viktig møtested for å drøfte personvernutfordringer. Berlin-gruppen lager felles anbefalinger om hvordan ulike utfordringer kan

løses. I meldingsåret var gruppen spesielt aktiv i forhold til nettskytjenester, sosiale nettverk og overvåkingstiltak innen telekommunikasjonssektoren.

Datatilsynet deltar aktivt i Berlin-gruppens arbeid. I 2012 har vi holdt innlegg om vårt arbeid i forbindelse Google Analytics og Facebook, samt sakene om Microsoft og Googles nettskytjenester. Vi har dessuten gitt innspill til gruppens memorandum om nettskytjenester.

### Nordisk samarbeid

Datatilsynet var i mai 2012 vertskap for en utvidet nordisk datatilsynskonferanse. Lederne for de nordiske datatilsynsmyndighetene samles en gang i året for å utveksle erfaringer fra egen virksomhet. I år var møtet utvidet til også å omfatte saksbehandlere innen de ulike fagdisiplinene. Representanter fra Finland, Sverige, Danmark, Island, Færøyene, Åland og Norge deltok.

De nordiske landene har mange fellestrekk i sin regulering av personvern, og det nordiske møtet er et viktig samlingspunkt for å finne felles posisjoner som kan trekkes inn i det internasjonale arbeidet. Det er også verdifullt å se hvordan like utfordringer løses i nabolandene. Hovedtemaet for møtet i meldingsåret var EU-kommisjonens forslag til ny personvernforordning, og hvordan fremtidens regelverk kan komme til å påvirke personvernmyndighetenes nasjonale og internasjonale oppgaver. Mulighetene for fremtidige felles tilsyn ble blant annet også diskutert.

### Den internasjonale personvernkonferansen

I 2012 ble den internasjonale personvernkonferansen avholdt i Uruguay. Datatilsynet deltok med to representanter. Konferansen var todelt; en åpen del hvor academia og næringsparter deltar sammen med personvernmyndighetene, og en lukket del for personvernmyndighetene. Hovedtema for den lukkede delen var personvernprofiler. De deltakende myndighetene vedtok tre dokumenter med prinsipper for hvordan personvernet skal ivaretas for henholdsvis personprofiler, nettskytjenester og The future of privacy. Sistnevnte peker på internasjonalt samarbeid og informasjonsdeling som sentralt for i fremtiden å kunne ivareta personvernmyndighetenes oppdrag.

### Global Privacy Enforcement Network – GPEN

GPEN er et samarbeidsforum for personvernmyndigheter. Datatilsynet ble medlem i 2012, og deltok på et møte i forumet i sammenheng med den internasjonale personvernkonferansen. GPEN legger til rette for informasjonsutveksling og det planlegges koordinerte aktiviteter som myndighetene kan velge å delta i.

### Ansvarlig tilsynsmyndighet – Binding Corporate Rules

I 2012 tok Datatilsynet oppdraget som ansvarlig tilsynsmyndighet (lead authority) i forbindelse med den første norske søknaden om "Binding Corporate Rules" (BCR). BCR er et instrument som skal sikre fri flyt av personopplysninger internt i et konsern på en måte som er i tråd med norske og europeiske personvernregler. Det er et omfattende arbeid å stå som ansvarlig for denne godkjennelsesprosessen, men det er en utfordring Datatilsynet tar for å sikre seg kompetanse på området for fremtiden.

## 4. Om Datatilsynet - organisasjon og ressursbruk

Datatilsynets verksemd kan i hovudsak delast inn i to hovudroller: Vi er eit forvaltnings- og tilsynsorgan som treffer enkeltvedtak og utøver myndigheit etter personvernlovgivinga. Samtidig har vi ei ombodsrolle ved at vi skal ta vare på og styrkje personvernet som samfunnsinteresse. I den samanhengen skal vi oppfordre til debatt og merksemd rundt personvernspørsmål, noko som også vil seie å kritisere private aktørar og offentlege styresmakter når dei etter vår vurdering utfordrar personverninteressene. For å gjennomføre dette har vi fire overordna verkemiddel; tilsynsverksemda, saksbehandlinga, kommunikasjonsverksemda og organisatoriske verkemiddel. Organisatoriske verkemiddel er for eksempel personvernombodsordninga og deltaking i råd og utval.

Gjennom tilsynsverksemda og saksbehandlinga tileignar tilsynet seg erfaring og kunnskap om korleis personvernomsynet blir teke vare på i ulike sektorar og bransjar. Denne kompetansen er avgjerande for å fylle ombodsrolla vår på ein god måte. Kommunikasjonsverksemda knyter seg i større grad til gjennomføringa av begge rollane; vi skal rettleie og informere om personvernlovgivinga og forvaltningspraksisen, men samtidig skal vi skape debatt og påverke.

Datatilsynets overordna målsetjing er å ta vare på og utvikle eit best mogeleg personvern for norske borgarar. Ved å analysere og planleggje ut frå kunnskapen vi får frå tilsynsverksemda, saksbehandlinga og publikumskontakten, kan vi setje i verk spissa informasjonstiltak, ta initiativ til regelverksutvikling eller opplæringstiltak, oppmode til debatt eller gjennomføre andre aktuelle tiltak.

Ei kontinuerleg merksemd rundt korleis vi kombinerer roller og verkemiddel er slik viktig for å oppnå eit samfunn som i størst mogeleg grad tek vare på personvernet.

### Tilsynsverksemda

Datatilsynets mål for tilsynsverksemda er å kontrollere at lover og reglar blir følgde ved å drive tilsynsarbeid av god kvalitet, basert på risikoanalyse.

I 2012 gjennomførde vi tilsyn innan ni ulike bransjar, fordelt på våre prioriterte område. Det blei gjennomført 55 tilsyn, noko som er ein auke frå 38 tilsyn i 2011.

Det som blir rekna som tilsyn her er ein kontroll med om regelverket vert følgd, og der det blir utarbeidd ein rapport i etterkant. Tilsyn blir normalt gjennomført ved at to medarbeidarar frå Datatilsynet besøker verksemda. Når det er formålstenleg blir nokre tilsyn gjennomført skriftleg. I meldingsåret blei 45 av tilsyna gjennomført hos verksemdene, mens ti blei gjennomført via brev.

Tilsyn gjennomført i 2012 fordelt på områder:

Bransje	Tal på tilsyn
I Telekommunikasjon, Internett og DLD	7
II Samferdsel	-
III Arbeidsliv	10
IV Økonomi og finans	6
V Helse	5
VI Justis	2
VII Offentleg sektor	13
VIII Kameraovervaking	4
IX Internkontroll og informasjonstryggleik	4
Etterkontrollar	4
<b>Sum</b>	<b>55</b>

Datatilsynet gjennomfører også ein omfattande kontroll gjennom ordinær saksbehandling, blant anna gjennom oppfølging av klager frå publikum og ved hjelp av avviksmeldingar. Slike saker kjem ikkje fram av denne oversikta.

For ei fullstendig oversikt over alle tilsynsobjekta, sjå *vedlegg A*. Viktige funn frå tilsyn er omtalt i kapittel 3 om utvalde område.

### Trender

Å bruke funn frå tilsyna for å skildre trendar føreset lik tematikk over fleire år. Dette er krevjande med ei avgrensa mengde tilsyn, og med varierende sektorval og tematikk for tilsyna. Alle rapportane var dessutan ikkje klare ved årsskiftet.

Ein generell trend er likevel manglande kjennskap til pliktene rundt internkontroll og informasjonstryggleik. Dette er identifisert blant anna gjennom tilsyna hos statlege verksemder og i kommuneundersøkinga som blei gjennomført i 2010/2011. Funna er nærmare omtalte i kapittel 3 under *Offentleg sektor*.

### Om bruk av tilsyn for å undersøkje og avklare praksis

Datatilsynet bruker tilsynsverksemda for å undersøkje og avklare praksis. I mange tilfelle vil praksisen vere relativt lik i mange verksemder, og tilsyn med nokre få verksemder kan slik vere tilstrekkeleg for å eventuelt arbeide vidare med sektoren dersom avvik blir avdekt. Frå 2012 kan vi trekke fram følgjande:

**Kameraovervaking ved bank i butikk.** Det blei gjennomført tre tilsyn der sentrale tema var ansvar og lagringstid, noko som er ulikt for bank- og butikkverksemda. Vurderingane som følgjer av tilsyna vil ein så kunne overføre til eit stort tal verksemder.

**Lyddopptak ved call-senter.** Tilsyn og dialog med aktørane, inklusive bransjeforeininga, vil følgjast opp ved at rettleiinga som er tilgjengeleg på nettsidene våre blir revidert. Denne rettleiinga skal vareta både personvernet og behovet verksemda har for opptak.

**Vedvarande kameraovervaking i taxiar.** To taxiselskap blei kontrollerte. Vurderingane i sakene er ikkje ferdige, men vi legg til grunn at sakene vil få konsekvensar for korleis vedvarande kameraovervaking eventuelt skal etablerast i taxiar.

### Om bruk av funn frå tilsyn

Funn frå tilsyn blir i fyrste rekkje samla og systematisert i dei individuelle tilsynsrapportane.

Førebelse rapportar blir sende til tilsynsobjektet, tilbakemeldingane blir vurdert og det blir utforma ein endeleg rapport. Alle endelege rapportar blir publiserte på Datatilsynets nettsider slik at andre aktørar i tilsvarande bransjar kan lese om relevante funn. Vidare stadfestar rapportane tilsynet sin forvaltningspraksis innan dei aktuelle områda. Funna blir òg brukt i dialog med bransjeforeningar som igjen tek utfordringane vidare med medlemene sine.

Eksempel på oppfølging som allereie er gjennomført eller som er under planlegging:

- Funn som er knytte til mobilapplikasjonar skal kommuniserast tilbake til næringa, og vil inngå i arbeidet vårt både nasjonalt og internasjonalt. Miljø der applikasjonar blir utvikla, skal etter planen følgjast opp for å påverke dei til å arbeide etter prinsippa for innebygd personvern.
- Funn frå tilsyna mot nokre utvalde politiske parti vil bli kommunisert til alle parti når konklusjonane er klare.
- Funn frå tilsyna i kommunane blir kommuniserte tilbake til sektoren, samt blir teke med i diskusjonar om verkemiddelbruk overfor sektoren.
- På bakgrunn av tidlegare tilsyn bad Datatilsynet i 2012 Helsedirektoratet om ei tolking av dei rettslege rammene for kvalitetsregister. Svaret vi fekk vil bli brukt i arbeidet vårt framover, og er kommunisert til sektoren ved hjelp av personvernomboda.
- Funn frå tidlegare tilsyn innan helseforskning var tema for Datatilsynets dialog med dei Regionale Ethiske Komiteer (REK). Funna er også presenterte for sektoren.

## Juridisk saksbehandling

Datatilsynets mål er at det juridiske arbeidet skal kjenneteiknast av god juridisk metode, klarleik og høg kvalitet.

Saksbehandlninga i Datatilsynet er definert til å vere alle aktivitetar knytte til spørsmål frå offentlege og private verksemder, samt frå enkeltpersonar. Spørsmåla kjem både via brev, e-post og telefon.

Datatilsynet erfarer at fleire saker er meir komplekse enn tidlegare og at problemstillingane blir fleire og meir samansette. Ein trend innan helseforskning er til dømes at det er ønskeleg med kopling mellom fleire og fleire opplysningar på individnivå. Såkalla registerstudiar er store studiar er baserte på opplysningar frå ulike register. Opplysningane blir så kopla saman og brukte i forskingssamanheng. Desse studiane kan omfatte svært mange personar, og Datatilsynet har sett fleire slike studiar no enn tidlegare.

I 2012 har vi òg sett nærmare på praksisen vår rundt konsesjonar for helseregister som går over lange tidsrom. Vi har sett på grensa for Datatilsynets kompetanse, opp mot helseregisterlovens formalkrav til oppretting av permanente helseregister. Fleire av konsesjonane Datatilsynet har gitt dei siste åra kan tyde på at nokre av registera som var meldt å vere tidsavgrensa, ikkje er det i praksis. Kva dette vil ha å seie for Datatilsynets framtidige praktisering vil avgjerast i 2013.

Internasjonaliseringa gjer seg òg gjeldande i dei sakene vi mottek. Det er stadig fleire behandlingsansvarlege som nyttar underleverandørar og partnerar i utlandet, og stadig fleire også utanfor EU/EØS. Det er etablert forskjellige instrument for at personopplysningar ikkje blir brukte til anna enn det som er avtalt. Eit slikt instrument er til dømes Safe Harbour-avtalen når det gjeld utlevering av opplysningar til USA. Alle slike mekanismar baserer seg på tillit mellom partane, men utfordringa er at det er vanskeleg å føre kontroll med kva som skjer i andre delar av verda.

### Prioriteringar

I meldingsåret har det blitt jobba systematisk med prioritering av innkomne saker og spørsmål. Nokre enkeltsaker og nokon type saker har derfor ikkje gått gjennom ei fullstendig saksbehandling. Vi har for eksempel vurdert om enkeltspørsmål indikerer ein større systemfeil i ei aktuell verksemd eller bransje, eller om det er ei isolert og enkeltstående sak.

Alle som vender seg til Datatilsynet skal likevel få eit svar. Hovudforskjellen er at vi ikkje går inn i sakene som ved ordinær saksbehandling, men at vi gir eit svar av meir rettleiande karakter. Målet er då å setje borgarane i stand til å ta vare på sitt eige personvern.

Prioriteringane har også vore styrande for kva for nokre saker som vi har gått grundigare inn i, og kva for nokre verksemder vi har valt gjennomføre tilsyn hos. I samband med eit prosjekt om kontroll i arbeidslivet tok vi til dømes opp saker til behandling som vi elles ikkje ville ha prioritert.

### Dokument og saker

Det blei journalført til saman 4 858 dokument i meldingsåret. Av desse var 2 646 innkomne dokument som hovudsakleg gjekk gjennom full sakshandsaming. Dette er ein nedgang samanlikna med året før, men som ein ser av tabellen under har mengda sendte dokument auka.

Det blei oppretta 1 220 nye saker i 2012, mot 1 345 året før. Mange som tek kontakt med Datatilsynet ønskjer enkle råd og rettleiing om korleis dei kan gå vidare med saka si. Det er betre ressursbruk og betre service å gi eit kjapt og uformelt svar, framfor å ta saka opp til full saksbehandling. Mykje av forklaringa på nedgangen i registrerte saker skuldast nett dette.

Oversikt over alle journalførde dokument hos Datatilsynet i 2012:

	2010	2011	2012
<b>Dokument inn</b>	3 111	2 740	2 646
<b>Dokument ut</b>	3 184	2 138	2 212

### *Klager på vedtak*

I meldingsåret blei det klaga på 35 av Datatilsynets vedtak. I tre av desse sakene blei vedtaket omgjort eller endra, og tre saker blei avslutta etter å ha rettleidd klagaren. 17 av sakene er framleis til behandling, mens resten blei sende til Personvernemnda.

### *Innsynskrav*

I 2012 handterte tilsynet krav om innsyn i til saman 2 826 dokument. Av desse blei det bedt om innsyn i 2 029 dokument via Offentlig Elektronisk Postjournal (OEP), mens innsynskrava som gjaldt dei resterande 797 dokumenta gjekk direkte til arkivtenesta i Datatilsynet. Arkivet handterer alle desse krava saman med den einskilde saksbehandlaren som vurderer dokumenta. Det er viktig for oss at vi har høg kvalitet i vurderinga av kva dokument vi vel ikkje å levere ut etter krav om innsyn.

Oversikt over innsynskrava via OEP i 2012:

	Tal
<b>Dokument</b>	2 029
<b>Sladda dokument sendt ut</b>	251
<b>Avslag</b>	137

Datatilsynet fekk åtte formelle klager på avslag på innsyn i løpet av meldingsåret. Fire av klagene blei sendt over til klageinstansen som er Fornyings-, administrasjons- og kyrkjedepartementet. Vi fekk medhald i alle. Dei resterande fire sakene blei omgjorde av eige tiltak.

### *Lovbrottsgebyr og tvangsmulkt*

Datatilsynet har som strategisk mål å søkje ein balansert verkemiddelbruk for å oppnå best mogeleg personvern for borgarane. Lovbrottsgebyr og tvangsmulkt er ein del av verkemidla vi har til rådighet, men det er ikkje intensjonen at dette skal vere primære verkemiddel for å få verksemder til å følgje regelverket. Dette skal vere noko vi nyttar i dei mest alvorlege tilfella vi avdekkjer, og på område kor det er viktig å sikre at vedtaka våre blir følgt opp raskt.

I meldingsåret har vi gitt lovbrotsgebyr i sju saker, og vedteke tvangsmulkt i to saker. Ein av desse er framleis ikkje avslutta.



Oversikt over dei lovbrotsgebyra og tvangsmulktene Datatilsynet har gitt i meldingsåret:

Lovbrotsgebyr		Tvangsmulkt	
Posten Norge	kr 100 000,-	Berg kommune	kr 49 000,-
Protector AS	kr 250 000,-	Mestringshuset Øst AS	Ikkje avslutta
St. Olavs Hospital	kr 250 000,-		
Google Inc	kr 250 000,-		
Universitetet i Bergen	kr 250 000,-		
Pegasus Kontroll AS	kr 100 000,-		
Reitan Convenience AS	kr 100 000,-		

Dei to sakene om tvangsmulkt er ein konsekvens av ikkje å svare Datatilsynet som er ei tilsynsstyresmakt. I den eine saka har verksemda svart etter varsel om pålegg, men det var ved årsskiftet framleis ikkje motteke svar frå Mestringshuset Øst.

Forsikringselskapet Protector AS fekk lovbrotsgebyr for ikkje å ha hatt nødvendig konsesjon for å drive forsikringselskap. Dei gjekk ut ifrå at ein konsesjon tilhøyrande eit tidlegare selskap, som no var slått saman med det nye selskapet, var tilstrekkeleg. Tilsynet meinte derimot at ein profesjonell part innan forsikringsbransjen, må klare å sørge for at dei løyva som regelverket krev at verksemda skal ha, er på plass.

St. Olavs Hospital fekk lovbrotsgebyr etter å ha lagra opplysningar – som dei verken hadde grunnlag for å oppbevare eller behandle – heilt sidan 2007. Helseføretaket var gjort merksame på at det måtte innhentast samtykke frå dei registrerte, utan at det hadde blitt teke tak i dette. Alternativet hadde vore å slette eller anonymisere opplysningane, noko som heller ikkje var gjort.

Universitetet i Bergen (UiB) fekk lovbrotsgebyr for ikkje å ha overhalde ein konsesjon om løyve til eit forskingsprosjekt. UiB hadde ikkje kontroll på om konsesjonen blei følgt, noko som førte til at fleire opplysningar blei brukt i det aktuelle forskingsprosjektet enn konsesjonen gav løyve til. Det vert sett på som eit alvorleg brot på personopplysningslova at konsesjonar ikkje blir overhaldne. Konsesjon er eit konkret løyve som mottakaren er kjend med og bør kunne rette seg etter forholdsvis enkelt.

Pegasus kontroll var engasjert av Reitan Convenience (RC) og hadde levert ut opplysningar om ein tilsett i RC til ein annan arbeidsgivar (Plantasjen). Opplysningane gjaldt økonomisk utruskap frå ein tilsett overfor RC. Plantasjen hadde på si side engasjert Pegasus kontroll for å sikre bedrifta mot svikefulle tilsette. Verken Pegasus eller Reitan Convenience hadde grunnlag for å levere ut opplysningar om ein konkret person til Plantasjen, og fekk derfor lovbrotsgebyr. Utlevering av slike sensitive personopplysningar er ikkje mogeleg å reparere overfor den registrerte, og konsekvensen av brotet på personopplysningslova vert derfor sett på som alvorleg.

Googles lovbrotsgebyr er omtalt nærmare i kapittel 3 under *Internett og telekommunikasjon*.

## Høyringar

Ei viktig oppgåve Datatilsynet har som ombod er å gje høyringsfråsegner i saker som har, eller kan ha, konsekvensar for personvernet. I 2012 var tilsynet høyringsinstans i 163 saker. I 58 av desse sakene

blei det gitt konkrete merknader. Dei resterande 105 høyringane blei dei ikkje gitt merknader til, då tilsynet meinte dei ikkje hadde nokon klar konsekvens for personvernet.

Oversikt over høyringssaker dei siste åra:

	2008	2009	2010	2011	2012
<b>Utan merknader</b>	81	75	72	64	105
<b>Med merknader</b>	55	87	51	58	58
<b>Sum</b>	<b>136</b>	<b>162</b>	<b>123</b>	<b>122</b>	<b>163</b>

Datatilsynet hadde merknader til mange høyringssaker innan helse- og omsorgssektoren, mens høyringar knytte til justissektoren var den andre store kategorien. At det er desse to sektorane som dominerer er naturleg. Innan helsesektoren blir det dagleg handtert store mengder sensitive personopplysningar. Det er sett frå vår ståstad, viktig at personvern er ein naturleg del av reglane som styrer korleis slike opplysningar skal handterast. Justissektoren er også storforbrukar av personopplysningar, men til forskjell frå helsesektoren er det også andre omsyn som gjer seg gjeldande her. Opplysningar blir brukte i kontrollføremål og til å etterforske enkeltindivid. Det er derfor svært viktig at reglane er tydelege og sikrar at borgarane veit kva styresmaktene kan gjere. Det er dessutan viktig at personvernet vert tatt godt vare på slik at ein oppnår god balanse mellom personvernet og samfunnet sine interesser og behov.

Høyringar der Datatilsynet har hatt vesentlege merknader er omtalte under dei respektive områda i kapittel 3. Sjå elles ei fullstendig oversikt over alle høyringane Datatilsynet hadde merknader til i 2012 i *vedlegg B*.

### Konsesjon/meldeplikt

Teknologiutviklinga påverkar personvernet på mange måtar, og tilsynet ser at fleire verksemder enn tidlegare er medvitne om at løysingar som blir utvikla også skal ta omsyn til personvernet. Mange verksemder kontaktar Datatilsynet og ønskjer rettleiingsmøte om nye løysingar og tenester. Eit av spørsmåla som då ofte blir stilt er om behandlinga vil krevje konsesjon eller om den utløyser meldeplikt.

Oversikt over konsesjonar Datatilsynet har gitt dei siste tre åra (det vil seie både søknad om konsesjon, forlenging og utviding av eksisterande konsesjonar, samt eventuelle tilleggsprosjekt):

	2010	2011	2012
<b>Konsesjonar</b>	324*	143	132

\*av desse var 215 bankkonsesjonar

Datatilsynet erfarer at konsesjonar som blir gitt mellom anna innan helse og forskning, seinare blir ønskt endra og ofte utvida. Å behandle endringssøknader er hovudsakleg like ressurskrevjande som å behandle nye søknader. Fleire forskingsprosjekt utviklar seg over tid og blir svært omfattande og tidkrevjande å behandle. Vi har derfor sett nærmare på eit par typar konsesjonar i meldingsåret; kvalitetssikringsregister og dei store befolkningsundersøkingane. Målet er å avklare om slike register framleis skal basere seg på konsesjon, eller om dei er blitt permanente og høyrer inn under helseforskningslova.

Meldeplikta inneber at den som ønskjer å setje i gong ei behandling av personopplysningar skal orientere Datatilsynet seinast 30 dagar før behandlinga startar. Meldingane blir lagde inn i ein offentlig tilgjengeleg database. Basen er tilgjengeleg for publikum via nettsidene våre. For vedvarande behandlingar skal meldinga fornyast kvart tredje år. Det er gitt unntak frå meldeplikta blant anna for verksemder som har oppretta personvernombod.

Oversikt over meldingar i meldingsbasen:

	2009	2010	2011	2012
<b>Nye meldingar</b>	3 778	3 693	4 010	2 954*
<b>Meldingar per 31.12 – totalt</b>	9 292	10 055	11 211	10 909

\* Det kom i meldingsåret inn over 2 000 meldingar frå ein leverandør av elektroniske kjørebøker. Per 31.12.2012 er framleis ikkje alle plotta inn.

Trenden er at talet på aktørar som handterer personopplysningar er aukande. Vi har dessutan grunn til å tru at det er mange som ikkje har oppfylt meldeplikta, og at det i realiteten er mange fleire som behandlar personopplysningar. Det syner seg blant anna når vi er på tilsyn. Vi reknar med at dette kjem av ein mangel på kunnskap om kva for nokre krav lova stiller. Dette er noko av det som gjer Datatilsynets rettleiingsteneste viktig, i tillegg til godt informasjonsmateriell på nettsidene våre.

### Rettleiingstenesta

Datatilsynets rettleiingsteneste er eit viktig "lågterskeltilbod". Tenesta handterer e-post og telefonførespurnader frå både enkeltpersonar og private og offentlige aktørar. Eit viktig mål med tenesta er å gjere borgarar og verksemder i stand til å ta eige ansvar for personvernet. Det er grunn til å tru at mange som nyttar tenesta, ville hatt ein høgare terskel for å bruke meir formelle måtar å ta kontakt på.

### Generelt om tenesta

Oversikt over omfanget av spørsmål til rettleiingstenesta (tala baserer seg på manuelle teljingar):

	2006	2007	2008	2009	2010	2011	2012
<b>Telefonar</b>	8 125	7 300	7 070	6 952	7 309	5 196	4 675
<b>E-post</b>	2 711	2 673	3 054	4 401	2 727	2 632	2 175

I 2012 har det vore færre faste personar som har svart på telefon og e-post enn tidlegare år, og ein større del av spørsmåla er svart på av andre i Datatilsynet enn rettleiingstenesta. Det blir det ikkje ført statistikk for, noko som gjer tala i tabellen lågare enn det reelle talet.

Trenden er likevel ganske klar, det synest som om vi får færre spørsmål via telefon og e-post enn tidlegare. Det kan ha samband med at vi i meldingsåret har bygt ut nettsidene våre med typiske spørsmål og tilhøyrande svar. Vi legg òg ut rettleiingsmateriell ved behov. Målet er at nettsidene skal vere det naturlege fyrstevalet når nokon har spørsmål om personvern. Fagavdelingane i tilsynet jobbar derfor tett med informasjonsavdelinga for jamleg å kvalitetssikre informasjonen som er tilgjengeleg på nettsidene.

Når nokon tek kontakt med rettleiingstenesta får dei informasjon og rettleiing om regelverket og kva som står på nettsidene våre, eller dei får ei orientering om kva for andre etatar dei kan ta kontakt med. Kvar einiskild får også eventuell rettleiing i korleis dei sjølve kan følgje opp saka si.

### *Innhaldet i spørsmåla*

Det er nokre område som peikar seg ut når det gjeld spørsmåla til denne tenesta.

Oversikt over kva spørsmåla til tenesta dreier seg om:

E-post			Telefon		
Tema	Totalt	Prosent	Tema	Totalt	Prosent
Arbeidsliv/skule	335	15 %	Arbeidsliv/skule	866	19 %
Kameraovervaking	326	15 %	Ulike typar register	709	15 %
Internett	301	14 %	Kameraovervaking	639	14 %
Ulike typar register	276	13 %	Melding/Konsesjon	510	11 %
Melding/Konsesjon	165	8 %	Internett	388	8 %
Fødselsnummer	147	7 %	Fødselsnummer	277	6 %
Anna	625	29 %	Anna	1 286	28 %
<b>Sum</b>	<b>2 175</b>	<b>100 %</b>	<b>Sum</b>	<b>4 675</b>	<b>100 %</b>

I oversikta ser ein at kategorien **"anna"** representerer ein stor del av spørsmåla til tenesta. Omkring halvparten fell utanfor personopplysningslova, og kan typisk vere spørsmål som fangast av unnataket i personopplysningslova om journalistiske formål, spørsmål om teieplikt (som oftast fell inn under forvaltningslova) eller politiet si behandling av personopplysningar. Anna som hamnar i denne samlekategorien er spørsmål om lydopptak, databehandlaravtale, overføring av personopplysningar til utlandet og informasjonstryggleik.

Spørsmåla i kategorien **arbeidsliv/skule** er hovudsakleg konsentrert om temaa GPS, kameraovervaking, bruk av bilete, kontrolltiltak, e-post, personalmapper og lydopptak. Kontrolltiltak i arbeidslivet kan til dømes vere innføring av inngangskontrollsystem, detaljregistrering av arbeid som blir utført, effektivitetsmålingar, evalueringar og programvarekontroll.

Spørsmåla om **fødselsnummer** kjem i hovudsak frå privatpersonar, og gjeld i stor grad bruk av fødselsnummer i kunderelasjonar eller i kunderegister, men det er òg spørsmål om offentlege etatar og deira bruk av fødselsnummer. Folk er urolege for ID-tjuveri, og dei synest å ha eit ønske om at fødselsnummeret skal vere verna mot spreiding, og reservert dei situasjonane kor det er nødvendig. Ein liten del gjeld sending av fødselsnummer i usikra e-post.

Når det gjeld **Internett** er spørsmåla i hovudsak fordelte på følgjande hovudområde; Facebook, krenkingar på nett, offentleg journal på nett, journalistiske formål, bloggar og andre nettforum, samt nummeropplysningstenester. Dei fleste spørsmåla i denne kategorien gjeld framleis Facebook og handlar om sletting av profil, stenging av konto eller sletting av bilete og annan informasjon. Ein del av desse blir viste vidare til tenesta Slettmeg.no. eller direkte til Facebook.

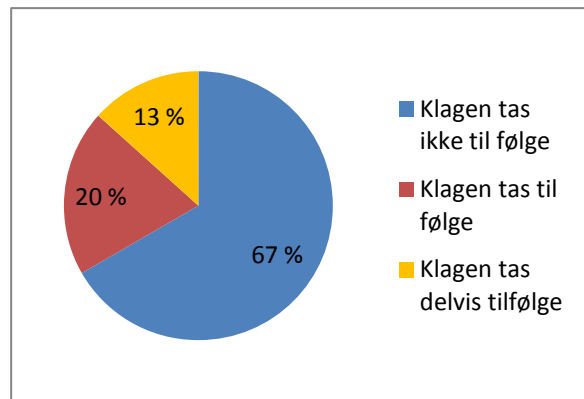
**Kameraovervaking** er ein gjengangar i spørsmåla til tilsynet. Overvaking i burettslag og nabosituasjonar, samt bruk av web-kamera i ulike samanhengar, er typiske situasjonar det kjem spørsmål om. Tilsynet nyttar då standardsvar saman med konkrete råd i kvar enkelt sak.

Spørsmåla om **register** gjeld eit breitt spekter av register slik som helse-, kreditt-, kunde-, medlems- eller offentlege register. Av desse kjem det flest spørsmål om private næringslivsaktørar og deira kredittopplysningsverksemd og kunderegister.

### Personvernemnda

I løpet av 2012 blei det sendt 15 saker over til behandling i klagenemnda. Av sakene som blei behandla i meldingsåret, blei berre tre omgjorde og klagaren gitt fullt medhald.

Omgjeringsprosenten er ei god stadfesting på Datatilsynets arbeid i og med at dei fleste vedtaka blir ståande. Sakene det blir klaga på har dessutan ofte ikkje eit klart svar. Balansen mellom tilsynet og klageinstansen synest derfor å fungere godt, og gir ofte avklaringar på område som er kompliserte og uavklarte.



### Kredittopplysningskonesjonen

Kredittopplysningsbyråas behandling av personopplysningar er underlagt konsesjonsplikt. Det har lenge eksistert ein standardkonesjon som har regulert denne forma for verksemd, men på bakgrunn av fleire enkeltsaker som har vore til behandling hos Datatilsynet og Personvernemnda, blei det tydeleg at standardkonesjonen som var utforma i 2006, var moden for ein revisjon.

Norske kredittopplysningsbyrås foreining klaga på den nye konsesjonen som blei sendt ut i 2009, og tilsynet gjekk i dialog med foreininga om dei omstridde vilkåra. Det blei oppnådd semje om fleire av merknadene, men fire av dei fann Datatilsynet ikkje grunnlag for å kunne godta. Desse gjaldt bruk av adressehistorikk som parameter for betalingsevne (kor mange gonger den registrerte har flytta), tilsvarende bruk av opplysningar om kor mange kredittvurderingar som var gjennomført tidlegare, eigarskap til fast eigedom og opplysningar om fakturaer betalt før forfall.

Datatilsynet mottok tidleg i 2012 ei ny formell klage som omfatta desse fire parametrane som bransjen meinte var relevante. Saka blei derfor sendt til Personvernemnda for klagebehandling. I oktober 2012 mottok tilsynet nemndas avklaring. Klaga blei teken delvis til følge, ved at det blei opna for at kredittopplysningssselskap kan leggje vekt på opplysningar om eigarskap til fast eigedom og opplysningar om fakturaer betalte før forfall (for juridiske personar sin del). Det er likevel framleis ikkje høve til å leggje vekt på flyttevagnar eller talet på gjennomførde kredittvurderingar.

Dei andre mest sentrale vedtaka i nemnda er omtalte under respektive område i kapittel 3. Sjå elles *vedlegg C* for ei fullstendig oversikt over sakene som blei sendt til Personvernemnda i 2012.

### Offentlege granskingskommisjonar

Datatilsynet gav i 2012 konsesjon til to offentlege granskingskommisjonar som var nedsette ad hoc for behandling av personopplysningar. Dette gjaldt 22. julkommisjonen og utvalet for undersøking av politikken overfor tatarar/romanifolket.

Granskingar i regi av slike kommunisjonar reiser ei rekkje prinsipielle og vanskelege problemstillingar knytt til rettsvernet for dei personane som får forholde sine undersøkte. Granskingane blei nærmare klargjorde av Undersøkelseskommisjonsutvalget i 2009 (NOU 2009:9). Utvalet konkluderte med at denne typen undersøkingar bør regulerast i lov, men problematiserte også verksemda. Utgreiinga er ikkje følgd opp av regjeringa.

Dei to konsesjonssøknadene som blei sende til Datatilsynet aktualiserte ei rekkje av dei skildra problemstillingane. Frå ein personvernståstad er det særleg problematisk at granskingsverksemda ikkje er heimla i lov. Ein lovheimel vil sikre at proporsjonaliteten i arbeidet blir sett nærare på og vurdert i ein brei demokratisk prosess. Ein lovheimel vil også kunne skape klarleik for dei registrerte - og særleg for dei som får forholde sine undersøkte av kommunisjonen.

Det er etter vår vurdering ikkje tilfredsstillande at granskingsverksemda blir regulert i enkeltvedtak frå Datatilsynet. Samtidig kan Datatilsynet vanskeleg setje til side ein kongeleg resolusjon som vel ein slik kommunisjon, og tilsynet ser seg i praksis nøydd til å gi kommunisjonen konsesjon.

Tilsynet har skrivne til Justisdepartementet i eit forsøk på å få ei avklaring. Det er nødvendig å få ei avklaring på om granskingskommisjonar skal opprettast i framtida, og kva regelverk som eventuelt skal regulere ei slik verksemd.

### Regelverksutvikling - politiregisterlov og forskrift

Politiregisterlova blei vedteken i 2010, men er framleis ikkje gjeldande. Datatilsynet har vore i referansegruppa for forskriftsarbeidet sidan 2010 gjennom god dialog med Justisdepartementet. Forskrifta var heller ikkje heilt ferdig innan utgangen av meldingsåret.

I høyringa uttrykte vi at vi er tilfreds med at det blir etablert eit regelverk på politiregisterområdet, og ser behovet for at politiregisterlova blir supplert med eit forskriftsverk. Men, forslaget var svært omfattande, og det kan vere ein fare for at regelverket blir vanskeleg tilgjengeleg for dei som skal bruke det.

Datatilsynet hadde planlagt aktivitetar for 2012 i samband endringane i lov og forskrift. Nokre av aktivitetane blei påstarta, men dei blei nedtona då det viste seg at det nye regelverket framleis ikkje gjeld. Det er oppretta dialog med sentrale partar slik som Politidirektoratet og Kripos, og tilsynet har halde innlegg i fellesforum for politiet. Vi har også starta opp arbeidet med å styrkje den interne kompetansen, samt etablere kommunikasjon med personvernrådgivarar i politiet.

### Nye reglar om kameraovervaking

I april 2012 blei regelverket om kameraovervaking endra. Det kom reglar for det som ofte blir kalla dummykamera, i tillegg til at alle vilkåra i personopplysningslova no også gjeld for kameraovervaking, i motsetning til tidlegare. Reglane gjeld også for eventuelle lydopptak og lydoverføringar i tilknytning til biletbehandlinga.

Definisjonen av kameraovervaking blei endra til å omfatte *”utstyr som lett kan forvekslast med ei ekte kameraløysing”*, såkalla dummykamera. For slikt utstyr gjeld lova *”så langt den passar”*. Det inneber at delar av personopplysningslova gjeld sjølv om det faktisk ikkje blir behandla personopplysningar. Datatilsynet har vurdert det slik at inngangsvilkåra i personopplysningslova om kameraovervaking må vere oppfylt dersom det skal monterast dummykamera. Terskelen blir altså den same som for fungerande kamera.

Lovendringa har altså gjort det klart at personopplysningslova gjeld fullt ut når ein skal kameraovervake. Dette gjeld også konsesjonsplikta. Etter lovendringa vil det derfor oppstå konsesjonsplikt når sensitive opplysningar utgjer ein vesentleg del av overvakinga. Dette gjeld likevel ikkje for kameraovervaking som kan ha vesentleg verdi for førebygging og oppklaring av straffbare handlingar. Datatilsynet har ikkje motteke søknader om konsesjon for kameraovervaking etter at lovendringa kom.

## Personvernombod

Ved utgangen av meldingsåret har Datatilsynet registrert 203 personvernombod, noko som er ti fleire enn på same tid året før. Personvernomboda representerer rundt 390 verksemder. Auken er noko mindre enn tidlegare år. Dette kan skuldast at det samanlikna med 2010 og 2011 har vore gjennomført lite marknadsføring av ordninga.

I 2012 har Datatilsynet brukt omtrent eitt årsverk på arbeidet med personvernomboda. Arbeidet består i hovudsak av å arrangere kurs og ein større fagdag for omboda, rettleiing over telefon og e-post, sende ut nyheitsbrev til omboda, samt behandling av søknader.

Det har blitt arrangert blant anna grunnkurs, kurs i informasjonstryggleik og kurs i juridisk fordjuping for både nybyrjarar og vidarekomne. Kursa for omboda har jamt over god deltaking, og tilbakemeldingane frå kursdeltakarane vitnar om at kursa er godt likte. Nokre ombod har ønska seg meir bransjeretta kurs, men dette har ikkje blitt prioritert i 2012.

## Deltagelse i offentlige råd og utvalg

Datatilsynet har en utstrakt kontakt med andre aktører. Nedenfor følger en oversikt over de nasjonale rådene og utvalgene vi er representert i. I tillegg til disse kommer det et stort antall kontaktmøter med sentrale aktører og samarbeid av mer kortvarig art.

### *Standardisering – komitédeltagelse*

Datatilsynet deltar i enkelte komiteer for standardisering der arbeidet har direkte relevans for vårt arbeidsområde. Standarder er førende for virksomhetenes praksis, også når det gjelder behandling av personopplysninger. Formålet med deltakelse i komiteene er å sikre kunnskap om pågående prosesser internasjonalt, påvirke fremtidige rammebetingelser, samt bidra til å påvirke relevante standarder med hensyn til personvern og informasjonssikkerhet. Det er også viktig å få innblikk i hvilken praksis som anses som god.

Tilsynet deltar i fire komiteer. Disse arbeider innen informasjonssikkerhet, intelligente transportsystemer, identitetshåndtering og semantisk web (neste generasjons Internett), og automatisert datafangst.

### *Arbeidet knyttet til forslaget om ny personvernforordning i EU*

Datatilsynet har i meldingsåret tilbudt bistand i ulike sammenhenger når det gjelder arbeidet med EU-kommisjonens forslag til forordning. Tilsynet har blant annet gitt bistand til Fornyings-, administrasjons- og kirke departementet. Vi har også deltatt i Justisdepartementets referansegruppe i forbindelse med nasjonal representasjon i Brussel. Det er dessuten avholdt møter med norske representanter i Brussel. Dette for å sikre at så mange norske interesser som mulig er kjent med tilsynets oppfatning og ønske om å være tilgjengelig med faglige råd.

### *Kontroll og overvåking i arbeidslivet*

I 2012 har Datatilsynet hatt kontroll og overvåking i arbeidslivet som prioritert arbeidsområde. Vi har i den anledning deltatt i Arbeidsdepartementets referansegruppe om temaet. Tilsynet vil fortsatt ha oppmerksomhet rundt dette i 2013, og vil fortsette samarbeidet med departementet.

### *Folkeregisterprosjektet*

Det er viktig for Datatilsynet å følge med på utviklingen av hvordan folkeregisteret kommer til å se ut i fremtiden. Vi har per i dag med én representant i dette prosjektet, men vil fortløpende vurdere om dette riktig ettersom hva prosjektet jobber med. Tilgang til opplysninger fra folkeregisteret er en problemstilling Datatilsynet jevnlig må forholde seg til.

### *Infoflyt*

En representant fra Datatilsynet har sittet i et utvalg som skulle se på regler for informasjonsflyten mellom politi og kriminalomsorg. Rapporten er nå levert og har vært ute på høring. Utvalget foreslår et regelsett basert på samme mal som politiregisterforskriften, med særlige regler for hvordan svært beskyttelsesverdige personopplysninger skal håndteres. Hensikten er at det meste av informasjonsutvekslingen skal skje gjennom alminnelige kanaler og at den beskyttelsesverdige informasjonen skal minimaliseres.



### *Styringsgruppe for bransjenorm innen helse*

En bransjenorm om informasjonssikkerhet for helsesektoren ble lansert i september 2006. Arbeidet i styringsgruppen består i å få en hensiktsmessig spredning og implementering av normen i sektoren. Dette skaper store utfordringer på grunn av sammensetningen av små, mellomstore og store aktører. Datatilsynet deltar som observatør i styringsgruppen.

Ved behov deltar også Datatilsynet i grupper knyttet til utarbeidelse av faktaark etter normen. I meldingsåret gjaldt dette bruk av sosiale medier og publikumskommunikasjon.

### *Interdepartemental arbeidsgruppe*

Datatilsynet deltar i en arbeidsgruppe som skal kartlegge praktiseringen av regler om taushetsplikt, opplysningsrett og -plikt. Dette arbeidet er viktig da det er svært sentralt at publikum har evne og mulighet til å ivareta egne rettigheter etter helselovgivningen og personopplysningsloven. Datatilsynet mottar en rekke spørsmål om dette, og det er viktig for tilsynet å være med og påvirke arbeidet.

### *Arbeidsgruppe i Samferdselsdepartementet – helautomatiske bomstasjoner*

Prosessen er ikke helt ferdig og det er viktig for Datatilsynet å være med å søke etter personvernvennlige løsninger når det gjelder enkeltpersoners reiser og kommunikasjon. Arbeidet frem mot en anonym løsning for passering av automatiske bomstasjoner fortsetter sammen med de andre hovedaktørene, Samferdselsdepartementet og Statens vegvesen.

### *Referansegruppe – ny politiregisterforskrift*

Datatilsynet deltar i Justisdepartementets arbeid med å utforme ny politiregisterforskrift. Dette har pågått siden 2011, og vi regner med at vi kommer til å være med i dette arbeidet frem til forskriften er vedtatt.

### *Referansegruppe – utvikling av SIS II (ELYS II)*

Det er opprettet en egen referansegruppe som følger utviklingen av Schengen Informasjonssystem versjon 2 (SIS II). Dette er et internasjonalt prosjekt hvor målet er at alle som er knyttet til SIS skal over på ny versjon samtidig. Prosjektet har gått over flere år, og har vært gjenstand for mange forsinkelser. Det synes nå som om det nærmer seg endelig ferdigstilling i 2013.

### *Koordineringsorgan for forebyggende informasjonssikkerhet*

Datatilsynet er representert i Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS). KIS er et tverrsektorielt koordineringsorgan for regelverksforvaltere og tilsynsmyndigheter med ansvar innen informasjonssikkerhet.

### *Norsk senter for Informasjonssikring – NorSIS*

Datatilsynet deltok aktivt i ID-tyveriprojektet så lenge det var finansiert gjennom prosjektmidler, men NorSIS overtok prosjektet i 2012. Tilsynet har gjennomført aktiviteter i samarbeid med NorSIS også etter overføringen. Datatilsynet er representert i styret til NorSIS ved direktøren.

## Kommunikasjonsvirksomheten

Datatilsynet har som et av sine overordnede mål at borgeren skal få økt kjennskap til sine rettigheter, og slik settes i stand til å ivareta sitt eget personvern. Vi skal også arbeide aktivt for at virksomheter og beslutningstakere vet hvilke plikter de har og legger vekt på personvern hensyn i sitt arbeid.

For at tilsynets saksbehandling og tilsynsvirksomhet skal få skikkelig effekt, må arbeidet understøttes av informasjon og dialog. Uten kunnskap kan plikt- og rettighetshavere ikke ta eget ansvar for etterlevelse av lovgivningen. Kommunikasjon brukes derfor aktivt både ved utøvelse av Datatilsynets ombudsrolle og i rollen som forvaltningsorgan.

### Foredragsvirksomhet

Det ble i meldingsåret holdt 118 foredrag på arrangementer i regi av andre, mot 129 året før.

Antall foredrag de siste årene:

År	2006	2007	2008	2009	2010	2011	2012
Antall	157	140	162	110	136	129	118

Forespørsler om foredrag har blitt vurdert ut fra satsingsområder i virksomhetsplanen for 2012 og er gitt prioritet ut fra bransje, antall deltakere, tema, samt kapasitet på aktuelt tidspunkt. Tilsynet har derfor sett seg nødt til å gi avslag på en del henvendelser. Vi mener likevel at nivået på foredragsvirksomheten per i dag er riktig, og at aktiviteten gir god uttelling i forhold til den innsats som legges ned.

I tillegg til å holde eksterne foredrag, har flere ansatte holdt innlegg på arrangementer i regi av Datatilsynet. Dette gjelder på kursene i forbindelse med personvernombudsordningen, og på de to miniseminarene som ble arrangert i 2012. Disse miniseminarene skal samle personverninteresserte og andre til faglig påfyll og gode diskusjoner om personvern. I meldingsåret var temaene *”Demokrati og terrorisme – før og etter 22. juli”* og *”Big Data”*. Seminarene er veldig populære og samler aktører fra mange ulike virksomheter.

### Mediekontakt

I løpet av 2012 har Datatilsynet registrert 876 besvarte medie henvendelser:

År	2006	2007	2008	2009	2010	2011	2012
Antall	1 425	1 350	1 614	1 293	1 432	1 120	876

Som det går frem av tabellen har vi registrert en del færre medie henvendelser enn tidligere år. Årsaken til dette er nok sammensatt. Debatten om datalagringsdirektivet preget tiden frem til Stortinget gjorde sitt vedtak våren 2011. I 2012 tok nok 22. juli-rettssaken mye av medienes oppmerksomhet og ressurser. Ikke minst har de største kommunikasjonsprosjektene våre – lanseringen av Du Bestemmer, kunstprosjektet på Oslo S og Slettmeg.no – ført til økt interesse for Datatilsynet i tidligere perioder, når prosjektene ble lansert og fikk mye oppmerksomhet.

I meldingsåret hadde vi ti egenproduserte kronikker og debattinnlegg på trykk i andre medier, noe som er omtrent på linje med tidligere år:

År	2009	2010	2011	2012
Antall	16	13	6	10

### Nye nettsider

Datatilsynets nye nettsider ble lansert i januar 2012. De har en struktur som er bedre tilpasset brukernes etterspørsel, nytt design og ny publiseringsløsning. Nettsidene er vår viktigste informasjonskanal, og nyheter, tilsynsrapporter, høringsuttalelser og publiseres løpende. Publisering og oppdatering av veiledningsmateriell er også et prioritert arbeid.

Den nye løsningen gir bedre muligheter enn tidligere for å prioritere saker basert på brukernes behov. Søkeverktøyet gir gode indikasjoner på hva brukerne leter etter, slik at vi kan tilpasse informasjon, søkeresultat og struktur med utgangspunkt i dette. Via en tilbakemeldingsfunksjon på artiklene får vi også direkte tilbakemeldinger fra brukerne, og disse følges opp fortløpende. I løpet av 2012 fikk vi rundt 420 positive tilbakemeldinger og 240 kommentarer med forslag til forbedringer.

Vi har som mål å tilpasse løsningen til brukernes forventninger og krav. Dette krever et tilfredsstillende webanalyseverktøy, noe vi ikke har lyktes med å etablere. Utfordringen er å tilpasse verktøyet slik at det følger personvernbestemmelsene og ekomlovgivningen med hensyn til logging av IP-adresser og bruk av informasjonskapsler. Det jobbes med å finne en tilfredsstillende løsning på dette.

Selv om vi ikke har en god webanalyse, har vi likevel noen indikasjoner på bruksmønstre: Omlag elleve prosent av brukerne benytter mobile plattformer for å besøke våre nettsider. Vi regner med at denne andelen vil øke kraftig fremover.

### Sosiale nettsamfunn

Datatilsynet utarbeidet i 2012 en strategi for bruk av sosiale medier. Der er det blant annet slått fast at Datatilsynet skal etablere en personvernblogg i 2013, som et prøveprosjekt på ett år. Bloggen skal være en arena der vi har dialog med aktører som har kunnskap om – og interesse for – personvern. Vi er også representert på Facebook gjennom prosjektet Du Bestemmer, som har en egen Facebook-side.

Ut over dette har vi foreløpig valgt ikke å etablere oss på Facebook. En aktiv tilstedeværelse forutsetter dialog, moderering og veiledning av brukerne og dermed økt ressursbehov. En del temaer som en bruker vil kunne ha behov for veiledning om via Facebook, faller dessuten sammen med hva som dekkes opp av andre aktører, slik som for eksempel tjenesten Slettmeg.no.

Det knytter seg dessuten utvilsomt noen utfordringer for Datatilsynet – som personvernmyndighet – til å utnytte all den funksjonalitet som ville vært naturlig for å oppnå god og effektiv kommunikasjon på Facebook og tilsvarende sosiale medier. Dette gjelder for eksempel bruk av "liker"-knappen på Facebook.

### Twitter

Når det gjelder mikroblogg-tjenesten Twitter og vår konto @datatilsynet som allerede er godt

etablert, har vi som mål å være fortsatt aktive. I løpet av meldingsåret ble det publisert 391 meldinger, mot 275 året før. Vi legger stor vekt på å besvare alle direkte meldinger, samt meldinger som omhandler Datatilsynet, raskt. Ved utgangen av året hadde Datatilsynet 7 500 følgere (followers), noe som vil si en økning på over 50 prosent fra året før.

År	2009	2010	2011	2012
Antall meldinger	135	168	275	391
Antall følgere	1 000	3 000	4 900	7 500

I tillegg har direktør Bjørn Erik Thon en twitterkonto som brukes aktivt, og som har over tre tusen følgere.

### Brukerundersøkelse/omdømme

Datatilsynet finner det ikke riktig å benytte midler til måling av etatens omdømme via de mange undersøkelsesoppleggene som tilbys av ulike analyse- og konsulentbyråer. For å få til naturlige sammenligningsgrunnlag mellom private og offentlige virksomheter blir likevel Datatilsynet gjenstand for målinger fra disse selskaperes side med jevne mellomrom.

I mai 2012 ble resultatene fra PR-Barometeret Samfunn Norge presentert. Dette er en undersøkelse i regi av analyseselskapet Aalund og kartlegger journalisters erfaring med, og oppfattelse av, offentlige institusjoner, interesseorganisasjoner og politiske partier.

Datatilsynet viste seg å være den statlige institusjonen som samlet sett ble vurdert best av journalistene. Av alle de 116 institusjonene som ble vurdert innen både privat og offentlig sektor, samt organisasjoner, var det bare Røde Kors som fikk en høyere samlet score. Datatilsynet fikk toppscore blant annet når det gjelder:

- eksperters evne til å uttale seg i klartekst,
- informasjonsavdelingens reaksjonstid,
- informasjonsavdelingens kunnskap om aktuelle saker,
- forståelse for medienes arbeidstider,
- evne til å finne interessante saker for pressen, og
- troverdighet.

Datatilsynet tar dette som en indikator på at vi oppnår resultater i tråd med våre uttalte verdier og strategiske satsinger når det gjelder vår kommunikasjonsvirksomhet, slik det fremkommer i strategiplanen.

### The Norwegian Data Protection Authority

Datatilsynet endret i 2012 den engelske oversettelsen fra *"The Norwegian Data Inspectorate"* til *"The Norwegian Data Protection Authority"* (DPA). Dette samsvarer bedre med navnene til andre lands personvernmyndigheter, og tydeliggjør bedre hva vi jobber med. Navnet er innarbeidet på våre nettsider, og i den engelske oversettelsen av personopplysningsloven.

### Barn og unges personvern – Du Bestemmer

Du Bestemmer er et samarbeid mellom Senter for IKT i utdanningen, Teknologirådet og Datatilsynet. Undervisningsopplegget ble lansert i forbindelse med den internasjonale personverndagen i januar

2007. Målet med prosjektet er å øke ungdoms kunnskap om personvern generelt, samt heve deres bevissthet om valg man gjør ved bruk av digitale medier slik som Internett og mobiltelefon. Ungdommene skal lære seg å ta kontroll over egne personopplysninger. Undervisningsopplegget er laget for to aldersgrupper, 9-13 år og 13-17 år, og er til nå brukt av over 575 000 norske skoleelever. Det er dessuten tatt i bruk i hele 16 andre land.

#### *Evaluering – positiv holdningsendring*

En evaluering gjennomført av en masterstudent ved høyskolen i Stord og Haugesund i 2012, viser en positiv holdningsendring blant elevene som har vært gjennom undervisningsopplegget.

Undersøkelsen viser at Du Bestemmer har økt elevenes bevissthet om personvern og egen nettbruk, blant annet fordi det legges opp til egenaktivitet, diskusjon og refleksjon blant elevene.

#### *Prisbelønnet film i ny modul*

Høsten 2012 ble det lansert en ny modul som handler om ytringsansvar på nett. Den skal skape diskusjon rundt hva man kan ytre på nett, hvor grensene går – eller bør gå – i diskusjonsforum og lignende, og om anonymitet er en løsning. Animasjonsfilmen "Trollus Netticus" ble utviklet i forbindelse med lanseringen, og vant prisen for beste oppdragsfilm under Fredrikstad Animation Festival 2012.

#### *Fortsatt god etterspørsel*

Det kommer fremdeles jevnlig inn bestillinger på klassesett fra hele landet, og nettstedet [dubestemmer.no](http://dubestemmer.no) er godt besøkt. Heftene benyttes ikke bare til undervisning i skolene, men bestilles også jevnlig av politi, frivillige organisasjoner, bibliotek, helsestasjoner, foreldrerepresentanter, til konformasjonsundervisning og lignende. I meldingsåret gikk nok en gang opplaget tomt, og det ble trykket opp et nytt opplag etter en relativt omfattende revisjon.

Visning av korte reklameinnslag for Du Bestemmer på TV-Norge og TV2 under reklamefrie dager i påske-, pinse- og julehøytidene resulterte i stor pågang på nettsidene, med etterfølgende bestillinger av heftene. Erfaringen viser at det er nødvendig å markedsføre undervisningsopplegget jevnlig for å holde oppe interessen og etterspørselen. Samtidig må vi legge inn ressurser på videreutvikling av prosjektet, slik at det fortsatt oppfattes som interessant og relevant.

Det at vi har klart å utvikle Du Bestemmer på en slik måte at det fortsatt oppfattes et viktig tilskudd til undervisningen på norske skoler, seks år etter lansering, må karakteriseres som en ubetinget suksess, og et vellykket statlig samarbeidsprosjekt.

Antall bestillinger av Du Bestemmer 13-17 år:

Tidsperiode	Bestillinger	Klassesett	Brosjyrer
Fra mai 2007 t.o.m. 2008	1 848	7 341	220 230
2009	460	1 417	42 510
2010	291	901	27 030
2011	376	1 086	32 580
2012	331	1 015	30 450
<b>Samlet 2007-2012</b>	<b>3 306</b>	<b>11 760</b>	<b>352 800</b>

Antall bestillinger av Du Bestemmer 9-13 år:

Tidsperiode	Bestillinger	Klassesett	Brosjyrer
2009 (fra april)	1 312	3 920	117 600
2010	363	942	28 260
2011	603	1 618	48 540
2012	426	927	27 810
<b>Samlet 2009-2012</b>	<b>2 704</b>	<b>7 404</b>	<b>222 210</b>

### I beste mening

Veilederen *I beste mening* handler om hvordan man skal håndtere bilder av barn på nett, og om bildene i det hele tatt bør være på nett. Veilederen finnes både på bokmål, nynorsk og engelsk. Den benyttes i størst grad av ansatte i barnehager, men også foreldre, skoler, frivillige organisasjoner, sykehus og bibliotek bruker den aktivt.

I løpet av 2012 ble det, på bakgrunn av bestillinger, sendt ut over 6 600 eksemplarer av veilederen. For å imøtekomme etterspørselen ble det derfor trykket et nytt opplag i november.

### Klart språk

Datatilsynet søkte i meldingsåret om støtte til ekstraordinære klarspråktiltak fra Direktorat for forvaltning og IKT (Difi). Vi fikk tildelt 50 000 kroner, et internt språkkurs, prosjektrådgivning fra Difi og rådgivning til utarbeidelse av språkprofil fra Språkrådet. Følgende språktiltak ble gjennomført i 2012:

- Et klarspråkkurs for 15 ansatte ble gjennomført i samarbeid med kompetansesenheten i NTB.
- Det ble gjennomført en brukerundersøkelse på nett for å kartlegge brukernes holdninger til språket i våre tekster. Svarprosenten var relativt lav, men resultatene viser en tendens til at respondentene vurderer at tekstene på nettsidene våre har et forståelig språk. Enkelte mente imidlertid at det var vanskelig å finne fram på sidene.
- Det ble gjennomført en kartlegging av språket i flere av våre tekster, slik som veiledere, tilsynsrapporter og høringsuttalelser. Kartleggingen, som ble gjennomført av byrået Arkitekst, viser at vi har potensial for å forbedre flere av våre tekster og måten vi utarbeider disse på.

- Et utkast til språkprofil ble laget med utgangspunkt i kartleggingsrapporten, og skal introduseres for alle ansatte i løpet av 2013.

### Samisk

I St.meld. nr. 28 (2007-2008) *Samepolitikken* legges det særlig vekt på "hverdagspolitikken", det vil si den praktiske integreringen av samiske hensyn i politikktutforming og tiltak på alle samfunnsområder og forvaltningsnivåer. Innenfor forvaltningsområdet for samisk språk skal virksomhetene følge opp språkreglene i sameloven. På bakgrunn av dette har Datatilsynet valgt å gjøre følgende tilgjengelig på samisk:

- Personopplysningsloven (datatilsynet.no),
- Personvernprinsippene (datatilsynet.no),
- informasjonen "Hva er personvern?" (datatilsynet.no), og
- hele undervisningsopplegget Du Bestemmer.

## Budsjett, organisasjon og administrasjon

Datatilsynets bevilgning for 2012 var 35 015 000 kroner. Dette var en økning på 9,2 prosent i forhold til i 2011. I tillegg ble det gitt kompensasjon for lønnsoppgjør med 713 000 kroner. Tildelingen dekket utgifter til lønn og drift. Økningen dekket også utgifter som følger av nye oppgaver Datatilsynet er tillagt ved implementering av datalagringsdirektivet og ny politiregisterlov. Det ble i 2011 bevilget midler til å dekke deler av dette (fire måneder). I 2012 ble halvårseffekten innarbeidet. En økt bevilgning kompenserer også for prisstigning i 2012.

Datatilsynets lønnsutgifter var i meldingsåret var på 69 prosent, mens øvrige driftsutgifter var på 31 prosent av bevilgningen. I 2011 lå disse utgiftene på henholdsvis 75 prosent og 25. At det ble brukt mindre midler til lønn i meldingsåret enn i 2011 skyldes det at flere stillinger ble stående ubesatt i perioder av meldingsåret.

År	Beløp
2009	kr 29 020 000,-
2010	kr 30 989 000,-
2011	kr 32 051 000,-
2012	kr 35 015 000,-

### Organisasjon

Datatilsynet ledes av direktør Bjørn Erik Thon, og er organisert i fire avdelinger. Hver avdeling ledes av en avdelingsdirektør. Datatilsynets ledelse består av fire menn og én kvinne.

Datatilsynet har i 2012 hatt 41 fast tilsatte. Av disse var 51 prosent kvinner og 49 prosent menn.

Tabellen viser faste stillinger fordelt på avdelinger:

	2011			2012		
	Totalt	Kvinner	Menn	Totalt	Kvinner	Menn
Direktør	1	-	1	1	-	1
Informasjonsavdelingen	4	3	1	4	3	1
Juridisk avdeling	15	8	7	16	9	7
Tilsyns- og sikkerhetsavdelingen	9	2	7	12	2	10
Administrasjonsavdelingen	8*	8	-	8*	8	-
SUM	37	21	16	41	22	19

\* I administrasjonsavdelingen har to ansatte hatt redusert stillingsandel. Avdelingen har totalt hatt syv fulle årsverk i 2011 og 2012.

Fire kvinner og fire menn har hatt foreldrepermisjon hele eller deler av året.



### *Administrasjon og kompetanse*

Datatilsynet bidrar med kunnskap til en opplyst debatt om sentrale personvernspørsmål og gir råd og veiledning til befolkningen, private virksomheter og offentlig forvaltning. De ansatte skal føre tilsyn med områder i stadig utvikling, vurdere teknologibaserte utfordringer og kjenne til hvordan teknologi kan benyttes for å avhjelpe trusler mot personvernet. For å få til dette må Datatilsynet ha motiverte medarbeidere med høy kompetanse og god rolleforståelse. Sentralt i Datatilsynets lønns- og personalpolitikk står derfor tiltak for å rekruttere, utvikle og beholde medarbeidere med høy kompetanse.

I 2012 har arbeidet med forbedring og effektivisering av vår personaladministrasjon hatt høy prioritet. Det er satset spesielt på kompetanseutvikling og kompetansehevende tiltak. Budsjettposten til kurs- og seminarvirksomhet ble styrket og det ble etablert et eget kompetansefond. To medarbeidere søkte midler fra fondet til videreutdanning innen prosjektledelse. Gjennom året er det også hentet inn ekstern ekspertise for å gi de ansatte faglig påfyll. Det er også lagt vekt på deling av kompetanse internt.

Tilsynet har erfart at den kompetansen våre medarbeidere sitter på er svært ettertraktet både i privat og offentlig sektor. I 2012 har dette vært spesielt utfordrende da det har vært stor interesse for arbeidstakere med personvernkompetanse. Dette skyldes blant annet implementeringen av datalagringsdirektivet og ny politiregisterlov, samt stor satsing på informasjonssikkerhet og beredskap i både privat og offentlig sektor.

I meldingsåret sluttet til sammen ni medarbeidere, hvorav flere svært erfarne med høy kompetanse på personvern. Det ble av den grunn nødvendig å benytte en god del ressurser på å rekruttere nye, dyktige medarbeidere. Det ble også nødvendig å iverksette tiltak for å beholde kunnskapsrike medarbeidere og å kunne tilby utviklingsmuligheter i etaten. Det ble blant annet opprettet to fagdirektørstillinger. Én i juridisk avdeling og én i tilsyns- og sikkerhetsavdelingen. Tilsynets utredningskapasitet ble også økt og samlet i én avdeling. Utrederne er nå etablert i tilsyns- og sikkerhetsavdelingen.

Med hele åtte nye medarbeidere (en stilling er ved utgangen av 2012 ikke besatt) har det vært naturlig å videreutvikle interne prosedyrer for tilsetting og fratreden. Det er også etablert felles introduksjonsplaner og individuelle planer for opplæring av nytilsatte. Vi anser introduksjonsfasen i et ansettelsesforhold som svært viktig i forhold til å få en rask faglig og sosial integrering. Dette arbeidet har derfor hatt prioritet det siste året.

Datatilsynet er omfattet av avtalen om inkluderende arbeidsliv og har spesiell oppmerksomhet på forebygging og oppfølging av sykefravær. Sykefraværet var i meldingsåret 2,0 prosent mot 2,8 prosent i 2011. Det har ikke vært behov for å iverksette spesielle tiltak. I løpet av det siste året har det vært arrangert førstehjelpskurs, og det har vært gjennomført kurs om livsstil og stressmestring.

Tilsynet har som målsetting å hindre at søkere med redusert arbeidsevne blir diskriminert, og å bidra til å heve den generelle pensjonsalderen. Datatilsynet understreker målsettingen om mangfold med tanke på etnisk bakgrunn, funksjonsevne, kjønn og alder i våre stillingsutlysninger.

## 5. Vedlegg

### Vedlegg A. Gjennomførte tilsyn

	Saksnr.	Tittel	Område
1	12/01173	Kontroll hos Byrknes Auto avdeling Tromsø 17122012 - Kameraovervåking	Arbeidsliv
2	12/00897	Kontroll hos Transcom 25092012 - Arbeidsliv	Arbeidsliv
3	12/00812	Kontroll ved Eidsvoll vaktelskap 31082012 - Felles tilsyn sammen med Arbeidstilsynet - Arbeidsliv	Arbeidsliv
4	12/00717	Kontroll hos Sandnes Taxi AS - 07092012 - Kameraovervåking	Arbeidsliv
5	12/00716	Kontroll hos Stavanger Taxi AS 05092012 - Kameraovervåking	Arbeidsliv
6	12/00708	Kontroll hos Bianco Footwear Oslo City - 11072012 - Kameraovervåking	Arbeidsliv
7	12/00704	Kontroll hos GoExcellent Norway AS 10072012 - Bruk av lydopptak	Arbeidsliv
8	12/00579	Kontroll hos Viasat og People in Motion 19062012 - Bruk av lydopptak	Arbeidsliv
9	12/00376	Kontroll hos Statens arbeidsmiljøinstitutt - STAMI	Arbeidsliv
10	12/00188	Kontroll hos Avfallsservice 0506012 - Kameraovervåking	Arbeidsliv
11	12/01192	Etterkontroll - Brevkontroll hos Atferdssenteret AS	Etterkontroll
12	12/01191	Etterkontroll – Brevkontroll hos Barne- ungdoms- og familiedirektoratet - Minde Barne- og ungdomshjem	Etterkontroll
13	12/01116	Etterkontroll - Brevkontroll hos Norsk pasientskadeerstatning (NPE)	Etterkontroll
14	12/00707	Kontroll hos BIT Oslo City 11072012 - Etterkontroll - Kameraovervåking	Etterkontroll
15	12/01084	Brevkontroll ved Universitetssykehuset Nord-Norge HF - Reservasjonsregisteret	Helse
16	12/01084	Brevkontroll ved St. Olavs Hospital HF - Reservasjonsregisteret	Helse
17	12/01084	Brevkontroll ved Haukeland universitetssykehus HF - Reservasjonsregisteret	Helse
18	12/01084	Kontroll hos Folkehelseinstituttet 11122012 universitetssykehus - Reservasjonsregisteret	Helse
19	12/00116	Kontroll hos Arbeids- og velferdsdirektoratet 07032012 - NAV Kontroll	Helse
20	12/00456	Kontroll ved Mestringshusene Bolkesjø AS 16052012 - Tilgangsstyring	Internkontroll / sikkerhet
21	12/00321	Kontroll hos Fremskrittspartiet 29052012 - Politiske partier - Internkontroll og info.sikkerhet	Internkontroll / sikkerhet
22	12/00320	Kontroll hos Høyre 05062012 - Politiske partier - Internkontroll og info.sikkerhet	Internkontroll / sikkerhet
23	12/00319	Kontroll hos Sosialistisk Venstreparti ( SV ) 02052012 - Politiske partier - Internkontroll og info.sikkerhet	Internkontroll / sikkerhet
24	12/00754	Kontroll hos Toll- og avgiftsdirektoratet 29082012 - Kjennetegngjenkjenningssystemet	Justis
25	12/00753	Kontroll hos Statens Vegvesen 16082012 – Kjennetegngjenkjenningssystemet	Justis

	Saksnr.	Tittel	Område
26	12/01141	Kontroll hos Grottebadet AS 28112012 - Kameraovervåking	Kameraovervåking
27	12/00814	Kontroll hos Teletaxi Asker og Bærum AS 22112011 - Kameraovervåking	Kameraovervåking
28	12/00058	Kontroll hos Sørlandsbadet AS 18012012 - Kameraovervåking	Kameraovervåking
29	12/00057	Kontroll ved Paulsens Hotell 18012012 - Kameraovervåking	Kameraovervåking
30	12/01053	Kontroll hos Blålys 22112012 - Medlemsopplysninger	Offentlig
31	12/01045	Kontroll hos Direktoratet for naturforvaltning 04122012 - Internkontroll og informasjonssikkerhet	Offentlig
32	12/01044	Kontroll hos Direktoratet for arbeidstilsynet 05122012 - Internkontroll og informasjonssikkerhet	Offentlig
33	12/01022	Kontroll hos Havarikommisjonen for Transport 27112012 - Internkontroll og informasjonssikkerhet	Offentlig
34	12/00994	Kontroll hos Utlendingsnemnda - UNE - 26112012 - Internkontroll og informasjonssikkerhet	Offentlig
35	12/00973	Kontroll hos Utdanningsdirektoratet 23112012 - Offentlig forvaltning - Internkontroll og informasjonssikkerhet	Offentlig
36	12/00417	Kontroll hos Nasjonalbiblioteket 12062012 - Internkontroll og informasjonssikkerhet	Offentlig
37	12/00179	Kontroll hos Storfjord kommune 28032012 - Internkontroll	Offentlig
38	12/00178	Kontroll hos Lyngen kommune 28032012 - Internkontroll	Offentlig
39	12/00176	Kontroll hos Kåfjord kommune 27032012 - Internkontroll	Offentlig
40	12/00173	Kontroll hos Nordreisa kommune 27032012 - Internkontroll	Offentlig
41	12/00157	Kontroll hos Kvænangen kommune 26032012 - Internkontroll	Offentlig
42	12/00064	Kontroll hos Rekruttering AS 02022012 - Innsamling av personopplysninger - Klagesak i Personvernemnda - PVN-2012-02	Offentlig
43	12/00014	Mobil ISP - Ice Norge AS - Tilgang til innholdsdata	Tele / Internett
44	12/00013	Mobil ISP - Netcom - Tilgang til innholdsdata	Tele / Internett
45	12/0012	Mobil ISP - Telenor - Tilgang til innholdsdata	Tele / Internett
46	11/01319	Mobil ISP - Network Norway - Tilgang til innholdsdata	Tele / Internett
47	12/00276	Kontroll hos DNB Eiendom 19042012 - Personopplysninger og mobilapplikasjoner	Tele / Internett
48	12/00275	Kontroll hos WiMP MUSIC AS 11042012 - Personopplysninger og mobilapplikasjoner	Tele / Internett
49	12/00274	Kontroll hos NSB 13042012 - Personopplysninger og mobilapplikasjoner	Tele / Internett
50	12/00864	Kontroll hos Sparebank 1 Markets 17102012 - Lydopptak	Økonomi
51	12/00863	Kontroll hos Navigea Security 15102012 - Lydopptak	Økonomi
52	12/00859	Kontroll hos Ica Norge AS ved Rimi Semsbyen 12102012 - Kameraovervåking for Post i butikk	Økonomi
53	12/00853	Kontroll hos Kiwi Sognsveien 10102012 - Kameraovervåking for Bank i butikk-tjenester	Økonomi
54	12/00852	Kontroll hos SPAR Tåsen 10102012 - Kameraovervåking for Bank i butikk-tjenester	Økonomi
55	12/00060	Kontroll hos Protector Forsikring ASA 14022012 - Skadeforsikring	Økonomi

## Vedlegg B. Høringer

	Dok.nr.	Navn	Dok.dato	Avsender / mottager
1	11/00697-5	Høringsuttalelse - Forslag til politiregisterforskriften - De resterende 5 deler	30.4.2012	Justis- og beredskapsdepartementet
2	11/00792-2	Høringsuttalelse - NOU 2011:10 - I velferdsstatens venterom - Om mottakstilbudet for asylsøkere	12.1.2012	Justis- og politidepartementet
3	11/00914-3	Høringsuttalelse - NOU 2011:9 Økt selvbestemmelse og rettsikkerhet - Helse- og omsorgsdepartementet	19.1.2012	Helse- og omsorgsdepartementet
4	11/00931-2	Høringsuttalelse - NOU 2011:13 Når sant skal skrives - Juryutvalget - Justis- og politidepartementet	17.2.2012	Justis- og politidepartementet
5	11/00970-3	Høring - Tilleggsuttalelse - Revidert utkast til bestemmelser om registerkontroll	4.6.2012	Arbeidsdepartementet
6	11/01203-2	Høringsuttalelse - Endring i ekomlov og forskrift 2011	3.1.2012	Samferdselsdepartementet
7	11/01219-2	Høringsuttalelse - Evaluering av Teknologirådet	10.2.2012	Nærings- og handelsdepartementet
8	11/01264-2	Høringsuttalelse - Forslag til endringer i forskrift om innsamling og behandling av helseopplysninger i MSIS- og Tuberkuloseregisterforskriften	28.2.2012	Helse- og omsorgsdepartementet
9	11/01275-2	Høringsuttalelse - Endringer i statsborgerloven og statsborgerforskriften - Adgang til å innhente opplysninger fra andre offentlige organer - Barne- likestillings- og inkluderingsdepartementet	4.1.2012	Barne-, likestillings- og inkluderingsdepartementet
10	11/01275-3	Tilleggsuttalelse - høring vedrørende endringer i statsborgerloven	26.4.2012	Barne-, likestillings- og inkluderingsdepartementet
11	11/01277-2	Høringsuttalelse – Behandlingen av sivile krav etter terrorhandlingene 22 juli 2011 - Forslag til enkelte endringer i Voldsoffererstatningsloven og Straffeprosessloven - videooverføring av rettsforhandlinger - Justisdepartementet	4.1.2012	Justis- og politidepartementet
12	11/01306-2	Høringsuttalelse - Krav til oppbevaring av opplysninger om ekspedisjon av resept og rekvisisjon og utdyping av journalføringsplikt for helsehjelp i apotek	28.3.2012	Helse- og omsorgsdepartementet
13	11/01317-2	Høringsuttalelse - Utkast til forskrift om virksomhetsovergrepene behandlingsrettede helseregistre i formaliserte arbeidsfellesskap	16.3.2012	Helse- og omsorgsdepartementet

	<b>Dok.nr.</b>	<b>Navn</b>	<b>Dok.dato</b>	<b>Avsender / mottager</b>
14	11/01325-2	Høringsuttalelse - Forslag til innføring av valgfag på ungdomstrinnet	2.3.2012	Utdanningsdirektoratet
15	11/01333-2	Høringsuttalelse - Forslag til endringer i kreftregisterforskriftens regler om behandling av opplysninger om personer som har deltatt i program for tidlig diagnose eller kontroll for konkret kreftsykdom - kreftscreening	19.3.2012	Helse- og omsorgsdepartementet
16	11/01336-2	Høringsuttalelse - Forskrift om oversikt over helsetilstand og påvirkningsfaktorer - Folkehelseforskriften	16.3.2012	Helse- og omsorgsdepartementet
17	11/01339-2	Høringsuttalelse - Revidert fastlegeforskrift	22.3.2012	Helse- og omsorgsdepartementet
18	11/01342-2	Høringsuttalelse - Forslag til endringer i helseforetaksloven	19.3.2012	Helse- og omsorgsdepartementet
19	12/00010-2	Høringsuttalelse - Ny forskrift om gjennomføring av Europeisk avtale om kjøre- og hviletid mv for mannskaper på kjøretøy i internasjonal vegtransport - AETR	5.3.2012	Statens vegvesen - Vegdirektoratet
20	12/00015-2	Høringsuttalelse - Utkast til norsk bokføringsstandard NBS(HU) Elektronisk fakturering	17.4.2012	Norsk RegnskapsStiftelse
21	12/00048-2	Høringsuttalelse - Forslag til endring av tobakksloven	23.3.2012	Helse- og omsorgsdepartementet
22	12/00111-2	Høringsuttalelse - Forslag til presiseringer i ligningsloven § 6-15 om kontroll hos tredjemann og ny forskrift om gjennomføring av kontroll på skatte- og avgiftsområde	26.4.2012	Finansdepartementet
23	12/00125-3	Høringsuttalelse - Endringer i helsesektorens tilgang til folkeregisteropplysninger	29.4.2012	Finansdepartementet
24	12/00143-2	Høringsuttalelse - Forslag til innføring av elektronisk skattekort	30.3.2012	Finansdepartementet
25	12/00148-2	Høringsuttalelse - Forslag til endring i forskrift om bruk av kjøretøy - Opphør av kontrollmerker på kjøretøy	13.2.2012	Statens vegvesen - Vegdirektoratet
26	12/00151-2	Høringsuttalelse - Utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data - Datalagringsforskriften	30.3.2012	Post- og teletilsynet
27	12/00158-2	Høringsuttalelse - Diverse endringer i lov av 21 juni 2002 nr 45 om yrkestransport med motorvogn og fartøy - Yrkestransportloven	4.5.2012	Samferdselsdepartementet
28	12/00172-2	Høringsuttalelse - Forslag til nytt regelverk for kassasystemer	25.5.2012	Finansdepartementet

	<b>Dok.nr.</b>	<b>Navn</b>	<b>Dok.dato</b>	<b>Avsender / mottager</b>
29	12/00175-2	Høringsuttalelse - NOU 2012: 1 Til barnas beste	23.4.2012	Kunnskapsdepartementet
30	12/00228-2	Høringsuttalelse - Forslag om særlige regler for gjennomføring av psykisk helsevern i regionale sikkerhetsavdelinger herunder i enhet med særlig høyt sikkerhetsnivå	19.3.2012	Helse- og omsorgsdepartementet
31	12/00237-2	Høringsuttalelse - NOU 2011:17 Når sant skal sies om pårørendeomsorg - Fra usynlig til verdsatt og inkludert	6.7.2012	Helse- og omsorgsdepartementet
32	12/00272-2	Høringsuttalelse - Nye anbefalte IT-standarder for offentlig sektor	15.4.2012	Direktoratet for forvaltning og IKT
33	12/00282-2	Høringsuttalelse - NOU 2011-19 - Ny våpenlov	26.3.2012	Justis- og beredskapsdepartementet
34	12/00309-2	Høringsuttalelse - Forslag om endringer i reglene om tollmyndighetenes adgang til undersøkelse på person	26.3.2012	Finansdepartementet
35	12/00313-2	Høringsuttalelse - Kostnadsdelingsmodeller for datalagringsdirektivet	12.4.2012	Samferdselsdepartementet
36	12/00355-2	Høringsuttalelse - Forslag til avtale om tilknytning til helsenettet - Norsk Helsenett SF	29.4.2012	Norsk Helsenett SF
37	12/00398-2	Høringsuttalelse - EU-kommisjonens forslag til nye personvernregler	4.7.2012	Justis- og beredskapsdepartementet
38	12/00400-2	Høringsuttalelse - Vurdering av tiltak i markedet for internasjonale betalingskort i Norge - Finansdepartementet	11.6.2012	Finansdepartementet
39	12/00476-2	Høringsuttalelse - Utredning om formidling av grunnbok- og matrikkelinformasjon fra Statens kartverk	13.8.2012	Miljøverndepartementet
40	12/00484-2	Høringsuttalelse - Forslag om å pålegge drosjesentraler å innberette opplysninger om tilknyttede drosjeeieres omsetning mv til skatte- og avgiftsmyndighetene - Finansdepartementet	4.7.2012	Finansdepartementet
41	12/00489-2	Høringsuttalelse - NOU 2012:5 Bedre beskyttelse av barns utvikling	13.9.2012	Barne-, likestillings- og inkluderingsdepartementet
42	12/00565-5	Kommentarer til rapporten - Effektivt sluttbrukermarked for kraft	15.8.2012	Norges vassdrags- og energidirektorat
43	12/00595-2	Høringsuttalelse - Forslag om forskriftsendringer som innfører ny turnustjeneste for leger	3.7.2012	Helse- og omsorgsdepartementet
44	12/00622-2	Høringsuttalelse - Forslag til endringer i personopplysningsforskriften	27.9.2012	Fornyings-, administrasjons- og kirke departementet

	<b>Dok.nr.</b>	<b>Navn</b>	<b>Dok.dato</b>	<b>Avsender / mottager</b>
45	12/00631-2	Høringsuttalelse - INFOFLYT-utvalgets rapport	28.11.2012	Justis- og beredskapsdepartementet
46	12/00635-3	Høringsuttalelse - Nye bevarings- og kassasjonsbestemmelser for kommunene og fylkeskommunene	21.12.2012	Riksarkivet
47	12/00642-2	Høringsuttalelse - Utkast til forskrift om krav til kvalitet og sikkerhet for humane organer beregnet på transplantasjon	20.9.2012	Helse- og omsorgsdepartementet
48	12/00647-2	Høringsuttalelse - Forslag om endring av forskrift om IT-standarder i offentlig forvaltning	24.9.2012	Direktoratet for forvaltning og IKT
49	12/00706-2	Høringsuttalelse - Opprettelse av Miljøvedtaksregisteret	5.9.2012	Direktoratet for naturforvaltning
50	12/00785-2	Høringsuttalelse - Forslag til endringer i utlendingsforskriften - Adgang til å ta lyd- og bildeopptak av asylregistreringen	7.11.2012	Justis- og beredskapsdepartementet
51	12/00832-2	Høringsuttalelse - Beslagleggelse og destruksjon av ulovlig privatimporterte legemidler samt forslag til endringer i reglene for privatimport av legemidler	29.11.2012	Helse- og omsorgsdepartementet
52	12/00849-2	Høringsuttalelse - Forslag til endringer i barneloven - Forslag om endringer i finansieringsansvaret og i den faglige samhandlingen mellom stat og kommune forslag om styrking av barns rettigheter mv	15.11.2012	Barne-, likestillings- og inkluderingsdepartementet
53	12/00865-2	Høringsuttalelse - Kriminalisering av forberedelse til terrorhandling - utvidet adgang til tvangsmiddelbruk og endringer i straffeloven 1902 § 60a	25.10.2012	Justis- og beredskapsdepartementet
54	12/00868-3	Høringsuttalelse - Europakommisjonens forslag til forordning om eID og e-signatur mm	30.11.2012	Nærings- og handelsdepartementet
55	12/00964-2	Høringsuttalelse - Forslag til endringer i utlendingsforskriften §§ 10-8 og 10-9 heving av underholdskravet mv - Justis- og beredskapsdepartementet	10.12.2012	Justis- og beredskapsdepartementet
56	12/00970-2	Høringsuttalelse - Forslag til endringer i vaktvirksomhetsforskriftens utdanningskrav	15.11.2012	Justis- og beredskapsdepartementet
57	12/01021-2	Høringsuttalelse - Forslag til lovendringer for å gi barn bedre beskyttelse mot vold og overgrep	27.11.2012	Barne-, likestillings- og inkluderingsdepartementet
58	12/01060-2	Høringsuttalelse - Forslag til endringer i opplæringslov og privatskolelov - Spesialundervisning og psykososialt miljø	17.12.2012	Kunnskapsdepartementet

## Vedlegg C. Saker oversendt til Personvernemnda

	Klager	Tittel	Saksnummer hos nemnda	Vedtak i PVN
1	Rettsmedisinsk institutt	Klage på avslag på søknad om konsesjon til å behandle personopplysninger i forskning samt pålegg om sletting av innhentede opplysninger - Hovedoppgave om Barn med påførte dødelige skader – hva gjør helsevesenet og rettsvesenet?	PVN-2012-01	Klagen tas til følge
2	Rekruttering AS	Klage på Datatilsynets planlagte kontroll mot Rekruttering AS	PVN-2012-02	Klagen tas ikke til følge
3	Bing Hodneland advokatfirma på vegne av VG	Klage på vedtak om sletting av personopplysninger som stammer fra det nedlagte nettsamfunnet Nettby	PVN-2012-03	Klagen tas ikke til følge
4	Privatperson	Klage på vedtak om å ikke ilegge arbeidsgiver overtredelsesgebyr i sak vedrørende innsyn i e-post – Sparebank 1 Skadeforsikring	PVN-2012-04 Se også PVN-2011-01	Klagen tas ikke til følge
5	Privatpersoner (2 stk)	Klage på vedtak om sletting av mangelfulle og feilaktige opplysninger vedrørende fosterforeldre	PVN-2012-05	Klagen tas til følge
6	Teletopia Gruppen AS	Klage på pålegg om utlevering av opplysninger og på publisering av foreløpig kontrollrapport hvor administrerende direktør navngis	PVN-2012-06	Klagen tas ikke til følge
7	Wikborg Rein & Co	Klage på standardkonsesjon til å behandle personopplysninger i kredittopplysningsvirksomhet	PVN-2012-07	Klagen tas delvis til følge
8	Privatperson	Klage på vedtak om å avslutte sak som omhandlet krav om sletting av dokumenter i elevmappe – Nesset kommune	PVN-2012-08	Klagen tas ikke til følge
9	Folkehelseinstituttet	Klage på avslag på søknad om konsesjon for gjennomføring av et pilotprosjekt – Testing av innsamling av legemiddelinformasjon fra pasientkurver	PVN-2012-09	Klagen tas ikke til følge
10	Helse- direktoratet/ SUSS-telefonen	Klage på vedtak om pålegg etter kontroll ved SUSS – Senter for ungdom, samliv og seksualitet	PVN-2012-10	Klagen tas ikke til følge
11	Kreftregisteret	Klage på avvisning av å realitetsbehandle Kreftregisterets søknad om konsesjon til å behandle negative funn ved mammografiscreening uten samtykke fra den registrerte	PVN-2012-11	Klagen tas til følge
12	Kreftregisteret	Klage på oppheving av vedtak om å tillate registrering av negative funn ved livmorhalscreening uten samtykke fra de registrerte	PVN-2012-12	Klagen tas ikke til følge
13	Stopp Jobbmobben på vegne av klient	Klage på vedtak vedrørende nektet innsyn i personalmappe	PVN-2012-13	Klagen tas delvis til følge
14	Privatperson	Klage på avvisning av sak – Klage på NAV Midtbyen i Trondheim og vaktelskapet NOKAS	PVN-2012-14	Klagen tas ikke til følge
15	Privatperson	Klage på vedtak om avvisning av sak – Kameraovervåking på privat eiendom	PVN-2012-15	Klagen tas ikke til følge