ÅRSMELDING FOR 2013

Hva rører seg på personvernfeltet – og hva har Datatilsynet gjort i året som gikk

Datatilsynet

Forord

Den 7. juni i år trykket Washington Post en artikkel om en mann med navn Edward Snowden. Han var IT-konsulent og jobbet for det amerikanske NSA. Han avslørte blant annet at det i USA fantes et hemmelig overvåkingsprogram rettet mot utenlandske borgere, at NSA hadde hatt sine fingre langt inn i serverne til Microsoft og Google, og at selveste Angela Merkels telefon var blitt avlyttet. Saken vakte stor oppmerksomhet verden over, ikke minst spurte mange hva konsekvensene ville bli. Ville vi slutte å stole på Internett som en kommunikasjonskanal? Datatilsynet gjennomførte derfor en personvernundersøkelse der vi spurte om folks syn på denne saken, og om den hadde hatt en nedkjølende effekt på folks vilje til å kommunisere. Funnene fra undersøkelsen står å lese i denne årsmeldingen.

Den teknologisk utviklingen går i rasende fart. 90 prosent av all data som er produsert i verden til nå er produsert de siste to årene. Mer enn seks milliarder enheter kommuniserer med Internett og tallet vil fordobles på to år. Vi står på spranget inn i det som kalles tingenes Internett. Nå er det ikke bare mobiltelefoner som gjelder, men også klokker, briller, sko og klær vil få internettoppkobling. Dette er en utvikling Datatilsynet er opptatt av, og et eget kapittel i denne meldingen er viet kroppsnær teknologi.

Det er viktig å huske på at personvern til syvende og sist dreier seg om det enkelte menneske. Det er viktig for oss i Datatilsynet å ha oppmerksomhet på hva som treffer hver og en av oss. Vi er bekymret over at mer enn 20 prosent av alle henvendelser til Datatilsynet gjelder personvern i arbeidslivet. Derfor er det viktig å gi gode råd til folk som tar kontakt, ha god informasjon på hjemmesiden og en klar og tydelig stemme i den offentlige debatten.

Personvern er viktigere enn noen gang, og personvernundersøkelsen viser at personvern ikke bare er for spesielt interesserte, men at flere og flere ser viktigheten av et godt personvern. For oss som er så heldig å jobbe i Datatilsynet er dette inspirerende og utfordrende. Derfor sier vi også uten blygsel at det aldri har vært viktigere å ha et troverdig, entusiastisk, kunnskapsrikt og modig Datatilsyn.

Lykke til med lesingen av årsmeldingen for 2013.

Bjørn Erik Thon
Direktør

Innhold

1. Datatilsynet – Hva har vi gjort og hvor går vi?

Året 2013 har vært preget av høyt aktivitetsnivå i Datatilsynet. Dette skyldes at personvern er viktig i nær sagt alle sektorer. Den teknologiske utviklingen gjør det mulig å samle inn, bruke og dele personopplysninger på nye måter. Det har vært et politisk ønske at også offentlige data skal gjenbrukes. Vi i Datatilsynet er selvsagt ikke imot dette, men vi har samtidig påpekt at prinsippet om at data som hovedregel ikke skal brukes til andre formål enn det de er samlet inn for, utfordres med en slik politikk.

Det er sentralt for Datatilsynet å komme tidlig inn viktige prosesser, og vi glade for at både offentlige organer, organisasjoner og næringsdrivende ser på oss som en viktig samtalepartner. Vi er imidlertid opptatt av at det gjøres gode personvernutredning så tidlig i utviklingsprosessen som overhode mulig. Dessverre ser vi at utredninger av personvernkonsekvenser i lovprosesser ofte er mangelfulle eller helt fraværende. Dette er ikke bare et brudd på utredningsinstruksen, men også et uttrykk for at det fortsatt er et stykke vei å gå før bevisstheten om personvern er så tilstedeværende som den bør være. Vi erfarer dessuten at det gir bedre og mer balanserte løsninger dersom personvernhensyn tas tidlig inn i prosessen.

De siste årene har vi forsøkt å markedsføre prinsippene for innebygd personvern. I dette ligger at personvern bygges inn i de teknologiske løsningene på et tidlig tidspunkt. Dette kan for eksempel være automatisk sletting av opplysninger eller automatiserte innsynsløsninger. I Stortingsmeldingen *«Personvern – utsikter og utfordringar»*[1] er det slått fast at prinsippene for innebygd personvern skal benyttes ved utviklingen av statlige IKT-løsninger. Dette er et svært viktig signal og vi i Datatilsynet ser det som en viktig oppgave å være en pådriver for at dette faktisk følges opp.

Datatilsynet skal delta i debatten om personvernspørsmål og har som mål å være landets mest kompetente personvernmiljø. Det er viktig at våre synspunkter i størst mulig grad er basert på kunnskap. De siste årene har det vært en prioritert oppgave i Datatilsynet både å satse på utredningsarbeid, men også å samarbeide med forsknings- og utviklingsmiljøer. Dette har vært en vellykket satsing. Vi har blitt invitert inn som deltager i viktige forskningsprosjekter, og dette sender et tydelig signal om at personvern tas på alvor. Vår egen utredning «Big Data – personvernprinsipper under press», ble svært godt mottatt og har vært en døråpner for deltagelse i spennende prosjekter. Vi har også holdt en lang rekke foredrag om temaet, og er for første gang i tilsynets historie ansvarlig for å utarbeide en rapport for Berlin-gruppen.

I løpet av meldingsåret gjennomførte vi flere tilsyn i virksomheter som driver etterforskning og granskning, enten av egne kunder eller ved å ta oppdrag for andre. Tilsynene avdekket store mangler og betydelige lovbrudd. I etterkant av disse tilsynene fikk vi et bestemt inntrykk av at de som drev granskninger, i stor grad satte i gang interne prosesser for å gjennomgå rutinene sine for behandling av personopplysninger. Flere bransjeorganisasjoner kom dessuten på banen og ønsket et samarbeid med Datatilsynet for å utvikle bransjenormer.

[1] Meld. St. 11 (2012-13)

På mange måter er dette et skoleeksempel på vellykket tilsynsarbeid; først gjennomføre tilsyn for å avdekke problemer, og deretter gå i dialog for å hjelpe bransjen til selv å rydde opp. Men, et underliggende problem gjenstår; de rettslige rammene for granskningsvirksomhet ikke er gode nok. Det er også grunn til å være kritisk til at store virksomheter bygger opp etterforskningsenheter. Enheter som gjør en jobb som egentlig hører inn hos politiet. Etterforskning skal alltid være preget av objektivitet, og det er krevende når man for eksempel etterforsker sine egne kunder. De rettsikkerhetsgarantiene som er bygd inn i for eksempel straffeprosessloven gjelder selvsagt heller ikke for privat etterforskning. Datatilsynet tok derfor til orde for at et sterkere politi gir bedre personvern, og fikk støtte fra blant annet Advokatforeningen.

Meldingsåret var dessuten sterkt preget av Edward Snowdens avsløringer av amerikansk etterretning. Datatilsynet har deltatt aktivt i debatten som har fulgt i kjølvannet av saken. Den viser at det knapt finnes noen grense for hvor langt en stat kan gå i å overvåke sine innbyggere. Teknologiens muligheter er ubegrensede og det har fra vår side vært viktig å påpeke at overvåking ikke er akseptabelt, selv om det er teknisk mulig. Dette er en viktig lærdom i mange bransjer. Det er viktig at det settes klare rammer for hvilke virkemidler for eksempel de hemmelige tjenestene skal ha. Ny teknologi åpner for fantastiske muligheter for å leve en enklere og bedre liv, men har samtidig i seg et potensial til å skape det komplette overvåkingssamfunn. For å forhindre at utviklingen går i feil retning, trenger vi politikere som forstår verdien av et godt personvern.

2. Tema

Året med Snowden

I begynnelsen av juni 2013 avslørte The Washington Post og The Guardian det som ble kjent som PRISM-saken. Kilden til avsløringene var Edward Snowden, en dataingeniør ansatt i et privat dataselskap som var engasjert av National Security Agency (NSA). I løpet av sommeren og høsten kom det stadig nye avsløringer, blant annet at NSA hadde avlyttet Tysklands forbundskansler Angela Merkels telefon, og at flere utenlandske ambassader var blitt avlyttet.

Saken vakte naturlig nok reaksjoner også i Norge, men etter Datatilsynets oppfatning var norske myndigheter tilbakeholdne med å kritisere den amerikanske overvåkingen. Også for Datatilsynet skapte saken usikkerhet og bekymring, både når det gjelder omfanget av overvåkingen og hvilken betydning den ville få for vår håndhevelse av regelverket. Saken kunne få stor betydning for norske kommuner som lagret data hos amerikanske selskaper slik som Google og Microsoft.

Datatilsynet reagerer

I august sendte derfor Datatilsynet et brev til daværende justisminister Grete Faremo[2]. Her ba vi statsråden forsøke å bringe på det rene hva slags data som var samlet inn, og fra hvilke kilder. Særlig bekymringsfullt var det selvsagt at det var samlet inn data fra selskaper som norske borgere bruker kontinuerlig, slik som Google, Facebook og Microsoft. Det var også viktig å få avklart hva kriteriene var for at NSA kunne samle inn data om norske borgere, og ikke minst om det var noen domstolskontroll knyttet til innsamlingen og bruken av personopplysningene.

Svaret fra statsråden var utfyllende og nyttig, men dessverre ikke beroligende. Som vi antok var det ingen domstolskontroll knyttet til hver enkelt sak, kun en kontroll utført av den såkalte FISA-domstolen[3], og som gjaldt lovligheten av selve overvåkingsprogrammet. Dette kan sammenlignes med at datalagringsdirektivet ble godkjent av en domstol som helhet, og at det deretter var opp til politiet selv å hente ut data i overensstemmelse med domstolsvedtaket. Fra et rettssikkerhets- og personvernperspektiv er dette helt uakseptabelt.

I kjølvannet av avsløringene fikk Datatilsynet mange henvendelser om lagring av data i skyen nå ville bli forbudt. Dette var særlig knyttet til to avgjørelser fra 2012, der Datatilsynet godtok at Moss og Narvik kommune tok i bruk skytjenester fra henholdsvis Microsoft og Google. Vår foreløpige konklusjon var at avsløringene kunne få betydning for den risikovurderingen som alle behandlingsansvarlige må foreta før de tar i bruk skytjenester, og at vi ville vurdere å gjennomføre tilsyn mot virksomheter og kommuner som lagrer i skyen i 2014.

Kritikken øker

Utover høsten og vinteren økte kritikken mot amerikanske myndigheter. Også teknologigigantene selv reagerte. Flere selskaper har de siste årene publisert såkalte *transparency reports* der de gir opplysninger om hvor mange forespørsler om utlevering som kommer fra myndighetene i ulike land.

---

[2] Se Datatilsynets samleside for PRISM: http://www.datatilsynet.no/Sektor/Politi-justis/overvaaking-PRISM/

[3] Amerikansk domstol som godkjenner program som overvåker utenlandske borgere.

I disse kan vi for eksempel lese at norske myndigheter i første halvår av 2013 rettet 205 henvendelser til Microsoft (i tillegg til 40 henvendelser som gjaldt Skype). Det var utelukkende snakk om informasjon om abonnenten, ikke innhold fra kommunikasjonen[4]. I august 2013 varslet Google og Microsoft at de ville gå til søksmål mot amerikanske myndigheter. Dette fordi de ønsker å vise mer åpenhet om hvilke opplysninger de blir bedt om å utlevere i medhold av blant annet FISA-regelverket[5].

Også blant andre personvernmyndigheter vakte saken sterke reaksjoner. Berlin-gruppen, et globalt ekspertorgan på personvern, avga i september 2013 en resolusjon der det ble understreket at det var en viktig menneskerett å kunne kommunisere fritt, også ved hjelp av elektroniske hjelpemidler, og at det måtte utvises mye større åpenhet om hva slags overvåking som ble utført, samt at det måtte gis bedre informasjon til de som ble overvåket i etterkant[6]. Datatilsynet deltok aktivt i debatten og ga innspill til denne resolusjonen.

Bryr folk seg i Norge?

Hvilken betydning har saken så hatt for den enkelte norske borger? I november 2013 gjennomførte Datatilsynet en større befolkningsundersøkelse der vi blant annet ønsket å se på hvor god kjennskap folk flest har til denne saken, deres holdning til det som hadde skjedd og hvordan saken hadde påvirket deres vilje til å kommunisere[7].

Undersøkelsen viste at så å si alle (94 prosent) nordmenn over 15 år har hørt om Snowden-saken. Vi spurte hva de mener om den amerikanske overvåkingen. Hele 72 prosent uttrykte bekymring ved å indikere at overvåkingen er «uakseptabel» eller «bekymringsverdig, men nødvendig». At 27 prosent mener overvåkingen er «bekymringsverdig, men nødvendig» illustrerer at det kan være vanskelig for folk flest å bedømme i hvilken grad et overvåkingstiltak er nødvendig for å avverge terror eller alvorig kriminalitet. Kun tolv prosent mente at overvåkingen er uproblematisk.

Nedkjøling etter Snowden?

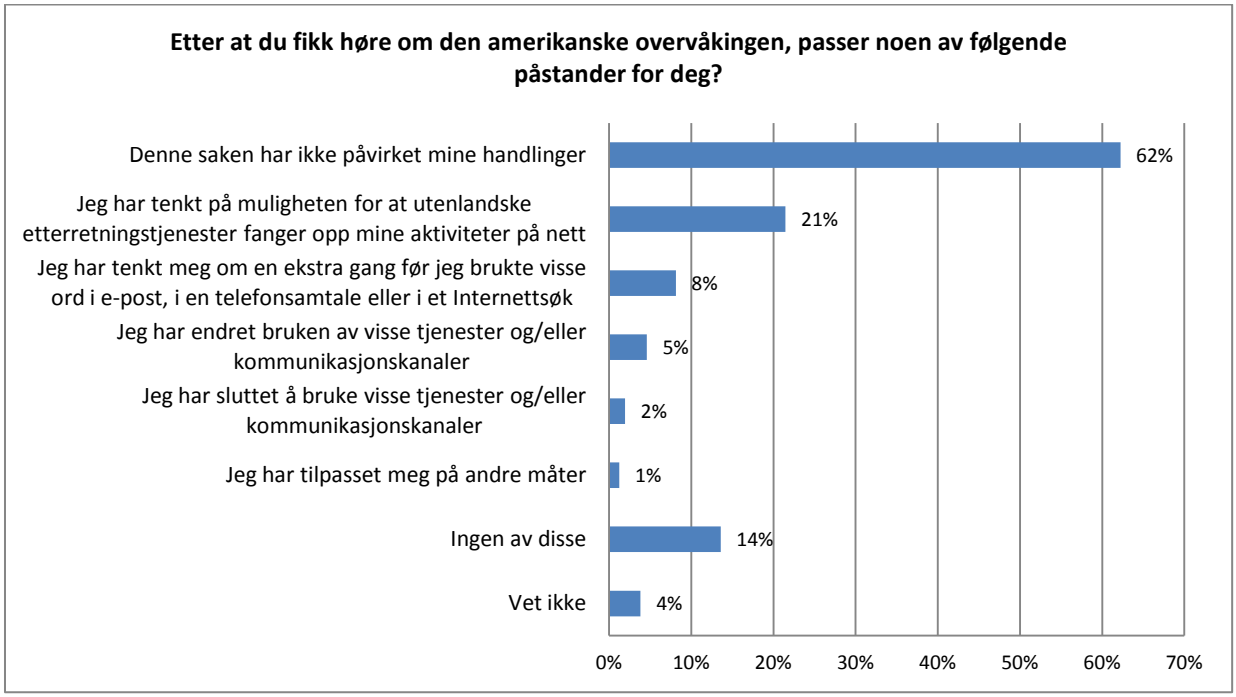
Den store majoriteten synes altså at den massive overvåkingen som er kommet for dagen er bekymringsverdig. Men fører bekymringen til at nordmenn legger om sine kommunikasjonsvaner fordi de frykter hvordan sporene de legger igjen kan brukes av amerikanske, eller andre etterretningsmyndigheter?

Mennesker som vet at de kan bli iakttatt, endrer ofte oppførsel – tillitten til omgivelsene endres. Hvis vi er usikre på hvem som har tilgang til opplysningene vi legger igjen, er vi tvunget til å ta hensyn til denne usikkerhetsfaktoren. Vi vil begynne å tenke gjennom hva vi skriver, hva vi foretar oss og hvem vi har kontakt med. Fenomenet omtales som nedkjølingseffekt, eller *chilling effect* på engelsk. En sentral følge av nedkjølingseffekten, er press på ytringsfriheten, noe som i neste konsekvens kan svekke demokratiet ved at borgerne begrenser sin deltakelse i den åpne meningsutvekslingen.

Kan vi se tegn til nedkjølingseffekt i Norge som direkte følge av Snowden-avsløringene? I USA har for

[4] https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
[5] http://www.nbcnews.com/technology/google-microsoft-efforts-stalled-release-government-data-requests-8C11045508
[6] http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group
[7] *"Personvern – Tilstand og trender 2014"*, Datatilsynet og Teknologirådet, Oslo

eksempel Electronic Frontiers Foundation anlagt sak mot NSA på vegne av 22 organisasjoner som mener de har opplevd nedkjølingseffekt som en direkte konsekvens av NSAs overvåking[8]. Å måle graden av nedkjølingseffekt i samfunnet er en krevende øvelse. Det er vanskelig å kvantifisere *fravær* av handling. Vi har forsøkt å få et inntrykk av om det er tendenser til nedkjølingseffekt ved å spørre folk om de har endret eller lagt bånd på sin kommunikasjon etter Snowden-saken.



Undersøkelsen viser at Snowden-saken ikke synes å ha hatt en sterk nedkjølingseffekt på norske borgere. Seks av ti oppgir at denne konkrete saken ikke har påvirket deres handlinger. Dette til tross for at majoriteten av de spurte mener at overvåkingen enten uakseptabel eller bekymringsverdig. Dette kan skyldes flere forhold.

For det første gjenspeiler nok svarprosenten hvor vanskelig det er å legge om på sine digitale vaner selv om man føler ubehag knyttet til hvordan etterretningstjenestene arbeider. For det andre er det nok fortsatt slik at majoriteten av befolkningen i Norge ikke opplever å være interessante for etterretningstjenestene. De fleste vil tenke at overvåkingen er rettet mot grupper de ikke inngår i eller har befatning med selv – de føler seg ikke rammet på et personlig nivå. Dette til tross for at Snowden-avsløringene nettopp har vist at dagens etterretningsmyndigheter samler inn data om folk flest, ikke kun bestemte grupper. For det tredje er det antageligvis også mange som tenker at selv om myndighetene ser gjennom alle deres data, så betyr ikke det noe ettersom de ikke har noe å skjule allikevel. Dessuten har nordmenn generelt høy tillitt til myndighetene. Folk har tillitt til at etterretningstjenestene ikke vil misbruke informasjonen som samles inn, og at det derfor er trygt å fortsette som før.

[8] https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association

Åtte prosent av de spurte har imidlertid tenkt seg om en ekstra gang før de brukte visse ord i sin korrespondanse og i internettsøk. Det er med andre ord indikasjoner på en svak nedkjølingseffekt etter Snowden-saken. Ser vi på tallene fordelt på alder, slår nedkjølingseffekten signifikant mer ut i aldersgruppen 15-29 år. Åtte prosent av de spurte i den yngste aldersgruppen, har endret bruken av visse tjenester, mot i gjennomsnitt fem prosent i de høyere aldersgruppene. At det er flere blant de unge som har endret på sine kommunikasjonsvaner, kommer antageligvis av at denne gruppen består av de mest aktive og allsidige brukerne av digitale tjenester. De lever store deler av sine liv på nett, og føler seg kanskje derfor i større grad utsatt og sårbare for overvåkingstrykket enn de som er eldre.

Tap av tillitt til Internett?

Kan Snowden-avsløringene føre til at vi stoler mindre på ulike aktører på Internett og derfor vil bruke nett i mindre grad? I USA har flere internettjenester stengt dørene i etterkant av Snowden-avsløringene. Dette gjelder blant annet Lavabit og Silent Circle, to leverandører av krypterte e-postløsninger. Lavabit forklarte nedleggelsen av tjenesten med at de "ikke ville stå i ledtog med myndighetene i overvåkingen av det amerikanske folk"[9].

Det norske selskapet Jottacloud som tilbyr nettskyløsninger, opplevde en voldsom kundetilstrømning etter Snowden-saken. Rett etter at saken ble kjent, gikk eierne ut og garanterte at de ikke ville gi ut lagret informasjon til myndigheter eller andre aktører uten rettslig kjennelse[10]. Dette førte til at de fikk mange nye kunder, også fra USA.

Tap av tillitt til Internett som kanal og arena for meningsutveksling, vil ikke bare ha negative konsekvenser for et levende og aktivt demokrati, det vil også ha alvorlige konsekvenser for den digitale økonomien. Det kan etter hvert være mange brukere, både selskap og privatpersoner, som for eksempel ikke ønsker å benytte e-handelsløsninger der de vet at hver eneste transaksjon blir indeksert og sporet av ulike lands myndigheter. Særlig europeiske virksomheter kan velge bort amerikanske skytjenester for å beskytte kundenes personvern.

Lyser varsellampene nå?

Sikkerhet og personvern blir ofte satt opp mot hverandre. Men i stedet for å se på dette som begreper i konflikt med hverandre, bør vi heller erkjenne at de tvert imot er gjensidig avhengig av hverandre. Begge verdiene er nødvendige om vi skal ha et fungerende demokratisk samfunn. Ivaretakelse av tillit er i denne sammenhengen et stikkord. En stadig mer inngripende overvåking vil føre til tap av tillitt til myndighetene i form av nedkjølingseffekt. Mister myndighetene tillitten i befolkningen, vil det være vanskelig for myndighetene å gi oss den sikkerheten og tryggheten vi ønsker. I ett klima preget av lav tillitt vil det også være utfordrende for etterretningsmyndighetene å gjøre en effektiv jobb – folket vil ikke lenger være på myndighetens side i kampen om å verne felles verdier. Et for sterkt overvåkingstrykk vil medføre tap av både personvern og sikkerhet[11].

Vår undersøkelse viser at Snowden-saken har hatt en svak nedkjølingseffekt blant norske borgere. Selv om kun åtte prosent av befolkningen oppgir å ha lagt bånd på sin kommunikasjon, gir tallet

[9] http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden
[10] http://e24.no/digital/snowden-saken-ga-kundeboom-for-norsk-nettsky/21106285
[11] van der Hilst, Rozemarijn: *"Putting Privacy to the Test: How Counter-Terrorism Technology is Challenging Article 8 of the European Convention on Human Rights"*, University of Oslo, 2013, Oslo

likevel grunn til ettertanke. En viktig forutsetning for et fritt og åpent demokrati er at *ingen* skal frykte konsekvensene av å ytre seg. Sikkerhet er viktig, men det er også vår trygghet for at personvernet ivaretas. Alternativet kan bli en nedkjølingseffekt som forringer det samfunnet vi vil ha, og som vi forsøker å beskytte.

Fra storebror til mange lillebrødre

I 2014 vil Google Glass trolig lanseres kommersielt. Google vil ta datamaskinen ut av lomma og sette den på nesa vår. Google Glass er et eksempel på såkalt *wearable computing*, eller kroppsnær teknologi. Bruk av slik teknologi vil øke kraftig i årene fremover. Google har fått mest oppmerksomhet for sine briller, men også andre aktører er ventet å lansere lignende produkter i løpet av året[12].

Kroppsnær teknologi er små elektroniske enheter som bæres tett på kroppen. Et sentralt kjennetegn ved slik teknologi er at den er i konstant interaksjon med brukeren – den er alltid aktivert. En annen viktig funksjon ved kroppsnær teknologi, er at den legger til rette for å kunne utføre flere handlinger på en gang. Det er ikke nødvendig å stoppe opp med det man holder på med for å bruke enheten. Du kan sykle, spille fotball eller sove, og samtidig bruke teknologien[13].

Kroppsnær teknologi er ikke et nytt konsept. Kalkulatorklokkene som kom på midten av 70-tallet er et tidlig uttrykk for slik teknologi. Det som er nytt med dagens teknologi, er langt større funksjonalitet og datakraft, gjerne i kombinasjon med internettilkobling og nettskylagring. Kroppsnær teknologi fungerer ofte i partnerskap med smarttelefonen, noe som åpner opp for en lang rekke ulike bruksområder for de kroppsnære enhetene.

Såkalte smarte briller er kanskje den formen for kroppsnær teknologi som har fått mest oppmerksomhet den siste tiden. Google Glass kan ta opp video og bilder, og gir tilgang til Internett via et skjermbilde som projiseres over bærerens høyre øye. Brillene aktiveres ved hjelp av taleteknologi, eller ved å stryke en finger langs brillestangen. Men det finnes også en lang rekke andre typer kroppsnær teknologi som allerede er på markedet, slik som små bærbare kameraer, et mangfold av trenings- og helsesensorer, smarte klær og smarte klokker. Snart vil sensorer puttes inn i alle mulige ting rundt oss for å gjøre dem også smarte. Da vil de kroppsnære enhetene kunne kommunisere med disse gjenstandene i våre omgivelser. Det digitale armbåndet som måler hjertefrekvens, søvnmønster og kondisjon, vil også kunne brukes til å slå på lyset når du våkner om morgenen. Det smarte kjøleskapet vil kunne sende en melding til de smarte brillene dine om at du mangler melk. Det er interessant å nevne i denne sammenhengen at Google nylig kjøpte selskapet Nest som spesialiserer seg på å lage smarte røykvarslere og termostater[14].

Personvernutfordringer

Kroppsnær teknologi kan brukes til mange gode formål. Smarte briller kan for eksempel bli et nyttig hjelpemiddel for folk med ulike funksjonshemninger. Brillene kan kobles opp mot smarthus-teknologi og bidra til at eldre mennesker kan klare seg hjemme lengre på egen hånd. Trenings- og helsesensorer kan hjelpe folk til en sunnere livsstil.

Bruk av kroppsnær teknologi fører naturlig nok også med seg en rekke personvernutfordringer. Utfordringene avhenger av hvilken funksjonalitet teknologien er utstyrt med. Ulike typer helse- og treningssensorer for eksempel, samler kun inn data fra brukeren av utstyret. I slike sammenhenger er

[12] http://www.wired.com/gadgetlab/2013/12/wearable-computers/
[13] http://en.wikipedia.org/wiki/Wearable_computer
[14] http://www.aftenposten.no/digital/Google-kjoper-roykvarsler--og-termostatfirma-for-20-milliarder-kroner-7432819.html#.Ut9_etLsQ-V

det bare personvernet til brukeren selv som blir berørt. For kroppsnær teknologi med kamera- og mikrofonfunksjonalitet er det annerledes. Denne typen kroppsnær teknologi er spesielt personverninngripende da den også berører personvernet til *menneskene rundt* brukeren av utstyret. Det er denne typen problemstillinger, knyttet til kroppsnær teknologi som også påvirker tredjeparter, vi vil diskutere i det følgende.

Usynlig grensesnitt

Kameraer er i dag rundt oss på alle kanter. Vi er vant til å se overvåkingskameraer i gater og butikker, og til å bli tatt bilder av og filmet av mobilkameraer i private og offentlige sammenhenger. Vi er klar over at det er en viss mulighet for at vi kan bli tatt bilde av. En utfordring med den nye kamerateknologien er at den har et grensesnitt som gjør det vanskelig å se *om* man blir filmet eller ikke. Brukeren har på seg enheten hele tiden og trenger ikke foreta en tydelig bevegelse eller lignende for å iverksette bilde og videopptak. Hvis noen går inn på en kafé med smarte briller, eller med et kamera hengende som et smykke rundt halsen, kan ikke de andre kafégjestene vite om deres handlinger og samtaler blir registrert eller ikke.

Det at vi ikke vet om vi blir tatt bilde av eller filmet, kan skape stor usikkerhet i omgivelsene rundt brukerne av kroppsbårne kameraer. Det begrenser vår mulighet til å ha privat eller anonym sosial omgang med andre. Alle har ulike grenser for hvor mye overvåking av våre personlige gjøremål vi synes er greit. For at vi skal kunne sette egne grenser, er det helt nødvendig at vi ser og vet hva som foregår.

Andres personopplysninger blir betalingsmiddel

Ved bruk av Google Glass er det ikke bare brillebæreren som potensielt benytter dataene som samles inn fra omgivelsene. Brillene er også et viktig datainnhøstingsverktøy for Google. Bilder, videoer, lyd, lokasjonsdata og annen personlig informasjon som fanges opp av brillene, blir lagret i Googles nettsky. I dag sammenstiller Google brukerdata fra sine ulike plattformer for å utvikle individuelle brukerprofiler benyttet i markedsrettet reklame, og for å utvikle nye tjenester. Blant annet skannes innholdet i e-poster til gmail-brukere for disse formålene. Det er ikke usannsynlig at Google også vil gjøre det samme med dataene som brillene samler inn.

Folk som blir fanget opp på bilder og film av Google Glass vil altså få sine personopplysninger lagret på Googles servere. Mens eierne av brillene har samtykket til Googles avtalevilkår før bruk, har ikke Google et slikt samtykke fra ”ikke-brukerne” av utstyret, selv om disse også blir berørt. Det er en utbredt og alminnelig akseptert forretningsmodell på nett at vi betaler med våre personopplysninger for å få tilgang til gratis (eller rimelige) tjenester. Ved bruk av slike produkter som Google Glass, vil brukeren i tillegg betale med *andres* personopplysninger.

Tap av anonymitet

Når vi er ute i offentligheten kan vi ikke forvente samme grad av privatliv som når vi er hjemme. Vi kan imidlertid ha en forventning om å ikke få vår ferdsel løpende registrert. Vi forventer at vi kan gå nedover gaten og at vi kan blande oss i mengden, uten at våre bevegelser blir fanget opp.

Det spesielle med kroppsnær teknologi er at den alltid kan være på og aktivert, uansett hvor folk er og hva de gjør. Muligheten til å bevege seg rundt anonymt blir enda vanskeligere når teknologi som

kan overvåke omgivelsene kan være over alt. Den friheten som teknologien gir ett menneske, kan dermed redusere friheten til et annet.

Teknologi slik som ansiktsgjenkjenning, bidrar ytterligere til å gjøre det utfordrende å ferdes sporfritt. Ved bruk av ansiktsgjenkjenning kan fremmede mennesker bli gjenkjent og identifisert på bilder. Ansiktsgjenkjenning sammenstilt med annen informasjon, kan brukes til å utlede hvor andre folk enn bæreren av enheten har vært, hva de har gjort og når de var der. Dette er attraktive data for markedsførere og andre kommersielle aktører som ønsker å nå spesifikke målgrupper. Slike data er interessante også for politimyndigheter i etterforskningssammenheng og for etterretningstjenestene.

Google har foreløpig ikke åpnet for bruk av ansiktsgjenkjenning i brillene sine, men vi kan ikke utelukke at andre aktører vil tillate dette i tilsvarende produkter.

Interessante data for politi og etterretningstjenestene

Myndigheter – særlig politi og etterretningstjenester – vil være interessert i å få tilgang til data registrert gjennom bruk av kroppsnær teknologi. Slike enheter vil samle inn enorme volum av «alltid på-data», data som vil være svært interessante i forbindelse med etterforskning av kriminalitet. Under en drapssak i Ålesund viste det seg at en syklist hadde filmet gjerningsmannen rett før gjerningen faktisk fant sted[15]. Det er selvsagt viktig at politiet så raskt som mulig får tilgang til data der de er å finne for å raskt oppklare alvorlige kriminelle handlinger. Samtidig er det også viktig å sikre at ikke myndighetene får tilgang til data samlet inn av kroppsnære enheter uten at de har en rettslig kjennelse.

Nedkjøling

Hvis vi er usikre på om noen overvåker oss, vil vi begynne å oppføre oss som om vi blir overvåket. Fenomenet som kalles nedkjølingseffekt, er nærmere omtalt ovenfor. Personvern handler blant annet om at vi skal ha mulighet til å kontrollere hvem vi kommuniserer med. Med kroppsbårne enheter på alle kanter, enheter som potensielt kan registrere hva vi gjør og sier, har vi ikke lenger kontroll over hvem som er vårt publikum. Vi vet heller ikke hvordan dataene som registreres om oss kan komme til å bli brukt senere. Dette kan føre til at vi legger bånd på oss selv i frykt for at vår oppførsel kan tolkes i et uheldig lys av andre, i en annen sammenheng. En slik nedkjølingseffekt har ikke bare negative konsekvenser for rammene for fri meningsutveksling, men vil også kunne hemme folks kreativitet og innovasjonslyst.

Mange lillebrødre i tillegg til storebror

Personvernlovgivningen beskytter folks privatliv først og fremst fra selskaper og myndigheter. Privatpersoner er unntatt fra loven om behandling av personopplysninger. Hva om vi nå får en utvikling der folk lager enorme søkbare registre over alt de ser og hører – at vi får en verden der det i tillegg til storebrødre finnes en milliard lillebrødre[16]? Bilder og lydopptak kan deles og offentliggjøres uten at de som er på opptakene, og dermed er lagret i andres private registre, har kunnskap om at dette skjer. Fra bildene og lydopptakene som samles inn, kan det utledes hvor andre personer har vært, hva de har gjort, hvem de har vært sammen med og til hvilken tid, og kanskje også hva de sier. Fremmede mennesker kan identifiseres ved hjelp av ansikts- eller stemmegjenkjenning. Kan en slik

[15] http://www.dagbladet.no/2013/09/06/nyheter/innenriks/drap/anja_weloy_aarseth/29125461/
[16] http://www.economist.com/news/briefing/21589863-it-getting-ever-easier-record-anything-or-everything-you-see-opens

utvikling gjøre det problematisk å holde personlig bruk av personinformasjon utenfor personvernlovgivningen fremover? Bør folk ha rett til å få sine data fjernet fra en annen persons ikke-kommersielle dataregister?

Leverandørene må ta ansvar

Det ligger et ansvar hos leverandører av teknologi som kan overvåke omgivelsene på denne måten, et ansvar for å gjøre dette på en måte som i størst mulig grad tar hensyn til folks personvern. Kommersielle aktører er avhengige av publikums tillitt. For at teknologien skal tas i bruk i stor skala, er aktørene avhengige av at folk føler seg komfortable rundt den nye teknologien. Å utvikle løsninger etter prinsippene for innebygd personvern, handler nettopp om å lage løsninger som ivaretar brukernes tillitt. Selskap som vil utvikle kroppsnær teknologi etter disse prinsippene må blant annet tenke på følgende forhold:

- **Tydelig grensesnitt:** Kroppsnær teknologi som også samler inn informasjon om tredjeparter, bør så langt det er mulig utformes slik at omgivelsene er klar over at dette skjer. Google Glass har blant annet fått kritikk for at brillene ikke ser ut til å gi et tydelig nok signal om når bilde- og videofunksjonaliteten er i bruk.
- **Åpenhet og formålsbestemthet**: Tilbyderne av kroppsnær teknologi må informere om hvilke data som samles inn og til hvilke formål de skal benyttes. Hvis leverandøren benytter dataene som brukerne samler inn, til videre analyse eller til bruk for nye formål, skal brukeren informeres og gi sitt samtykke til slik viderebruk av opplysningene.
- **Ansiktsgjenkjenning:** Dette er en teknologi som kan ha svært inngripende personvernkonsekvenser.
- **Sletting:** Brukeren må ha mulighet til å få slettet alle data som den kroppsnære enheten har samlet inn om vedkommende.
- **Dataportabilitet:** Det bør være mulig for brukeren å få utlevert alle sine data i et portabelt og brukervennlig format, slik at de kan overføres til en ny tjenesteleverandør hvis det er ønskelig.
- **God sikkerhet:** Kroppsnær teknologi kan samle inn svært sensitive opplysninger, blant annet om brukerens helsetilstand. Det er derfor viktig at enhetene lagrer og overfører data på en sikker måte. Hvis brukeren for eksempel mister sin smartklokke, er det viktig at ikke andre kan få tilgang til dataene som ligger lagret.

3. Nærmere om utvalgte områder

Helse og velferd

Helse og velferd angår hele befolkningen i samtlige livsfaser. Personopplysningene som behandles i sektoren er blant de mest sensitive opplysningene som finnes. Helsesektoren er avhengig av å benytte helseopplysninger både i pasientbehandlingen (primære formål) og for andre formål slik som forskning og kvalitetssikring (sekundære formål). Primærkilden til disse opplysningene er den informasjonen hver og en av oss formidler i fortrolighet og i tillit til helsepersonell når det er nødvendig å få helsehjelp.

Helsesektoren er preget av omfattende organisatoriske endringsprosesser i kjølvannet av samhandlingsreformen som skal sikre pasientene bedre koordinerte og sammenhengende helse- og omsorgstjenester. Disse prosessene har også stor innvirkning på håndteringen av helseopplysninger. Å innfri kravene til sammenhengende helse- og omsorgstjenester mellom primærhelse- og omsorgstjeneste i kommunene og spesialisthelsetjenesten ligger derfor til grunn for regjeringens plan om å realisere stortingsmeldingen *«Én innbygger – én journal – Digitale tjenester i helse og omsorgssektoren»*[17]. Parallelt pågår også regjeringens satsing på flere og bedre helseregistre i *«Nasjonalt helseregisterprosjekt»*. Helse- og omsorgsdepartementet har ut fra dette laget et forslag til nye lover om helseregistre og pasientjournaler. Disse skal behandles av Stortinget i 2014.

Utfordringene sett fra et personvernperspektiv, er om enkeltindividets krav på beskyttelse av sine opplysninger blir tilstrekkelig tatt vare på både innenfor helsetjenestene og ved bruk til andre formål enn helsehjelp. Pasientene gir fra seg svært mange opplysninger «i bytte» mot helsehjelp, og den enkelte synes å ha begrenset kunnskap om, og kontroll med, hvordan disse opplysningene benyttes og videreformidles til andre formål.

Datatilsynet har i meldingsåret vært i god og regelmessig dialog med både Helse- og omsorgsdepartementet og Helsedirektoratet om videre planlegging og utforming av pasientjournaler som skal tilfredsstille samhandlingsbehovene. Den foreløpig største personvernutfordringen rundt målsettingen om å ha én sammenhengende journal for hver pasient, er tilgangskontroll. Denne skal sikre helseopplysningene mot innsyn fra uvedkommende helsepersonell og administrativt personell innenfor helsetjenestene. En annen utfordring med én felles journal, er om det skapes muligheter for å skjerme spesielt sensitive opplysninger, slik som psykiatri, rus og for eksempel seksualrelaterte sykdommer, slik at disse opplysningene faktisk bare er tilgjengelige når det er et reelt behov for dem.

På tross av gode samarbeidsrelasjoner mellom Helse- og omsorgsdepartementet, Helsedirektoratet og Datatilsynet, ser vi tydelig at vi i større grad bør trekkes inn så tidlig som mulig i utforming av premissene for utviklingen som angår forvaltning og organisering av helseopplysninger. Det er mange sektorspesifikke hensyn å ivareta i store IKT-utviklingsarbeider innenfor helseområdet, og erfaringene viser at kravene i utredningsinstruksen om konsekvensvurderinger for personvern ikke

[17] Meld. St. 9 (2012-2013)

overholdes. Både en rapport fra Direktoratet for forvaltning og IKT (Difi)[18] og Riksrevisjonens undersøkelse av kvaliteten på offentlige utredninger[19], bekrefter våre erfaringer med mangelfulle konsekvensutredninger. En slik praksis øker risikoen for en for ensidig vektlegging av sektorinteresser og ansvar, mens det overordnede samfunnsansvaret og ansvaret for enkeltindividene, ikke blir ivaretatt. I slike utredningsprosesser kommer ofte personvern for sent inn i prosessen og blir oppfattet som et hinder, fremfor en god mulighet til å få et balansert beslutningsgrunnlag med nødvendige avveininger mellom samfunnets og enkeltindividets interesser. Gode personverntiltak vil i tillegg kunne bidra til å verne om tillitsforholdet mellom helsetjenestene og befolkningen.

Teknologiutviklingen gir stadig flere muligheter til å skaffe ny informasjon om befolkningens nåværende og fremtidige helse, ved blant annet bruk av genetiske opplysninger. Tempoet i utviklingen av analyseverktøy for genetisk materiale (genomsekvensering), har bokstavelig talt tatt av og sprengt grensene for forventet anvendelse i vår tid.

Det utvikles også nye teknologiløsninger som kan gi den enkelte en viss kontroll med, og informasjon om, egen helse på en del områder gjennom «apper», nettjenester og andre former for velferdsteknologi. Denne type informasjon kan dels være innenfor og dels utenfor helsesektorens kontroll. Det betyr samtidig at private aktører i stadig større grad får tilgang til befolkningens helseopplysninger, og at det er vanskelig å ha oversikt over om informasjonen benyttes til andre formål enn til den tjenesten som ytes til kunden. Med en slik utviklingstakt er det enkleste å være positiv og mulighetsorientert, men det er også helt nødvendig å stille krav til grundige sårbarhets- og risikovurderinger både for samfunnet som helhet og for hver og en av oss. Det blir derfor viktig å trekke opp tydelige grenser for når forvaltningen har beslutningsmyndighet, og når Stortinget må trekkes inn for å opprettholde den nødvendige demokratiske kontroll og regulering av dette området.

Kombinasjonen av store endringer i sektoren og rask teknologiutvikling representerer altså både muligheter og utfordringer. Derfor ser Datatilsynet det som viktig at det blir gitt klare føringer for økt brukermedvirkning og effektiv bruk av innebygd personvern for utviklingen av fremtidige IKT-løsninger i sektoren.

Brukermedvirkning er også et sentralt element for å ivareta enkeltindividets krav på personvern. Utfordringene rundt medvirkning fra pasienter og brukere er å sørge for at mangfoldet av pasientinteresser er representert, og å sikre at de som medvirker har den nødvendige innsikten til å være reelle representanter for samtlige pasientgrupper, også de mest sårbare.

Hva er gjort på området?

Genteknologi

Genetiske opplysninger utledes av biologisk materiale, blant annet fra ulike typer blod-, celle- og vevsprøver som enkeltpersoner hovedsakelig leverer fra seg i forbindelse med nødvendig helsehjelp. Det er nå mulig å utlede genetiske opplysninger fra biologisk materiale i et helt annet omfang enn det eksisterende lovverket synes å ivareta. Først og fremst gir slike nye helseopplysninger gode muligheter for bedre diagnostisering og forskning på årsaker til sykdom, noe som uten tvil et gode for

[18] Difi-rapport 2012:8 ISSN 1890-6583, *"Graves det dypt nok?"*, Om utredningsarbeidet i departementene.
[19] Riksrevisjonen, dokument 3:10 (2012-2013) – Riksrevisjonens undersøkelse av om offentlige tiltak utredes på en tilfredsstillende måte

befolkningen. Men, i ytterste konsekvens kan slik informasjon avdekke «menneskehetens, nasjonens eller familiens sårbarhet», samt en uendelighet av mulige sykdomsdisposisjoner hos hver enkelt av oss. Vi antar også at kommersielle interesser, myndigheter og andre vil ha en stadig økende interesse i slikt materiale i fremtiden.

Det utleveres genetiske opplysninger fra pasientjournaler til flere sentrale helseregistre. En sentral personvernutfordring er at befolkningen har mangelfull kunnskap om det omfattende materialet som er lagret i landets biobanker. Vi har grunn til å tro at befolkningen også har svært begrenset kunnskap for å forstå det informasjonspotensialet som genetiske opplysninger gir. Datatilsynet mener at dette avdekker 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. For det tredje vil en giver av biologisk materiale og genetiske opplysninger også gi informasjon om sine barn, sine foreldre og slektninger. Dette kommer i konflikt med at den enkelte i utgangspunktet skal kunne bestemme over bruken av egne genetiske opplysninger og biologisk materiale.

Datatilsynet utarbeidet en rapport i 2012 om disse problemstillingene, «*Personvernutfordringer ved bruk av genetiske opplysninger».* Rapporten foreslo flere tiltak for å styrke personvernet på området. I meldingsåret arrangerte vi et seminar der vi presenterte og diskuterte rapporten og utfordringene på området med flere aktører fra helse- og forskningssektoren.

Velferdsteknologi

Velferdsteknologi har vært et sentralt tema for Datatilsynet i 2013, og vil også være det i tiden som kommer. En lovhjemmel for å kunne bruke sporingsteknologi på demente personer innen offentlig omsorg er trådt i kraft, og fokuset har blitt endret fra å handle om hjemmel til å benytte velferdsteknologi til å handle om *hvordan* slik teknologi kan benyttes på best mulig måte. Prinsippene for innebygd personvern er sentrale på dette området, og vi har arbeidet med å synliggjøre disse. Vi har holdt flere foredrag om dette temaet i 2013, og det har vært mye møtevirksomhet.

Datatilsynet er positiv til at velferdsteknologi tas i bruk. Teknologien kan gi personer med nedsatt funksjonsevne økt selvstendighet, trygghet og mobilitet. Vi støttet derfor endringene i pasient- og brukerrettighetsloven som åpner opp for bruk av GPS overfor personer uten samtykkekompetanse. Bruk av slikt utstyr vil kunne gi disse brukergruppene større frihet i hverdagen, og de pårørende økt trygghet.

Samtidig kan velferdsteknologi utfordre personvernet. Mange av løsningene vi ser i dag, innebærer en form for overvåking av enkeltpersoner. Det kan være lagring av bevegelsesmønster gjennom GPS-sporing, helseovervåking gjennom kroppssensorer og overvåking av atferdsmønster gjennom bruk av kamera og bevegelsessensorer. Nytten av teknologien må derfor avveies mot hensynet til personvernkonsekvensene, og disse konsekvensene må reduseres så mye som mulig gjennom samtykke, informasjon og tilfredsstillende sikkerhet, og ved at godt personvern bygges inn i løsningen fra starten av. Vi er særlig opptatt av at overskuddsinformasjon ikke lagres og brukes til andre formål enn det som er intensjonen med bruken av teknologien.

I Stortingsmeldingen *«Personvern – utsikter og utfordringar»* poengteres det at offentlige myndigheter bør være en pådriver for bruk av innebygd personvern. Vi er derfor opptatt av å fortsette den gode dialogen med kommuner, næringsliv og kompetansemiljøer for utvikle og diskutere nye felles løsninger. Vi ønsker også å sette personvern på agendaen ved bruk av omsorgsteknologi. Dette vil vi for eksempel gjøre gjennom å delta på konferanser og samlinger hvor fagmiljøene møtes. I tillegg ønsker tilsynet å formidle personvernperspektivet gjennom å skrive fagartikler og gjennom å gi relevant veiledning.

Datatilsynet vil i 2014 bidra til at det lages nødvendig veiledning på området, enten i regi av Normen eller av andre aktører. I Stortingsmeldingen *«Morgendagens omsorg»*[20] fremheves behovet for standardisering på velferdsteknologiområdet. Hvis personvernhensyn blir innarbeidet i utviklingsfasen ligger forholdene til rette for å lage fremtidige systemer som ivaretar personvernet på en god måte. Tilsynet ønsker å bidra i standardiseringsarbeid, og har for eksempel hatt møte med en interesseorganisasjon i denne forbindelse.

Vi planlegger også å gjennomføre tilsyn innenfor temaet velferdsteknologi. Formålet med tilsynene er blant annet å få informasjon om hvordan velferdsteknologi anvendes i dag, for å klargjøre hvordan vi skal arbeide videre innen dette feltet.

GE-sakene og informasjonsplikt – Personvernnemnda

Datatilsynet fikk i 2012 kunnskap om 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 til leverandøren, og omfattet blant annet pasienters navn, ID-nummer, fødselsdato og helseopplysninger. Avviket gjaldt elleve virksomheter i Norge. Det ble opprinnelig meldt til tilsynet at dette gjaldt 126 344 pasienter, men dette antallet er ikke verifisert.

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 slik at GE har kunnet hente ut helseopplysninger uten tekniske hindre.

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

Vedtakene om å informere pasientene om hendelsen ble påklaget av flere av virksomhetene, og sakene gikk i 2013 til Personvernnemnda. Der fikk tilsynet medhold i at virksomhetene hadde informasjonsplikt overfor pasientene. Dette resultatet er, etter Datatilsynets vurdering, en styrking av pasientenes rettigheter, i og med at pasientene har fått en rett til å bli informert konkret om noe som angår dem.

Kobling mellom reseptregisteret og HUNT 2 – Personvernnemnda

Datatilsynet har tidligere gitt konsesjon til et kortvarig og avgrenset prosjekt som tillot kobling mellom befolkningsundersøkelsen HUNT 2 og reseptregisteret, uten at det forelå eksplisitt samtykke til en slik kobling fra de som var registrert i HUNT. Vilkårene for konsesjonen var knyttet opp mot

[20] Meld. St. 29 (2012–2013)

prosjektets tematiske og tidsmessige avgrensning. Etter at konsesjonen var utløpt ble det søkt om forlengelse og utvidelse av konsesjonen. Ettersom vilkårene i den foregående konsesjonen ikke lenger var til stede, ble en ny konsesjon gitt under den forutsetningen at det ble innhentet samtykke fra de registrerte deltakerne i HUNT. Dette kravet ble påklaget, og Personvernnemnda behandlet saken i 2013.

Nemnda kom frem til en annen konklusjon enn Datatilsynet etter en fortolkning av det generelle og brede samtykket som de registrerte deltakerne i HUNT 2 hadde gitt til å benytte «andre helse- og sykdomsregistre». Nemnda legger derfor til grunn et samtykke som ble avgitt *før* reseptregisteret ble opprettet, og at dette registerets eksplisitte krav til de registrertes samtykke omfattes av et tidligere avgitt bredt samtykke.

Avslag på konsesjonssøknad om å opprette nasjonale helseregistre

Datatilsynet har i 2013 avslått to søknader om konsesjon til å opprette nasjonale helseregistre. Det ene registeret gjaldt samtlige HIV-pasienter i Norge. Den andre søknaden gjaldt en registersamling basert på den såkalte fellesregistermodellen (samme modell som ble benyttet for hjerte- og karregisteret), og inkluderer flere pasientgrupper som blir behandlet med biologiske legemidler.

Avslagene er begrunnet med at en konsesjon fra Datatilsynet ikke er tiltenkt som regulering av varige nasjonale registre. Slike registre skal opprettes etter helseregisterlovens spesielle regler, i disse tilfellene ved forskrift eller lov. Begge sakene er påklaget og oversendt Personvernnemnda for en avgjørelse.

Ny helseregisterlov og ny pasientjournallov – høringsuttalelse

I 2013 sendte Helse- og omsorgsdepartementet forslag til ny lov om helseregistre og ny lov om pasientjournal på høring. Datatilsynet støttet at gjeldende helseregisterlov deles opp i to lover, en for behandlingsrettede helseregistre og en for helseregistre til bruk for styrings-, administrasjons- og forskningsformål.

Datatilsynet hadde vesentlige innvendinger til at pasientenes rett til selvbestemmelse svekkes, og mener denne retten må *styrkes* i begge lovforslagene. Videre presiserte vi at pasientjournalloven må utformes tydeligere, med klare krav til informasjonssikkerhet og tilgangsstyring basert på de reelle behovene for informasjon. Reguleringen må samsvare med reglene om taushetsplikt og pasientenes krav på beskyttelse av opplysninger om seg selv. Et «implisitt» samtykke til helsehjelp kan ikke benyttes for enhver tilgang til journalopplysninger. Det må skilles mellom for eksempel akuttlignende behandling og planlagt behandling der effektivitetshensyn ikke bør veie tyngre enn pasientens selvbestemmelsesrett. Det ble understreket at en ny helseregisterlov bør videreføre hovedregelen om at pasientene skal samtykke til at opplysninger fra helsetjenesten skal utleveres og brukes til andre formål. Informasjonsplikt og en reell reservasjonsadgang for pasienten bør utformes på en tydelig måte.

Vi synes presiseringene om pasientenes medbestemmelsesrett er godt i samsvar med regjeringens politiske føringer om at pasientene skal stå i sentrum for en videreutvikling av helsetjenestene. Vi ser det som uheldig at lovforslaget ikke skiller mellom hvilke typer helseregistre som krever lovbehandling, hvilke helseregistre det er adgang til å opprette med forskrift fra regjeringen og hvilke typer helseregistre som kan opprettes i medhold av konsesjon fra Datatilsynet. I lovutkastet går det

frem at regjeringen skal ha de fullmakter som Stortinget har i dag. Datatilsynet mener viktige demokratihensyn taler for at Stortinget fortsatt skal avgjøre om nye nasjonale helseregistre skal opprettes uten pasientenes samtykke. Det er også nødvendig med tydelige grenser for hvilke helseregistre som kan opprettes av regjeringen i forskrift og hvilke som skal opprettes i medhold av konsesjon fra Datatilsynet.

Avslutning av Kreftregistersakene – spørsmål om personvernmyndighetens uavhengige stilling

I 2009 og 2010 traff Datatilsynet to vedtak overfor Kreftregisteret angående manglende sletting av helseopplysninger fra screeningprogrammene for brystkreft (Mammografiprogrammet) og livmorhalskreft. Kreftregisteret måtte slette opplysninger om kvinner med negative funn, og en eventuell videre behandling av opplysningene måtte baseres på kvinnenes frivillige og uttrykkelige samtykke. Vår lovforståelse ble opprettholdt av Personvernnemnda i 2009-saken. I 2012 sendte regjeringen to endringer i kreftregisterforskriften på høring. Disse endringene skulle erstatte samtykkevilkåret med en reservasjonsadgang. Endringene var ment å gjelde tilbake i tid, slik at de opplysningene vi hadde pålagt slettet, allikevel skulle kunne oppbevares uten kvinnenes samtykke.

I vår høringsuttalelse stilte vi spørsmål ved om tilbakevirkningsforbudet i Grunnloven kunne være til hinder for en slik endring. Videre pekte vi på at en slik endring i forskriften, i praksis ville oppheve våre enkeltvedtak, slik de også var stadfestet av Personvernnemnda. Vi viste til at personopplysningsloven har et forbud mot at Kongen eller departementet gir instruks om eller omgjør personvernmyndighetenes «utøving av myndighet i enkelttilfeller etter loven». Vi ba derfor om at departementet vurderte sin egen kompetanse i lys av dette forbudet. Departementet besluttet i stedet å fremme endringene som et lovforslag. Endringene ble, uten høringsrunde, vedtatt av Stortinget sommeren 2013.

Funn fra tilsyn

Informasjonsplikt ved utlevering til sentrale helseregistre

Høsten 2013 ble det gjennomført 15 brevkontroller med virksomheter som utleverer helseopplysninger til de sentrale helseregistrene. De som ble kontrollert var fastleger, spesialister og helseforetak. Det er sentralt for pasientenes mulighet til å ivareta sitt eget personvern at de informeres i samsvar med regelverket. Resultatet fra kontrollene var nedslående; generelt informeres ikke pasienten om at helseopplysninger blir utlevert til sentrale helseregistre, slik som for eksempel Norsk pasientregister og Kreftregisteret.

Datatilsynet har derfor varslet vedtak overfor de fleste av virksomhetene om at de må informere pasienten om at slik utlevering vil finne sted, og om at pasienten har rett til å sperre journalen etter pasient- og brukerettighetsloven.

Formaliserte arbeidsfellesskap

Helseregisterloven har som utgangspunkt at kun egne ansatte skal ha tilgang til, eller innsyn i, de helseopplysningene virksomheten er ansvarlig for. Det er gjort noen unntak fra dette, blant annet i forskriften om virksomhetsovergripende pasientjournal i såkalte formaliserte arbeidsfellesskap. Denne forskriften trådte i kraft høsten 2012, og åpner for at virksomheter som tilfredsstiller kravene i forskriften, og som inngår avtale om det, kan etablere en felles pasientjournal. For å undersøke om helsesektoren oppfyller denne forskriften, gjennomførte Datatilsynet seks kontroller høsten 2013.

Sentralt for disse kontrollene var å avklare hva som skal til for å kunne utgjøre et formalisert arbeidsfellesskap, hvilke type virksomheter som kan inngå en avtale om virksomhetsovergripende journal, hvilke tilgangsbegrensninger som skal gjelde, samt se på alternative samarbeidsformer som åpner for utveksling av helseopplysninger. Under kontrollene fant Datatilsynet blant annet deling av helseopplysninger som lovverket ikke åpner for, samarbeid som er i tråd med forskriften, men som mangler nødvendig avtaleverk, og samarbeid som oppfyller kravene i forskriften.

Sakene var ikke ferdigstilte ved årsskiftet.

Medisinsk fødselsregister og Kreftregisteret

Datatilsynet gjennomførte to brevlige kontroller som et ledd i oppfølgingen av rapporten om biologisk materiale (se omtale under Genteknologi lenger opp). Kontrollene ble gjort mot Medisinsk fødselsregister og Kreftregisteret. Vi ba om en redegjørelse rundt hvilke genetiske opplysninger som ble behandlet i registrene, og hvilke tiltak som ble gjort for å sikre at blant annet bioteknologilovens krav til behandlingen ble fulgt opp.

Erfaringene fra kontrollene var at registrene i begrenset grad behandlet genetiske opplysninger, og at opplysningene ble tilstrekkelig ivaretatt gjennom det generelle sikkerhetsregimet i registrene.

Justissektoren

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

Innen justissektoren setter personvernet grenser for statens maktbruk overfor sine borgere som en rettsverngaranti. 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 om hva som skjer 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 av Stortinget. Det er nødvendig både for å sikre forutberegnelighet for borgerne og for å sikre at forholdsmessigheten i tiltaket er belyst og vurdert i en bred, demokratisk prosess. Siden behandlinger 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 bidra til et tillitsbasert samfunn, hvor iverksettelse av kontrolltiltak overfor den enkelte må begrunnes særskilt, og der informasjon og åpenhet omkring offentlig myndighetsutøvelse er en selvfølge.

Hva er gjort på området?

Snowden-saken

Vår virksomhet innen justissektoren, var høsten 2013 preget av de såkalte Snowden-avsløringene. Avsløringene berører i liten grad vårt myndighetsområde som tilsynsorgan. Vi har allikevel vært aktive som ombud i den løpende debatten om denne saken, og forsøkt å belyse de utfordringene den reiser. I tillegg har vi stilt relevante spørsmål til Justis- og beredskapsdepartementet for å påskynde og bidra i deres kontakt med de amerikanske myndighetene.

Denne saken er nærmere omtalt i kapittel 2, under *Året med Snowden*.

Endringer i åndsverksloven – «fildelingsjakt»

Den 1. juli 2013 trådte endringene i åndsverksloven i kraft, slik at såkalt fildelingsjakt kan finne sted uten konsesjon fra Datatilsynet. Vi har i løpet av høsten mottatt 13 meldinger fra virksomheter som har iverksatt slik virksomhet, eller som har planer om det.

Implementering av SIS II

I april 2013 besluttet norske myndigheter at andre generasjon av Schengen informasjonssystem (SIS II) skulle tas i bruk i Norge, i samsvar med det vedtaket som ble fattet av EUs justisministre i mars samme år. Overgangen til SIS II innebærer at det nå kan lagres flere opplysninger i informasjonssystemet, for eksempel fingeravtrykk og foto av ettersøkte personer. Datatilsynet er tillagt kontrolloppgaver etter lov om Schengen informasjonssystem. Vi har oppdatert informasjonen om SIS på nettsidene våre i kjølvannet av implementeringen av SIS II, først og fremst for å gjøre rettighetshaverne etter regelverket i stand til å ivareta sine interesser.

RMI-saken – Personvernnemnda

I 2010 gjennomførte Datatilsynet en kontroll hos Rettsmedisinsk institutt (RMI), ved Folkehelseinstituttet. Det ble da avdekket at RMI hadde lagret sensitive personopplysninger fra straffesaker og andre oppdrag, uten at det var avtalt med deres oppdragsgivere. Datatilsynet mente at oppbevaringen ikke hadde behandlingsgrunnlag, og påla derfor instituttet å slette alle opplysninger som ikke ble behandlet i henhold til en databehandleravtale. Vedtaket ble påklaget til Personvernnemnda, som i meldingsåret opprettholdt tilsynet vedtak.

Kontaktmøter

Det er dessuten gjennomført en rekke kontaktmøter med relevante aktører i meldingsåret, blant annet PST, EOS-utvalget, Nasjonalt ID-senter og Justis- og beredskapsdepartementet.

Høringsarbeid

Det har det vært fremsatt flere lovendringsforslag som medfører utvidede fullmakter til både politiet og ulike forvaltningsorganer. Dette er tiltak som kan få store konsekvenser for den enkeltes personvern.

Forslag til endringer i tolloven – kontrollhjemler

Regjeringen la frem forslag om å endre tolloven for å gi Tollvesenet adgang til å benytte en rekke nye kontrolltiltak innen etatens ansvarsområde. Blant annet ble det foreslått å gi hjemmel til spaning (skjult observasjon), teknisk sporing, kameraovervåking og underretningsvirksomhet.

Datatilsynet stilte spørsmål ved om forslaget var i overensstemmelse med det europeiske personverndirektivet. Vi mente at forslaget ikke tilfredsstillende reflekterte de vilkårene og begrensningene som ligger i direktivet, og ser det nødvendig med en ny og grundigere utredning av forslaget for å sikre en regulering som er i overensstemmelse med våre internasjonale forpliktelser. Saken er ennå ikke ferdig behandlet i Finansdepartementet.

Endringer i politiloven – etablering av tiggerregistre

Regjeringen la frem forslag om å endre politiloven, slik at alle som samler inn penger på offentlig sted måtte melde fra til politiet om dette på forhånd. Politiet skulle kunne gi visse vilkår for innsamlingen, for eksempel begrense denne til nærmere angitt tid og sted. Forslaget var et sosialpolitisk tiltak, for å begrense antall tiggere uten å forby selve tiggingen.

Datatilsynet stilte spørsmål ved om det var nødvendig å etablere ett eller flere tiggerregistre for å administrere en slik ordning, og om det var nødvendig og betryggende at politiet selv administrerte slike registre. Vi la til grunn at behandlingsreglene for slike registre måtte reguleres særskilt.

Stortinget vedtok å innføre meldeplikt, og besluttet at det skulle reguleres i forskrift til politiregisterloven. En slik forskrift er ennå ikke trådt i kraft.

Endringer i passloven

Regjeringen fremmet forslag om å endre passloven, slik at politiet skulle få utvidet adgang til å benytte opplysninger fra passregisteret. Forslaget kom som en konsekvens av at Datatilsynet i 2010 vedtok at en slik bruk ikke var tillatt etter gjeldende rett.

I høringsuttalelsen skrev vi blant annet at vi frykter en utvikling der politiets adgang til å hente inn personopplysninger i etterforskningsøyemed blir regulert utenfor straffeprosessloven. Vi pekte på at hensikten med en slik lovgivning er å senke terskelen for politietterforskning, og at det dermed er en omgåelse av skrankene i straffeprosessloven. Dette er en type lovgivning som eventuelt bør reserveres for de mest alvorlige lovbruddene. Stortinget vedtok forslaget som trådte i kraft 21. juni 2013.

Forslag om å endre utlendingsforskriften

Regjeringen fremmet et forslag om å gi PST hjemmel til å søke direkte i utlendingsmyndighetenes dataregister og saksbehandlingssystem, for å ivareta sine oppgaver etter politiloven. Datatilsynet uttalte blant annet at vi frykter en utvikling hvor PSTs adgang til å hente inn personopplysninger i forbindelse med etterforskning reguleres utenfor straffeprosessloven. Vi pekte på at dette kan være en omgåelse av skrankene i straffeprosessloven. For å sikre klare ansvarsforhold bør det skje en utlevering av opplysninger fra Utlendingsdirektoratet (UDI) til PST, ikke at PST får egne tilganger til UDIs systemer. De foreslåtte endringen i forskriften er så langt ikke vedtatt.

Forslag om unntak fra advokaters taushetsplikt på skatte- og avgiftsområdet

Regjeringen fremmet et forslag om å gjøre unntak fra advokaters taushetsplikt på skatte- og avgiftsområdet. Datatilsynet pekte på betydningen av tillit i forholdet mellom advokat og klient. Vi advarer mot en utvikling med flere og flere, riktignok avgrensede, unntak fra taushetsplikten som hver for seg synes godt begrunnede. Vi mener det bør gjøres en samlet vurdering og prioritering av hvilke unntak som eventuelt bør og kan etableres, uten at det går på bekostning av dette tillitsforholdet. Vi anbefalte derfor Finansdepartementet om å avvente advokatlovutvalgets vurderinger og innstilling. Saken er fremdeles til behandling i Finansdepartementet.

NOU 2013:9 Ett politi – rustet til å møte fremtidens utfordringer

I meldingsåret sendte regjeringen det såkalte «*Politiutvalgets utredning om organisering og ressursforvaltning i politiet»* på høring. Utvalget ble nedsatt etter 22.julikommisjonens rapport. Datatilsynet uttalte at et politi som innfrir rimelige forventninger som samfunnet har, er nødvendig i en rettsstat. Når forventningene ikke innfris vil det vokse frem tiltak som har til hensikt å kompensere for dette. I den forbindelse pekte vi på fremveksten av privat etterforskningsvirksomhet. Vi pekte også på at flere forvaltningsorganer utstyres med stadig videre kontrollhjemler, for å kunne kompensere for manglende oppfølgning hos politiet. Dette er en utvikling som er uheldig av hensyn til både rettssikkerhet og personvern. Vi uttalte derfor at etterforskning og påtale også bør være prioriterte oppgaver for politiet i fremtiden.

Funn fra tilsyn

Hvilke kontrollobjekter som ble valgt ut, er et resultat av vårt valg av privat rettshåndhevelse som prioritert område i meldingsåret. Vi så på noen aktører som driver utrednings- og etterforskningsliknende virksomhet og valgte noen aktører fra denne gruppen.

Gjensidige forsikring – ulovlig utredningsvirksomhet

Datatilsynet gjennomførte i mai 2013 en kontroll hos Gjensidige Forsikring ASA. Hensikten var å kontrollere hvordan virksomheten behandler personopplysninger, særlig når de gjennomfører undersøkelser med tanke på å avdekke svik eller forsøk på svik (såkalt utredningsvirksomhet).

Kontrollen avdekket at selskapet benytter svært inngripende metoder i forbindelse med utredning. Blant annet blir det benyttet skjult observasjon og skjulte lyd- og bildeopptak for å dokumentere noens helseforhold. Samtidig ble det avdekket store mangler i selskapets internkontroll for behandling av personopplysninger i forbindelse med forsikringsvirksomhet generelt. Manglene var av en slik art og et slikt omfang at det forelå en uholdbar risiko for at selskapet skulle bryte med lovens øvrige bestemmelser.

Datatilsynet vurderte forholdene som så alvorlige at selskapet ble pålagt å betale 600 000 kroner i overtredelsesgebyr – det største gebyret Datatilsynet har ilagt så langt. Selskapet ble også pålagt å etablere internkontroll i samsvar med personopplysningsloven, innen 1. mars 2014. Dersom selskapet ikke innretter seg etter vedtakene vil tilsynets konsesjon fra 2005 falle bort. Selskapet fikk dessuten et pålegg om å slutte å benytte skjult observasjon og skjulte lyd- og bildeopptak for å belyse noens helseforhold. Det siste vedtaket er påklaget og oversendt til Personvernnemnda.

AS Skan-Kontroll – ulovlig analyse- og varslingstjeneste

AS Skan-Kontroll samler inn og behandler personopplysninger når de utfører kontrolltjenester for sine oppdragsgivere, i hovedsak innen detaljvarehandelen. Dette gjelder blant annet sensitive opplysninger om de ansatte hos oppdragsgiveren og deres kunder. I 2013 gjennomførte Datatilsynet et tilsyn hos selskapet.

Det ble da avdekket at det var uklare ansvarsforhold mellom Skan-Kontroll og selskapets kunder, som følge av mangler ved databehandleravtalene. Det ble også avdekket at selskapet har benyttet opplysningene utover det som var avtalt med oppdragsgiveren, i en såkalt analyse- og varslingstjeneste. Analysematerialet består av store mengder opplysninger som selskapet får fra egne kontrolltjenester, tilfeldige tips og media. Opplysningene blir analysert, og brukt til å varsle andre virksomheter. Formålet er å forhindre og oppklare straffbare forhold slik som underslag og butikktyverier. Opplysningene blir også utlevert til et selskap som gjør bakgrunnssjekk av personer.

Datatilsynet mener at selskapet ikke har behandlingsgrunnlag for en slik virksomhet, da dette er oppgaver som bare kan gjennomføres av politiet i tråd med straffeprosesslovens bestemmelser. De registrertes rettigheter var heller ikke ivaretatt ved behandlingen. En slik virksomhet skulle dessuten uansett ha hatt konsesjon fra Datatilsynet.

Skan-Kontroll er nå pålagt å avslutte sin analyse- og varslingstjeneste innen 1. april 2014. De må innen samme dato inngå nye avtaler med sine oppdragsgivere for å regulere kontrollvirksomheten.

Selskapet må i tillegg betale 600 000 kroner i overtredelsesgebyr. Vedtaket er påklaget, og vil bli oversendt Personvernnemnda for klagebehandling.

Securitas AS – uklare databehandleravtaler

Securitas AS samler inn og behandler personopplysninger når de utfører kontrolltjenester for oppdragsgiverne sine, i hovedsak innen detaljvarehandelen. Dette gjelder blant annet sensitive opplysninger om de ansatte hos oppdragsgiveren og deres kunder.

Datatilsynet gjennomførte i meldingsåret en kontroll hos Securitas, og kom til at denne type virksomhet medførte inngripende tiltak overfor den enkelte, uten at personvernet ble tilfredsstillende ivaretatt. Det ble blant annet avdekket at de ansvarlige manglet tilfredsstillende kontroll med slik virksomhet, samt uklare ansvarsforhold mellom Securitas AS og selskapets kunder som følge av mangler ved databehandleravtalene.

Som en konsekvens av dette ble selskapet ilagt et overtredelsesgebyr på 75 000 kroner.

Offentlig sektor

I april 2012 la regjeringen frem sitt digitaliseringsprogram *«På nett med innbyggerne»*, en strategi for å forbedre og effektivisere offentlige tjenester. Digitalisering betyr i denne sammenhengen å benytte moderne teknologi i kommunikasjonen mellom innbygger og offentlig myndighet, i saksbehandlingen, og i samhandlingen mellom offentlige instanser. For innbyggerne betyr dette flere nettbaserte offentlige tjenester. Når flere tjenester flyttes over på nett, skapes nye utfordringer for innbyggernes personvern.

Offentlig sektor er storforbruker av alle typer personopplysninger som særlig benyttes for å fastslå hvilke rettigheter og plikter næringslivet og den enkelte innbygger har. Det er derfor i både næringslivets og innbyggernes interesse at det offentlige har tilgang til korrekte personopplysninger. Ved deling og gjenbruk av personopplysninger, utfordres personopplysningslovens prinsipp om formålsavgrensning. Samtidig er det slik at teknologi gir muligheter for å utvikle og effektivisere offentlig sektor. For å sikre godt personvern ved utveksling og deling av personopplysninger mellom ulike offentlige instanser, og mellom offentlige og private aktører, må ansvarsforholdene være tydelige. For at innbyggerne skal kunne ivareta eget personvern, må de få informasjon om hvor opplysningene deres er, og hvilke formål de kan bli brukt til.

Hva er gjort på området?

Datatilsynets strategi

Datatilsynet lanserte i 2013 sin strategi for godt personvern i digitaliseringen av offentlig sektor. Dokumentet tar utgangspunkt i de områdene der forvaltningen har pågående digitaliseringsprosesser, eller der strukturene allerede er på plass. Strategien omtaler blant annet:

- Felles grunndataregistre
- Metadata
- eID
- Sikker digital postboks
- Felles teknologiplattform (Altinn)

I tillegg har strategien et vedlegg om innebygd personvern. Innebygd personvern er nøkkelen til godt personvern og god informasjonssikkerhet, også i fellesløsningene i offentlig sektor.

Folkeregisterprosjektet

Også i 2013 har Datatilsynet fulgt utviklingen i Skatteetatens prosjekt som har som mål å realisere nytt folkeregister. Vi har deltatt i referansegruppemøtene som har vært avholdt, og vi har gitt våre innspill i kommentarrunden knyttet til valg av ny indikator (nytt fødselsnummer). Der ga vi vår støtte til prosjektets forslag om å videreføre dagens system med elleve siffer, men med en annen bruk av kontrollsifrene enn i dag.

Meldingsutveksling internt i forvaltningen

Vi har blitt løpende orientert om Direktoratet for forvaltning og IKT (Difi) sitt arbeid med å utrede en fremtidig løsning for meldingsutveksling internt i forvaltningen, og vi har gitt våre synspunkter til i deres arbeid med en forstudierapport.

Bistand til veiledningsarbeid

Fornyings-, administrasjons- og kirkedepartementet ba våren 2013 Datatilsynet bistå i arbeidet med to veiledere. Den ene skulle være en veileder om etterlevelse av personopplysningslovens ulike informasjonsregler, både reglene om generell informasjon om behandling av personopplysninger og reglene om innsynsretten til den registrerte. Dette inkluderte maler for hvordan informasjonen kan utformes på en pedagogisk måte.

Den andre veilederen skulle være et utkast til internkontroll og informasjonssikkerhet for offentlig sektor. Begge veilederne ble skrevet og sendt til departementet høsten 2013.

Høringsarbeid

Kravspesifikasjon for sikker digital postboks

Difi hadde kravspesifikasjonen for sikker digital postboks på høring. Datatilsynet er positiv til opprettelsen av en sikker digital posttjeneste for kommunikasjon mellom innbyggere og forvaltningen, men mener denne ordningen burde være særskilt regulert i egen lov eller forskrift knyttet til digitale posttjenester. I høringsuttalelsen pekte vi også på at det er viktig å minimalisere oppbyggingen av nye offentlige personregistre, og at det meste av funksjonaliteten for digital postboks kan løses med registreringer i kundeforholdet mellom postbokstilbyder og innbygger. Vi understrekte dessuten viktigheten av å tilby kvalifiserte sertifikater der det skal sendes sensitive personopplysninger, og at det er viktig å tydeliggjøre hvor behandlingsansvaret faktisk ligger.

Endringer i e-forvaltningsforskriften

Fornyings-, administrasjons- og kirkedepartementet hadde forslag til endringer i e-forvaltningsforskriften på høring. Våre tilbakemeldinger reflekterte det vi skrev i høringen knyttet til kravspesifikasjon for sikker digital postboks (se over). Sentralt i endringen til digital kommunikasjon, er at man går fra samtykke til reservasjon som hovedregel. Dette var allerede vedtatt, og var derfor ikke en del av denne høringen.

I uttalelsen stilte vi spørsmål til hvorfor man søker å kun forskriftsregulere én elektronisk posttjeneste, når det finnes flere som faktisk er i bruk. Vi savnet stillingtaken til om tjenester slik som den allerede etablerte meldingstjenesten i Altinn, faller innenfor reguleringen eller ikke. Vi etterlyste også en større tydelighet på Datatilsynets rolle som tilsynsmyndighet innenfor informasjonssikkerhet. Som i høringen knyttet til digital postboks, drøftet vi også her utfordringene med å plassere behandlingsansvaret for kommunikasjonens innhold. Opprettelse av unødvendige latente kontoer var en annen problemstilling vi tok opp.

Funn fra tilsyn

Tilsyn med stat, fylke og kommune

I meldingsåret gjennomførte vi 15 tilsyn i stat, fylke og kommune, hvor tema var deres behandling av personopplysninger, særlig i forbindelse med plikten til å innføre internkontroll og å sørge for

tilfredsstillende informasjonssikkerhet. Kontrollene fordelte seg på ni kommuner, tre departement, et direktorat, en fylkesmann og en fylkesnemnd for barnevern og sosiale saker.

Disse objektene er forskjellige både når det gjelder organisering, hvor mange personopplysninger som behandles og sensitivitetsgraden på opplysningene som behandles. Departementene pekte seg klart ut ved å behandle færre og mindre sensitive personopplysninger, mens kommunene og fylkesnemnda for barnevern og sosiale saker, befinner seg i den andre enden av sensitivitetsskalaen.

Datatilsynet fant mangler hos alle de kontrollerte, spesielt knyttet til internkontrollplikten. De fleste manglet en fullverdig oversikt over hvilke behandlinger etaten gjorde. Dessuten var rutinene for generell informasjonsplikt og den registrertes rett til innsyn kritikkverdige. Det var også påtakelig at jo flere og jo mer sensitive personopplysninger som ble behandlet, jo mer mangelfull var etatens rutiner. Informasjonssikkerheten var generelt bra, men det var også her alvorlige mangler knyttet til risikovurderinger, særlig ved bruk av risikoutsatte medier slik som minnepenn, telefaks og lignende. Det var også en del mangelfulle databehandleravtaler.

På bakgrunn av dette sendte Datatilsynet brev til alle statlige virksomheter, med oppmoding om å gjennomføre en egenkontroll for å se om internkontrollen og informasjonssikkerheten var på plass.

Skole, barn og unge

Barnehager, grunnskoler og videregående skoler behandler store mengder opplysninger om barn, elever og foresatte. Opplysningene befinner seg gjerne på tradisjonelle lagringssteder slik som i papirbaserte arkiv, permer, notatbøker, ranselpost og lignende. Den teknologiske utviklingen har imidlertid ført til at opplysninger om barnehagebarn og elever i skolen i større grad enn tidligere behandles digitalt. Opplysningene befinner seg nå blant annet i saksbehandlingssystemer, skoleadministrative systemer, læringsplattformer, innloggingstjenester på Internett og digitale læringsressurser.

Det er mange aktører i sektoren, og kunnskapen om personvern blant barnehageeiere, skoleeiere, lærere og leverandører av digitale tjenester viser seg å være veldig varierende. Dette skaper utfordringer for personvernet fordi systemene som tas i bruk fordrer både at bestillerne (fylkeskommune, kommune, barnehage, skole) evner å sette de begrensningene som personopplysningsloven krever, og at leverandørene evner å tilby løsninger som legger til rette for og ikke sperrer for å oppfylle regelverkets krav.

Det er vår klare målsetting å bidra til at barn og unge læres opp til å bli bevisste om eget personvern. Det er i den sammenheng viktig at barnehage- og skoleeierne i større grad tar personvern på alvor både i egen organisasjon, og overfor barna og deres foresatte.

I 2013 ble det tatt inn et nytt ledd i personopplysningsloven § 11. Dette sier at personopplysninger som gjelder barn ikke skal behandles på en måte som er uforsvarlig av hensyn til barnets beste. Bestemmelsen kom som en følge av en rekke tilfeller der bilder og andre opplysninger om barn har blitt publisert på Internett, blant annet i tilknytning til barneverns- og barnefordelingssaker.

Datatilsynet har hittil ikke hatt saker hvor denne bestemmelsen har blitt prøvd ut. I året som er gått har vi imidlertid sett at barnehager og skolers økte bruk av internettbaserte løsninger, raskt kan endre dette. Forarbeidene nevner spesielt «utleverende bilder og belastende opplysninger om barnets helse» som eksempler på personopplysninger som omfattes. Lovens uttrykk «barnets beste» må selvfølgelig tolkes i lys av uttalelsene i forarbeidene, men på generelt grunnlag kan vi si at vi allerede ser at barnehager og skoler behandler denne type opplysninger i dag. I den grad de benytter seg av internettbaserte verktøy, er risikoen til stede for at opplysningene blir spredd.

Hva er gjort på området?

Forprosjekt – kartlegging

Datatilsynet har i 2013 gjennomført et forprosjekt hvor vi hadde som mål å kartlegge flyten av opplysninger om barn i barnehage, grunnskole og videregående skole. Det ble gjennomført en rekke møter med aktører innen skolesektoren. Gjennom disse møtene, saksbehandling og veiledning i skolerelaterte saker, identifiserte vi flere punkter som kunne være aktuelle å følge opp i form av tilsyn eller veiledning. Vi sitter igjen med følgende hovedpunkter:

- **Økt lagring av personopplysninger:** IKT-løsningene som skolene tar i bruk, legger til rette for lagring av flere personopplysninger enn det som har vært vanlig før, og vi er usikre på om

skolene har vurdert om all innsamlingen er nødvendig for det de vil oppnå. Eksempler på dette er at personopplysninger genereres gjennom logging av aktivitet og læringsmønster, kommunikasjonsverktøy som chat, kommentarfelt/diskusjonsforum, e-post og meldingstjeneste, samt mulighet til å ta opp lyd og bilde.

- **Deling av personopplysninger med tredjepart:** Lærere tar av og til i bruk nettbaserte verktøy til lærings- og administrative formål, uten at skoleeier har besluttet bruken. Antakelig er denne bruken ikke risikovurdert heller. Det er også en økning i antallet pedagogiske verktøy som tilbys over Internett. Bruken av slike verktøy innebærer ofte en integrering mellom skolens system og tilbyderens applikasjon, og betyr at personopplysninger overføres til tredjepart (tilbyder) uten at dette er tilstrekkelig forankret eller avklart.
- **Uoversiktlig informasjonsflyt og uklare ansvarsforhold:** Det er mange IKT-system og mange aktører involvert i behandlingen av personopplysninger i skolesektoren. Dette gjør at det er utfordrende å få oversikt over hvor opplysningene om elevene til enhver tid er, og hvem som har tilgang til dem. Ikke alle skoleeiere er like bevisste på ansvaret de har for opplysninger de samler inn og bruker. Opplysninger som i mange tilfeller tilflyter en leverandør av IT-system eller digitale verktøy.
- **Leverandøren setter standarden:** Det er stor variasjon i økonomi, kunnskap og kapasitet hos skoleeierne, og dette påvirker muligheten for å ivareta personvernet på systemnivå. Større kommuner kan ha større mulighet til å sette krav til produkter de kjøper, samt gjøre tilpasninger av system og bruk, slik at produktet oppfyller kravene til personvern og informasjonssikkerhet. Mindre aktører vil sannsynligvis i mange tilfeller kjøpe IKT-produkter som hyllevare, og bruke det etter beste evne uten nødvendigvis å ha et bevisst forhold til personvern. I praksis betyr det at leverandører av IKT-system har stor makt til å sette premissene for hvordan skolesektoren behandler personopplysninger.

Sentralt register med sensitive elevopplysninger – høringsuttalelse

Kunnskapsdepartementet foreslo i meldingsåret at sensitive opplysninger om elever på 10. trinn i grunnskolen og i videregående skole, skal lagres i et sentralt register. Opplysningene det er snakk om er blant annet elevenes fravær, karakterer, behov for spesialundervisning og andre taushetsbelagte opplysninger. Utdanningsdirektoratet vil få tilgang til disse opplysningene om hver enkelt elev.

Departementet og direktoratet mener at de trenger identifiserende informasjon for å forske på trender og utviklingstrekk, og for å administrere skolesektoren. Datatilsynet uttrykte i en høringsuttalelse i desember at vi er uenige i dette. Vi mener at det bør kunne være nok med aggregert informasjon om elevene, det vil si opplysninger som ikke kan spores tilbake til hver enkelt elev. Datatilsynet er selvsagt ikke imot forskning, men vi mener at behovet for å forske på trender og utviklingstrekk kan løses på andre måter enn å opprette enda et nytt register. Sentrale utdanningsmyndigheter kan for eksempel bruke opplysninger som Statistisk sentralbyrå allerede har, eller de kan følge de samme spillereglene som andre forskningsmiljøer må følge – de må be om samtykke fra elevene det skal forskes på.

Det foregår mye forskning på utviklingstrekk i arbeidslivet, og det skjer uten at arbeidsgivere rapporterer inn arbeidstakernes prestasjoner og skavanker til et nasjonalt register. Datatilsynet mener at det er uakseptabelt at opplysningene om barn i skolen skal brukes på helt andre vilkår. Det er viktig å huske at alle, også skoleelever, har rett til å vite hvem som har personopplysninger om

dem og hva disse opplysningene brukes til. De må også kunne velge om de vil bidra til forskningen eller ikke.

Barn og unges personvern – DuBestemmer

Datatilsynet jobber også aktivt med å styrke *barn og unges* kunnskap om eget personvern. Dette gjøres hovedsakelig gjennom undervisningsopplegget DuBestemmer, som er et samarbeid mellom Senter for IKT i utdanningen, Teknologirådet og Datatilsynet. Opplegget består av filmer og hefter med opplysende tekster og diskusjonsoppgaver, og ble lansert i forbindelse med den internasjonale personverndagen i januar 2007. Målet med opplegget er å øke elevenes kunnskap om personvern generelt, samt heve deres bevissthet om valg de gjør ved bruk av digitale medier slik som Internett og mobiltelefon. Elevene skal lære seg å ta kontroll over egne personopplysninger, og ikke minst respektere andres opplysninger. Undervisningsopplegget er laget for to aldersgrupper, 9–13 år og 13–17 år, og stikkord for opplegget er diskusjon og refleksjon. Opplegget er til nå tatt i bruk i over 16 andre land.

Nye nettsider under utvikling

Siden oppstarten av prosjektet i 2007 har det kommet til mye nytt innhold – både nye tema og filmer. Nettsidene fungerer derfor ikke optimalt lenger. Innholdet er blitt lite oversiktlig både for brukere og de som publiserer. Arbeidet med å lage nye nettsider, samt en omfattende omlegging og total revidering av innholdet for å få en bedre struktur og for å gjøre nettsidene mer brukervennlige, ble derfor startet opp i mai. Det er et mål at flere lærere etter hvert vil velge nettsidene som førstevalg i undervisningen, i stedet for å bestille heftene som tilbys.

Alt innhold skal dessuten legges over på Senter for IKT i utdanningen sin nettløsning. I forbindelse med omleggingen er det utarbeidet en ny grafisk profil med tilhørende illustrasjoner og logo. De nye nettsidene skal etter planen lanseres innen april 2014.

Fortsatt etterspørsel

Det kommer jevnlig inn bestillinger på opplegget fra hele landet, og nettstedet www.dubestemmer.no er godt besøkt. Opplegget benyttes ikke bare til undervisning i skolene, men bestilles også av politi, frivillige organisasjoner, bibliotek, helsestasjoner, foreldrerepresentanter, til konformasjonsundervisning og lignende. Til nå er det sendt ut over 633 000 hefter etter bestillinger.

Markedsføring av undervisningsopplegget på TVN og TV2 under reklamefrie dager i påske- og pinsedagene, har også resultert i økt pågang på nettsidene.

Antall bestillinger av Du Bestemmer 13-17 år:

Tidsperiode	Bestillinger	Brosjyrer
Fra mai 2007 t.o.m. 2008	1 848	220 230
2009	460	42 510
2010	291	27 030
2011	376	32 580
2012	331	30 450
2013	266	27 105
Totalt 2007-2013	**3 572**	**379 905**

Antall bestillinger av Du Bestemmer 9-13 år:

Tidsperiode	Bestillinger	Brosjyrer
2009 (fra april)	1 312	117 600
2010	363	28 260
2011	603	48 540
2012	426	27 810
2013	387	31 038
Totalt 2009-2013	**3 091**	**253 248**

Bilder av barn på nett

For å spre informasjon om de yngste barnas personvern på nett, fortsetter vi å sende ut veilederen *I beste mening.* Den handler om hvordan man skal håndtere bilder av barn på nett, og om bildene i det hele tatt bør publiseres. Veilederen finnes både på bokmål, nynorsk og engelsk, og er svært populær. Den benyttes i størst grad av ansatte i barnehager, men også foreldre, skoler, frivillige organisasjoner, sykehus og bibliotek bruker den aktivt.

I løpet av 2013 ble det, på bakgrunn av bestillinger, sendt ut 5 343 eksemplarer. Siden veilederen ble lansert i 2008, er det blitt distribuert nær 55 000 eksemplarer, noe som gir en god spredning av regelverk og etikk rundt dette temaet. Det er også jevnlig foredrags- og mediehenvendelser om dette temaet.

Funn fra tilsyn

Internkontroll og informasjonssikkerhet i barne- og ungdomsskoler

Høsten 2013 gjennomførte Datatilsynet åtte kontroller i kommuner (grunnskoler), fylkeskommuner (videregående skoler) og privatskoler med temaet internkontroll og informasjonssikkerhet. Vi så særlig på bruken av læringsplattformer, skoleadministrative systemer og andre læringsressurser. I tillegg gjennomførte vi to kontroller i grunnskoler som bruker verktøyet SWISS for å sørge for godt psykososialt miljø.

Vi kan konstatere at det er et gjennomgående problem at skolene ikke har tilfredsstillende rutiner for å oppfylle pliktene i personopplysningslovens med forskrift. Dette gjelder særlig pliktene til å ha

oversikt over hvilke behandlinger av personopplysninger skolen gjør, å sørge for at foresatte og elever blir informert om hvordan skolen håndterer opplysningene, å sørge for at innsyn blir håndtert på riktig måte, samt å sørge for å ha slette- og/eller arkivrutiner for de elevopplysningene skolene har ansvar for. Fylkeskommunen/kommunen har gjerne overordnede rutiner, men disse er enten lite kjent på skolen eller er for lite tilpasset til at de kan brukes i skolen.

I den grad skolene har skrevne rutiner om behandlingen av personopplysninger, handler de gjerne om informasjonssikkerhet. Inntrykket er imidlertid at tradisjonen med papirbasert dokumenthåndtering fortsatt er sterk, og at mange har en oppfatning av at informasjonssikkerhet hovedsakelig handler om å sørge for konfidensialitet. Tilgjengelighet og integritet (det vil si at opplysningene er oppdaterte og korrekte) er det ikke like mye fokus på. Et eksempel er at enkelte vi har snakket med har en oppfatning av at når de har lagret et dokument på en minnepenn og låst den inn i et skap – da er informasjonssikkerheten ivaretatt på en god måte. Opplysningene vil riktignok være vanskelige for en utenforstående å få tak i, men det er en tungvint ordning for de som skal ha tilgang til opplysningene for å gjøre jobben sin (tilgjengelighet) – og ved at det er tungvint er det ikke alltid sikkert at opplysningene blir oppdatert, noe som også er et krav i personopplysningsloven.

Flere av skoleeierne hadde mangler rundt etableringen av databehandleravtaler, og hadde mangelfull gjennomføring og oppfølging av risikovurderinger. I den grad risikovurderinger var foretatt var de mangelfulle både med tanke på hvem som utarbeidet dem, variasjon i scenarioer og forslag til sikkerhetstiltak.

Arbeidsliv

I 2013 var arbeidsliv et hovedsatsingsområde for Datatilsynet. Bakgrunnen var et stort antall henvendelser fra arbeidsgivere og arbeidstakere som hadde behov for råd og veiledning fra oss. Slike henvendelser utgjør et stort flertall av de spørsmålene som stilles til vår juridiske veiledningstjeneste.

Det har kommet en rekke nye elektroniske verktøy som gjør det mulig å hente inn detaljerte opplysninger om ansattes bevegelser og prestasjoner. Bruken av disse verktøyene blir etter alt å dømme stadig mer utbredt. Trolig har også konkurranseutsetting og det at flere og flere oppdrag legges ut på anbud, bidratt til den stadig mer inngående registreringen av hver enkelt ansatt sine prestasjoner. Vi har dessuten sett en tendens til at globaliseringen medfører at kontrollregimer som frem til nå har vært mer utbredt i utlandet, også innføres av norske arbeidsgivere. Ofte stiller utenlandske selskaper krav til at norske kontraktsparter kan dokumentere at slike tiltak er innført.

Maktstrukturene på en arbeidsplass innebærer at de ansatte er prisgitt de kravene som stilles fra ledelsen. I rollen som ansatt vil registreringen og kontrollpotensialet oppleves som mer inngripende enn i andre sammenhenger der det ikke eksisterer et slikt rangforhold.

Med bakgrunn i dette har Datatilsynet prioritert å gjennomføre flere kontroller rettet mot ulike arbeidsgivere, styrke dialogen med partene i arbeidslivet og inngå et tettere samarbeid med Arbeidstilsynet.

Les mer om hva folk kontakter oss om på dette feltet i kapittel 4, under *Juridisk saksbehandling*.

Hva er gjort på området?

Innsyn i e-post

Datatilsynet mottar et relativt høyt antall klager som gjelder innsyn i ansattes e-postkonto. Jevnlig blir vi tipset om arbeidsgivere som enten har gjennomført et uberettiget innsyn i en ansatts e-postkorrespondanse, eller som ikke har avsluttet en e-postkonto etter at arbeidsforholdet opphørte.

Det er påfallende mange arbeidsgivere som tilsynelatende uten motforestillinger går gjennom e-postkorrespondansen til ansatte eller som sørger for å få tilgang til all e-post som sendes til adressen til en tidligere arbeidstaker. Datatilsynet vurderer denne formen for lovbrudd som alvorlig.

Folks korrespondanse skal ha et særlig vern, og er derfor også særskilt beskyttet gjennom lovverket. At innsyn i en rekke tilfeller skjer uten at den ansatte blir orientert i forkant, gjør at overtrampet oppleves som enda mer krenkende. I de tilfellene der e-postkontoer opprettholdes etter at ansettesesforholdet har opphørt, og innholdet blir gjennomgått, opplever den tidligere ansatte maktesløshet. Ubehaget forsterkes ved at man selv er fratatt kontroll over innholdet på kontoen.

Henvendelser om dette følger vi vanligvis opp gjennom en skriftlig kontroll der vi ber virksomheten om en redegjørelse. På bakgrunn av det som kommer frem, tar vi stilling til hva som vil være en riktig reaksjon fra vår side. I de grove tilfellene vurderer vi alltid overtredelsesgebyr.

Teletopia – overtredelsesgebyr

Høsten 2011 gjennomførte Datatilsynet en uvarslet tipskontroll mot Teletopia Gruppen AS. Teletopia Gruppen er et holdingselskap som inngår i et konsern med selskaper som blant annet driver med telekommunikasjon, reiseliv, forlagsvirksomhet og taxidrift.

Kontrollen avdekket omfattende brudd på personopplysningsloven. Virksomheten overvåket blant annet kontorkorridorer i strid med et tidligere vedtak fra Datatilsynet. Det ble også foretatt skjulte lydopptak av eksterne og interne møter, samt telefonsamtaler.

Datatilsynet fant bruddene så alvorlige at virksomheten i meldingsåret ble ilagt et overtredelsesgebyr på 200 000 kroner. Virksomheten har klaget på vedtaket, og saken ligger nå til behandling hos Personvernnemnda.

Retura Sør-trøndelag – overtredelsesgebyr

Saken mot Retura Sør-Trøndelag omhandler samme tema som en kontrollsak fra 2012 mot firmaet Avfallsservice. Sakenes hovedtema var om en arbeidsgiver kunne benytte opplysninger fra en elektronisk kjørebok til å kontrollere den enkelte ansatte. Konkret dreide det seg om opplysninger som sier noe om hvor de ansatte hadde vært, og som så ble sammenholdt med timelister og krav om overtidsbetaling. Formålet med den elektroniske kjøreboken var ikke kontroll av de ansatte, men logistikkstyring av biler og avfallshåndtering. Personopplysingslovens regel om at opplysninger ikke skal benyttes til andre formål enn det opprinnelige – her logistikk – var etter vår oppfatning brutt, og Datatilsynet ila Retura Sør-Trøndelag AS et overtredelsesgebyr på 100 000 kroner.

Kommunikasjon med bransjen – GPS

Bruken av ulike GPS-systemer har vært økende de siste årene. Vi har sett at det er behov for informasjon og klargjøring av gjeldende regelverk. Dette har særlig vært tilfelle for aktørene i arbeidslivet. Datatilsynet har derfor holdt en rekke foredrag for arbeidsgivere og tillitsvalgte, samt hatt flere møter med utviklere og leverandører av GPS-systemer. Denne kommunikasjonen med bransjen bidrar til en større bevissthet rundt regelverket, og er dermed med på å minke sannsynligheten for regelverksbrudd. Målet med å ha dialog med leverandørene er at de skal kunne veilede sine kunder på en god måte, for slik å sikre etterlevelse av regelverket rundt bruken av GPS.

Kommunikasjon med bransjen – kamera

For regeletterlevelse og en bevisst holdning til bruk av kameraovervåking i samfunnet, er det viktig å ha kontakt med installatørbransjen og større virksomheter som benytter kameraovervåking. Datatilsynet har derfor prioritert kontakt med bransjeforeninger og deltagelse på sikkerhetsfora. Dette er gode arenaer for å formidle innholdet i regelverket, gjennom blant annet foredrag. Samtidig er det viktig for å følge med på problemstillinger, trender og utvikling innen dette området.

Datatilsynet har god kontakt med bransjeforeningen NELFO, og i løpet av året har tilsynet deltatt på flere konferanser knyttet til denne bransjen.

Kontaktmøter

Datatilsynet har gjennomført kontaktmøter med blant annet LO og NHO om hvilke utfordringer partene i arbeidslivet står overfor på dette området, og da særlig bruk av kontrolltiltak og behovet for klarere rettslig regulering. Slike møter er nyttige for oss.

Vi gikk også gjennom Hovedavtalen[21] og ble positivt overrasket over hvor mye plass som var viet personvernspørsmål og behandling av personopplysninger der. Dialogen med partene i arbeidslivet mener vi er et godt bidrag til at reglene i hovedavtalen kommer tydelig frem sammen med de generelle personvernprinsippene.

Vi har også hatt et kontaktmøte med Arbeidstilsynet og gjennomført tilsyn sammen med dem.

Foredragsvirksomhet

Datatilsynet har holdt flere foredrag om personvern i arbeidslivet, blant annet for tillitsvalgte og HMS-ansvarlige. Å spre informasjon om ansattes rettigheter til denne gruppen ser vi på som en hensiktsmessig måte å skape økt bevissthet om personvern i arbeidslivet. Vi får gode tilbakemeldinger fra organisasjonene, og gjør derfor det vi kan for å imøtekomme forespørsler om slike foredrag.

Vi har også holdt foredrag for brukere og leverandører av verktøy for flåtestyring og elektroniske kjørebøker. Dette anses også å være en meget formålstjenlig måte å veilede bransjen om relevant regelverk og om vår lovforståelse på området.

Funn fra tilsyn

Rusmiddeltesting

Vi hadde behov for å skaffe oss bedre kunnskap om bruken av rusmiddeltesting i arbeidslivet og om de rettslige skrankene for slik bruk. Datatilsynet gjennomførte derfor to kontroller som hadde rusmiddeltesting av ansatte som tema. Selve bruken av rusmiddeltesting er regulert i arbeidsmiljøloven, mens den videre behandlingen av personopplysningene som testingen genererer, er regulert av personopplysningsloven.

Hos tilsynsobjektene erfarte vi at den kretsen av personer som ble utsatt for testing, ikke var mer omfattende enn det behovet for sikkerhet skulle tilsi. Vi fant heller ingen åpenbare brudd på grunnleggende personvernhensyn. I en av kontrollsakene fikk arbeidsgiveren pålegg om å utbedre internkontrollsystemet i virksomheten, samt innføre rutiner som sikrer at de ansatte gis god nok informasjon.

På bakgrunn av kontrollene og henvendelser fra publikum er det imidlertid grunn til å anta at behandlingen av testresultatene ikke er tilfredsstillende beskrevet i virksomhetenes internkontrollsystem og at rutinene for testing ikke er godt nok kommunisert til de ansatte.

Kameraovervåking

Datatilsynet mottar jevnlig henvendelser om kameraovervåking i arbeidslivet. Det er både arbeidstagere og arbeidsgivere som henvender seg, og i de fleste tilfellene bistår vi med råd, veiledning og uttalelser. I løpet av 2013 ble det i tillegg gjennomført tre tipskontroller med kameraovervåking i arbeidslivet. To av dem ble gjennomført uten varsel. I alle sakene gjaldt det kameraovervåking inne i lokalene der de ansatte har sine arbeidsoppgaver og tilbringer hele eller deler av arbeidsdagen.

[21] Hovedavtalen LO/NHO 2010–2013

Kontrollene avdekket flere avvik fra kravene i loven, blant annet brudd på plikten til å melde fra om kameraovervåkingen til Datatilsynet, bruk av overvåkingsutstyr som ikke ga tilfredsstillende informasjonssikkerhet, mangelfull informasjon til de ansatte om overvåkingen og mangelfull sletting av opptak. I en av sakene, kontrollen med virksomheten Gull Adam, kom Datatilsynet dessuten til at overvåkingen ikke hadde tilstrekkelig rettslig grunnlag og dermed måtte opphøre eller begrenses.

Gull Adam – Personvernnemnda

Datatilsynet fattet vedtak om at kameraovervåkingen av den delen av forretningens lokaler som kun var tilgjengelig for ansatte, måtte opphøre. Spørsmålet var om overvåkingen var i samsvar med personopplysningsloven som krever «særskilt behov» for at overvåking skal være tillatt. Butikken er delt i tre soner; et kundeareal og et midtareal som begge er overvåket, samt et pauseareal hvor det ikke er kameraer. Formålet med overvåkingen var å hindre eller oppklare innbrudd og ran, samt å overvåke verdiene i lokalet.

Etter klage fra virksomheten, ble saken oversendt til Personvernnemnda for behandling. Nemnda kom til at overvåkingen var i samsvar med loven, og la vekt på at det dreier det seg om små gjenstander av stor verdi. Nemnda la også vekt på at pauserommet ikke ble overvåket og at de ansatte ble informert om kameraovervåkingen før ansettelsen. Datatilsynets vedtak ble derfor omgjort.

Innebygd personvern

Innebygd personvern, eller *Privacy by Design*, betyr at det tas hensyn til personvern i alle utviklingsfaser av et system. Personvern skal altså være del av designet til et system. Ved å ta med personvern fra starten av, er målet at virksomheten oppnår god kjernefunksjonalitet, samtidig som personvernet blir ivaretatt på en god måte. Begrepet ble utviklet av lederen for det canadiske datatilsynet i Ontario, Dr. Ann Cavoukian, og i 2010 ble *«Syv steg til innebygd personvern»* vedtatt som universelle prinsipp på den internasjonale personvernkonferansen.

I stortingsmeldingen «*Personvern – utsikter og utfordringar»*, ble innebygd personvern foreslått som et prinsipielt mål i alle sektorer. Meldingen sier videre at «*Dei førehandsdefinerte standardinnstillingane på utstyr, i system og i program bør setjast til den mest personvernvenlege løysinga.»* Datatilsynet har i 2013 hatt innebygd personvern som et prioritert område, og har jobbet aktivt for å gjøre veiledningsmateriell tilgjengelig og spre kunnskap om hvordan innebygd personvern kan brukes i praksis.

Hva er gjort på området?

Syv steg – sjekkliste og konsekvensvurderinger for personvernet

Datatilsynet har oversatt og tilrettelagt de syv stegene til innebygd personvern til norsk. Stegene er en liste med metodiske grep som er essensielle for å ivareta personvernet i en utviklingsprosess:

1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet; både-og, ikke enten-eller
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

En utfyllende forklaring og eksempler finnes på våre hjemmesider. Der finnes også en sjekkliste for bestillere og utviklere, med tips om hvilke personvernhensyn som bør tas i utviklingen av et system.

Å gjøre en vurdering av konsekvenser for personvernet i forkant av utviklingsprosessen, er en sentral del av arbeidet med innebygd personvern. En vurdering av personvernkonsekvenser, eller *Privacy Impact Assessment* (PIA), er å analysere hvordan personopplysninger kan håndteres ved å:

- sikre at behandlingen av personopplysninger er i samsvar med personvernregelverket
- vurdere risikoene ved å behandle personopplysninger
- vurdere om det finnes alternative metoder som ikke medfører behandling av personopplysninger eller som medfører redusert bruk av personopplysninger
- undersøke og evaluere om personopplysningene beskyttes på best mulig måte i systemet, eller om dette kan forbedres.

Datatilsynet har laget en norsk PIA-veileder basert på veiledere brukt i andre land.

Frokostseminar og foredrag

I mai 2013 arrangerte Datatilsynet er frokostseminar om innebygd personvern med innledere fra IBM, Ruter og Oslo Universitetssykehus. Målet med arrangementet var å spre kunnskap om begrepet, og vise hvordan dette kan settes ut i praksis, ved å invitere aktører som har erfaring med innebygd personvern. Arrangementet var fulltegnet, noe som ga en indikasjon på at dette er et tema det er stor interesse for.

I tillegg til å ha møter med ulike aktører, har Datatilsynet holdt foredrag om innebygd personvern for blant annet app-utviklere, og ansatte ved Universitet i Oslo og i helsesektoren. Innebygd personvern er et tema i de fleste av Datatilsynets foredrag i ulike kontekster, men vi har merket økt interesse for foredrag om temaet i seg selv.

Påvirkning

Prinsippene om innebygd personvern er aktivt kommunisert til ulike sektorer gjennom året, og begrepet begynner å få godt fotfeste. Utover aktivitetene ovenfor, har innbygd personvern vært tema på møter med ulike sektoraktører, og noe Datatilsynet har løftet frem i høringsuttalelser.

Spesielt har det vært en aktiv dialog med helsesektoren på grunn av de mange prosessene som innebærer ny og endret bruk av teknologi, slik som kjernejournal og velferdsteknologi.

Eksempler på bruk av innebygd data

MinJournal – personvern som del av grunnmuren

Oslo universitetssykehus (OUS) har, i samarbeid med flere store helseforetak, utviklet MinJournal. MinJournal er en nettbasert løsning for selvbetjening og kommunikasjon mellom helsevesen og pasient. Pasientene kan blant annet lese e-post fra lege, bestille time og hjelpemidler, samt se sin egen epikrise.

Da prosjektet startet i 2005 var OUS en av de første aktørene i Norge som utviklet en elektronisk løsning for pasienter. Sensitive helseopplysninger var en viktig del av MinJournal, og sykehuset var bevisst på at hvis man laget et system som ikke ivaretok personvernet på en god måte fra starten av, kunne det ødelegge folks tillitt til helsevesenet og de elektroniske systemene i sektoren. OUS ønsket også at systemet de utviklet skulle være solid nok, slik at det var mulig å utvide med nye tjenester etter hvert. Prosjektet hadde derfor allerede i starten en grundig gjennomgang av mulige personvernkonsekvenser, noe som resulterte i en solid grunnmur der personvernet ivaretas på en god måte.

RuterBillett – personvern som del av designet

Ruter har utviklet en applikasjon for billettkjøp, der selve designet legger til rette for at folk kan reise mest mulig anonymt – også hvis de kjøper billett på mobil. RuterBillett har en personvernerklæring før nedlastning der det står eksplisitt at det ikke samles inn IMEI-nummer, SIM-kortnummer, telefonnummer, UDID-er eller andre identifikatorer som kan brukes til å identifisere brukeren. Det eneste man må levere fra seg av opplysninger er kortinformasjon for kjøp av billett, og det blir kun kommunisert til PayEx. Appen er designet slik at de reisende selv kan velge om de vil slå på lokasjonssporing. Det samme gjelder om de vil sende anonyme brukerdata til Ruter.

Silent Circle – personvern som del av forretningsideen

Det amerikanske selskapet Silent Circle har utviklet en teknologi som bruker en enhet-til-enhet (peer-to-peer) krypteringsteknikk. Til mobiltelefon har de utviklet Silent Phone og Silent Text. Sistnevnte lar brukerne sende krypterte filer på opptil 60 MB gjennom en app. Senderen av filen kan sette på en tidtaker slik at filen automatisk slettes fra begge enhetene etter en bestemt tid.

Silent Circles-servere lagrer minimalt av informasjon om deres brukere. Det er kun e-postadresse som lagres, i tillegg til kortnummer til en tredjepart som styrer betalingsløsninger. Silent Circle informerer i sin personvernerklæring om at de ikke holder på metadata (slik som tidspunkt og dato for samtaler gjennom Silent Circle), og at innhold på serverne, slik som IP-adresser om hvem som har besøkt nettstedet, slettes etter syv dager. Anonymiserte utdrag kan lagres lenger. Når data ikke lenger trengs, slettes det. Hver sjette måned informerer selskapet om hvor mange henvendelser de har fått fra myndigheter verden over, hvor mange kunder dette involverer, og hvilke byråer eller organisasjoner som kom med henvendelsen.

Det brukes også innebygd personvern for å beskytte sikkerheten rundt brukernes krypterte filer. Når en bruker sender et bilde eller dokument, blir det kryptert; digitalt delt opp i tusenvis av biter, og midlertidig lagret i en sikker skytjeneste til den er sendt til mottakeren.

Big Data

Big Data viser til en trend der enorme mengder digitale data gjennomgår omfattende analyser. Dette er en av de store teknologi- og forretningstrendene som vil prege samfunnet fremover. Datatilsynet har derfor valgt å rette spesiell oppmerksomhet mot dette fenomenet i 2013.

Big Data kan brukes til mange gode og samfunnsnyttige formål. Analyseteknikkene benyttes i stor grad til å analysere anonymiserte data for å identifisere og forutsi trender og sammenhenger. Big Data kan for eksempel brukes til å forutsi spredning av epidemier, til å oppdage alvorlige bieffekter av medisiner og til å bekjempe forurensing i storbyer. Slik bruk av anonymiserte data utfordrer i utgangspunktet ikke personvernet. Det finnes også Big Data-analyse som ikke involverer bruk av personopplysninger i det hele tatt, slik som analyse av værdata eller sensordata fra utstyr på en oljeplattform.

Men, Big Data kan også brukes slik at enkeltindivider berøres direkte. *A*nalyseteknikken benyttes til å lage profiler og predikere atferd til enkeltindivider og grupper av individer, ved å sammenstille og analysere personopplysninger samlet inn fra mange ulike kilder. Selv om opplysningene aggregeres og avidentifiseres, kan resultatet av analysen likevel få konsekvenser for enkeltpersoner.

Bruken av Big Data er foreløpig i startgropen. Hvordan vi håndterer utviklingen mot en stadig mer omfattende utnyttelse av de enorme datastrømmene som genereres, er avgjørende for personvernet. Sterke krefter – både kommersielle aktører og offentlige myndigheter – omfavner Big Data. Utnyttelsen av datastrømmene, også omtalt som den nye oljen, vil være viktig for å fremme konkurransekraft og innovasjon i samfunnet. Men dette må gjøres på en måte som ikke truer personvernet.

Gjennom bruk av Big Data utfordres sentrale personvernprinsipper. Enkelte hevder derfor at dagens personvernlovgivning må tilpasses en ny virkelighet. Datatilsynet deler ikke denne oppfatningen. I en tid der stadig flere opplysninger om hver enkelt samles inn, er det viktigere enn noen gang å verne om grunnleggende personvernprinsipper. Prinsippene er vår garanti mot å bli gjort til gjenstand for profilering i stadig nye og flere sammenhenger.

Hva er gjort på området?

Publisering av rapporten «Big Data – personvernprinsipper under press»

Datatilsynet skrev i meldingsåret en omfattende rapport som kartlegger utfordringer for personvernet ved bruk av Big Data. Rapporten gir også råd for hvordan Big Data kan tas i bruk på en måte som respekterer personvernet til den enkelte. I rapporten trekker vi blant annet frem følgende utfordringer:

- **Bruk av data til nye formål:** Big Data handler i stor grad om gjenbruk av data. Dette utfordrer personvernprinsippet om formålsbegrensning. I henhold til dette prinsippet må virksomheter som benytter innsamlede personopplysninger, som grunnlag for prediktiv analyse, forsikre seg om at prediksjonsanalysen ikke er uforenlig med det opprinnelige innsamlingsformålet. Dette kan innebære en betydelig utfordring for kommersiell Big Data-analyse.

- **Datamaksimalisering:** Big data innebærer et nytt syn på data, der data får en verdi i seg selv. Verdien ligger i dataenes *fremtidige* bruksmuligheter. Et slikt syn på data påvirker virksomhetenes ønske om og motivasjon til å slette data. Verken private eller offentlige virksomheter vil ønske å slette data som på et senere tidspunkt, og sammenstilt med andre datasett, kan vise seg å bringe både penger og ny innsikt.
- **Mangel på åpenhet:** Mangel på åpenhet og informasjon om hvordan data benyttes og sammenstilles, kan føre til at vi som enkeltpersoner blir offer for beslutninger vi ikke forstår og ikke har kontroll over. Den alminnelige internettbruker har for eksempel liten innsikt i hvordan personopplysninger samles inn og utnyttes av kommersielle interesser. Flere av aktørene som opererer i dette markedet er i tillegg ukjente for folk flest.
- **Sammenstilling kan frembringe sensitiv informasjon:** En utfordring ved Big Data-analyse er at innsamlede opplysninger som hver for seg ikke er sensitive, kan gi et sensitivt resultat når de blir sammenstilt. Det er viktig at virksomheter som benytter Big Data er kjent med denne problemstillingen, og ikke utvikler algoritmer som kan komme til å avsløre svært privat informasjon.
- **Farvel anonymitet?:** En av de virkelig store utfordringene ved Big Data-analyse er risikoen for reidentifisering. Gjennom sammenstilling av data fra flere kilder kan det oppstå risiko for at enkeltindivider kan identifiseres fra i utgangspunktet anonyme datasett. Dette gjør anonymisering som metode for å hindre personvernulemper ved profilering og annen dataanalyse, mindre virkningsfull.
- **Datadeterminisme:** Utstrakt bruk av automatiserte avgjørelser og prediksjonsanalyse kan befeste eksisterende fordommer og forsterke sosial ekskludering og lagdeling. En utvikling der stadig flere beslutninger i samfunnet blir tatt basert på algoritmer, kan lede til et "dataenes diktatur"; vi blir ikke vurdert på basis av hva vi faktisk foretar oss, men på basis av hva alle dataene om oss sier at vi sannsynligvis kan komme til å gjøre. En svakhet ved Big Data-analyse er dessuten at den ofte ikke tar hensyn til kontekst. Å basere beslutninger på opplysninger som er tiltenkt andre formål og som har oppstått innenfor en annen kontekst, kan gi resultater som ikke samsvarer med den faktiske situasjonen.
- **Nedkjølingseffekt:** Bruk av Big Data har potensiale i seg til å legge til rette for et massivt overvåkingssamfunn. Hvis alle sporene vi etterlater oss, på Internett og andre steder, blir brukt til stadig nye og for oss ukjente formål, kan dette legge bånd på ytringsfriheten og hvordan vi deltar i samfunnet. Les mer om nedkjølingseffekten i kapittel 2, under *Året med Snowden*.

Selv om Big Data reiser flere utfordringer for personvernet, er det mulig å benytte denne analyseformen og samtidig respektere personvernet til den enkelte. Bruk av Big Data bør som hovedregel baseres på *samtykke*. Hvis det ikke er mulig eller ønskelig å benytte samtykke, bør opplysningene *anonymiseres*. Ettersom anonymisering som metode er blitt mer sårbar, er gode rutiner for anonymisering og avidentifisering av opplysningene av stor betydning. Dette vil bidra til å redusere faren for reidentifisering.

Det er videre viktig at virksomheter som benytter Big Data er åpne om hvordan de behandler personopplysningene de samler inn. Dette innebærer blant annet å gi den enkelte innsyn i hvilke

beslutningskriterier (algoritmer) som ligger til grunn for utvikling av profiler, og fra hvilke *kilder* opplysningene er hentet.

Working paper i Berlin-gruppen

Etter initiativ fra Datatilsynet, besluttet Berlin-gruppen, en internasjonal arbeidsgruppe som arbeider med problemstillinger knyttet til personvern innen telekommunikasjon, i mai 2013 å lage et såkalt *working paper* på Big Data. Datatilsynet fikk ansvar for utarbeide dokumentet, og et utkast ble lagt frem for medlemmene i Berlin-gruppen i september 2013. Dokumentet ble svært godt mottatt, og ventes å bli endelig godkjent på gruppens neste samling i mai 2014.

Foredrag

Det er stor etterspørsel etter kunnskap om hvordan Big Data kan benyttes innenfor gjeldende lovverk. Det er også interesse for hvilke overordnede personvernmessige og etiske utfordringer bruk av slik analyseteknologi kan medføre. Datatilsynet har derfor vært invitert til å holde en lang rekke foredrag om dette temaet etter at rapporten ble publisert. Etterspørselen etter foredrag er ventet å holde seg høy også i 2014.

Internasjonalt samarbeid

Internasjonalt arbeid er viktig for Datatilsynet. Ettersom Norge står utenfor EU, er det krevende å få innflytelse på EUs beslutningsprosesser. Vi deltar imidlertid i flere sentrale EU-organ, både som observatør og aktiv deltager. Gjennom det nordiske samarbeidet kan vi også indirekte få innflytelse inn i EU-systemet. Det har i 2013 vært særlig viktig å få bedre innsikt i utviklingen på personvernområdet i USA. Snowden-saken har vist at dette også bør være høyt prioritert fremover.

Studietur – USA

Store amerikanske selskaper som Google, Microsoft og Facebook, behandler personopplysninger for nær sagt samtlige norske borgere. Amerikansk personvernrett, ofte nedfelt i standardkontrakter, har derfor stor betydning for behandlingen av norske borgeres opplysninger. Snowden-avsløringene har vist at amerikanske sikkerhetsmyndigheter går meget langt i å overvåke europeiske borgere, helt opp på regjeringsnivå.

I februar 2013, gjennomførte fire medarbeidere fra Datatilsynet en studietur til USA for å besøke private bedrifter, organisasjoner, politiske myndigheter og offentlige etater med personvern som arbeidsfelt. Hensikten var å skaffe kunnskap om utviklingen, sammenligne lovverket i Norge og USA, knytte kontakter og bringe kunnskapen tilbake til Norge og Datatilsynet.

I Washington traff vi blant annet representanter fra vår søsterorganisasjon i *Federal Trade Commission*, fra personvernorganisasjonen EPIC og personvernkontoret til *Departement of Homeland Security* (DHS), samt en rådgiver for en sentral senator. Samtlige besøk ga svært god innsikt i hvordan disse institusjonene jobbet, og særlig besøket i DHS viste seg å være nyttig når Snowden-saken begynte å rulle i juni.

I San Francisco-regionen besøkte vi Facebook, Google og Microsoft, og fikk grundig innføring i hvordan de jobber med personvern, sikkerhetsspørsmål og skytjenester, og i hvordan de driver dataanalyse på brukernes data. Besøket hos merkeordningen TrustE, ga nyttig innsikt i hvordan en privat, kommersiell aktør kan spille en rolle som kan sammenlignes med hva et personvernombud gjør i en norsk virksomhet. Vi fikk dessuten en innføring i personvernforskning på Stanford.

Vi observerte klare forskjeller mellom norsk og amerikansk tilnærming til personvernspørsmål. I USA oppfattes personvern i større grad som et forbrukerspørsmål, og regelverket er mer fragmentert enn i Norge. Det finnes for eksempel ikke et sentralt lovverk om behandling av personopplysninger. Det ble lagt stor vekt på at selskaper hadde personvernerklæringer, og at de faktisk fulgte det som sto i dem. Grunnlovsvernet av personvernet var godt, og ikke minst var det interessant å se hvordan private personvernorganisasjoner anla rettssaker mot myndighetene. Det skjer sjelden eller aldri i Norge.

Det var viktig for oss å dele mest mulig av den kunnskapen vi fikk. Samtlige besøk ble derfor referert på www.personvernbloggen.no. Det ble holdt en presentasjon for de ansatte i tilsynet ved retur, og relevant materiale ble sendt til de som jobber med ulike sektorer. Studieturen ble oppfattet som meget lærerik og interessant; vi knyttet kontakter og fikk kunnskap som Datatilsynet har hatt stor nytte av.

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 2013 har det vært avholdt fem møter i gruppen.

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. Det er blant annet kommet uttalelser om personvernkonsekvenser knyttet til automatiske strømmålere (*Smart grids*), om samtykkeregimet for bruk av informasjonskapsler i nettlesere (*cookies*) og om grensekontroller (*Smart borders*). En viktig uttalelse gjelder personvernprinsippet formålsavgrensning. Uttalelsen vil være viktig også for Datatilsynets praktisering av den norske bestemmelsen om at opplysninger i utgangspunktet ikke skal brukes til andre formål enn det opprinnelige.

I tillegg til deltakelse i artikkel-29 gruppen, er vi 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 vi våre oppfatninger, men får også god innsikt i øvrige lands vurderinger i teknologispørsmål. I meldingsåret har undergruppen blant annet sett på anonymiseringsteknikker og avviksrapportering (*data breach notification*). Disse temaene blir viktige i tiden som kommer. I tillegg har oppfølgningen av to store aktørers avtaler vært viet stor oppmerksomhet – endringene som Google og Microsoft har foretatt i sine vilkår for brukerne.

Den internasjonale personvernkonferansen

I 2013 ble den internasjonale personvernkonferansen avholdt i Warszawa. Datatilsynet deltok med tre representanter. Konferansen var todelt; en åpen del hvor akademia og næringsparter deltok sammen med personvernmyndighetene, og en lukket del for personvernmyndighetene. Hovedtema for den lukkede delen var personvernutfordringer med apper (*Appification of society*), myndigheters overvåking i lys av Snowden-avsløringene og internasjonalt samarbeid.

De deltakende myndighetene vedtok en deklarasjon om såkalt *Appification*. Målet med denne er å bidra til at apper ivaretar personvernet til brukerne på en bedre måte. Deklarasjonen fremhever informasjon til brukerne, bruk av innebygd personvern når apper utvikles, samt aktivt bidrag fra aktørene bak operativsystemene (for eksempel Google med Android og Apple med iOS) som sentrale momenter for å lykkes med dette.

Myndighetene vedtok også dokumenter om profilering, åpenhet om behandling av personopplysninger, digital kunnskap og sporing på nettet.

Global Privacy Enforcement Network – GPEN

Global Privacy Enforcement (GPEN) er et samarbeidsforum for personvernmyndigheter. Datatilsynet deltok på et møte i forumet i sammenheng med den internasjonale personvernkonferansen, samt i telefonkonferanser gjennom året. GPEN legger til rette for informasjonsutveksling og det planlegges koordinerte aktiviteter som myndighetene kan velge å delta i.

Internet Sweep Day

Datatilsynets bidrag til GPEN har i 2013 stort sett vært knyttet til *«Internet Sweep Day»*. Som en del av den internasjonale innsatsen, sveipet Datatilsynet 222 nasjonale og internasjonale nettsider. Dette ble gjort for å få et inntrykk av i hvilken grad populære nettsider og store norske virksomheter opplyser om hvordan de behandler personopplysninger.

Norge var én av 19 aktører fra 13 land som deltok for å kartlegge bruken av personvernerklæringer (*privacy policies*). Dette er første gang medlemslandene utfører et samarbeidsprosjekt i denne skalaen. Resultatene fra det norske sveipet ble oppsummert i en rapport og viste at nettsidene som ble sveipet av det norske Datatilsynet, kom noe dårligere ut enn det internasjonale snittet ellers.

Berlin-gruppen

Dette er en gruppe som arbeider med personvern innen elektronisk kommunikasjon i utvidet forstand. Gruppa avgir uttalelser (*opinions*) om aktuelle personvernspørsmål. Deltagerne kommer fra personvernmyndigheter, akademia og næringsliv; hovedsakelig fra Europa, USA, Canada og Asia. De siste årene har Berlin-gruppen avgitt uttalelser om blant annet skytjenester, automatisk måleravlesning og retten til fri elektronisk kommunikasjon.

Det er strategisk viktig for Datatilsynet å delta aktivt i Berlin-gruppen. Den har en betydelig dagsordensfunksjon, og det er ofte denne gruppen som tar tak i nye trender og utviklingstrekk først. I 2013 påtok Datatilsynet seg ansvar for å skrive gruppens rapport om Big data. Det var først gang Datatilsynet skrev en rapport for denne gruppen.

Frihandelsavtale mellom EFTA og India

Datatilsynet har bistått Nærings- og handelsdepartementet (nå Fiskeri- og handelsdepartementet) under forhandlingene om en frihandelsavtale mellom EFTA og India. Dette gikk inn i en intensivert fase i siste kvartal av 2013. Et av spørsmålene som har skapt ekstra utfordringer i denne forhandlingsprosessen, gjelder vern av personopplysninger som overføres fra EFTA og Norge til India, særlig i forbindelse med utsetting av IKT-tjenester.

Datatilsynet har bidratt med kompetanse om gjeldende rett rundt overføring av personopplysninger til land utenfor EØS-området. Vi har også deltatt i interne møter i regi av departementet, og i telefon- og videokonferanser med representanter fra EFTA og India. Dessuten har vi levert en rekke skriftlige bidrag i forbindelse med forberedende utredninger av gjeldende rett, veiledningsmateriale myntet på indiske små og mellomstore bedrifter, samt kommentarer og forslag til en rekke traktatsutkast. Forhandlingene fortsetter i 2014.

Tilsyn ved den norske ambassaden i Ukraina

Datatilsynet gjennomførte høsten 2013 en kontroll ved den norske ambassaden i Ukraina. Kontrollen fant sted i utenriksstasjonens lokaler og i lokalene til VFS Global, som utfører visse visum-relaterte tjenester på vegne av ambassaden.

Målet med kontrollen var å få greie på om de relevante reglene om personvern overholdes når ambassaden behandler personopplysninger i forbindelse med visumsøknader. Datatilsynet vurderte også om ambassadens oppslag i Schengen informasjonssystem (SIS) og den videre behandlingen av SIS-opplysninger, var i samsvar med de kravene som lovverket stiller.

Kontrollen avdekket få mangler ved ambassadens behandling av personopplysninger i forbindelse med behandlingen av visumsaker. Datatilsynet har likevel varslet to pålegg om at eksisterende skriftlige rutiner og avtaler må oppdateres.

Samarbeid/bistand med republikken Makedonia

Det norske utenriksdepartementet har gitt direkte finansiell støtte til Republikken Makedonia (FYROM) til utvikling av landets personvernmyndighet, *Directorate for Personal Data Protection* (DPDP). Denne ble etablert i 2005, og består av 24 medarbeidere.

Fra det norske Datatilsynet sin side har vi forpliktet oss til å gi faglig støtte til DPDP særlig innen to temaer; personvern i sosiale nettsamfunn og cloud computing, herunder bruk av databehandleravtaler.

Datatilsynet deltar med to representanter i prosjektets styringsgruppe. I tillegg til å gi faglige innspill, rådgivning og opplæring, skal vi delta ved et lanseringsarrangement overfor internettleverandører/sosiale nettsamfunn og på en nasjonal workshop om cloud computing.

Opplæringen og den faglige støtten, vil i hovedsak foregå i løpet av første halvår 2014. Dette skjer ved at en delegasjon på tre personer fra Norge, reiser to ganger til Skopje for å bistå i opplæring hos DPDP. I tillegg tilrettelegger vi for et studiebesøk fra Makedonia til Norge i juni 2014. Norsk senter for informasjonssikring (NorSIS) bistår også i opplæringsaktivitetene, etter forespørsel fra oss.

4. Om Datatilsynet – organisasjon og ressursbruk

Tilsynsverksemda

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

I 2013 gjennomførde vi i hovudsak tilsyn innanfor våre prioriterte område. Det vart totalt gjennomført 76 tilsyn, noko som er ei auke frå 55 tilsyn i 2012.

Det som vert rekna som tilsyn, er ein kontroll med om regelverket vert følgd, og der det normalt vert utarbeidd ein rapport i etterkant. Tilsyn vert vanlegvis gjennomført ved at to eller tre medarbeidarar frå Datatilsynet besøker verksemda. Når det er formålstenleg vert nokre tilsyn gjennomført skriftleg. I meldingsåret vart 47 av tilsyna gjennomført hos verksemdene, mens 22 vart gjennomført via brev.

Det er òg starta opp 14 tilsyn som vil bli gjennomført i 2014 – disse er ikkje teke med i oversikta her.

Tilsyn gjennomført i 2013, fordelt på områder:

Bransje	Tal på tilsyn
Helse	28
Arbeidsliv	15
Offentleg forvalting	15
Skule og utdanning	10
Justis	5
Andre	3
Totalt	**76**

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 tilsyna er omtala under respektive område i kapittel 3.

Trendar

Å bruke funn frå tilsyna for å skildre trendar, føreset lik tematikk over fleire år. Dette er krevjande sidan det er ei avgrensa mengd tilsyn med varierande sektorval og tematikk. 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. Ein positiv trend er at tidlegare tilsyn med departement og påfølgjande dialog med Service- og tryggingsorganisasjonen til departementa (DSS) har medført meir avklara ansvar og bruk av databehandlaravtalar i sentraladministrasjonen.

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 avdekte. Frå 2013 kan vi trekkje fram følgjande:

Tilsyn med korleis private verksemder, slik som forsikringsselskap og vaktselskap, gjennomfører kontroll av enkeltpersonar, har synleggjort eit behov for å avklare rammene for slik kontroll. Ei sak om dei ytre rammene for slik kontroll gjeld Gjensidige forsikring, og er no i Personvernnemnda. Saka er omtala i kapittel 3, under *Justissektoren*.

Det vart gjennomført fleire kontrollar med skular. Dette arbeidet vert vidareført i 2014, og eit av måla er å avklare om bruken av læringsplattformar er akseptabel.

Innan helse vil særleg funn frå kontrollar om informasjonsplikt ved utlevering til sentrale helseregister, sette nye rammer for korleis informasjon blir gitt. Vi har òg sett at dei mindre helseverksemdene ikkje har tilpassa seg det nye regleverket om formaliserte arbeidsfellesskap.

Tilsyn med ei fylkesnemnd for barneverns- og sosialsaker viste mellom anna avvik knytt til usikker kommunikasjon, noko som skal følgjast opp med sentraleininga for fylkesnemndene. Tilsyn med berre ei nemnd er difor truleg tilstrekkeleg for å korrigere praksis hos alle.

Om bruk av funn frå tilsyn

Funn frå tilsyn blir i første rekkje samla og systematisert i dei individuelle tilsynsrapportane. Førebelse rapportar vert sende til tilsynsobjektet, tilbakemeldingane blir vurdert og det blir utforma ein endeleg rapport. Alle endelege rapportar vert publiserte på Datatilsynets nettsider slik at andre aktørar i tilsvarande bransjar kan lese om relevante funn. Rapportane stadfestar dessutan vår forvaltningspraksis innan dei aktuelle områda. Funna blir òg brukt i dialog med bransjeforeiningar, som igjen tek utfordringane vidare med medlemmane sine.

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

- Funn frå skule og utdanning vil bli kommunisert til sektoren, og Datatilsynet skal samanfatte funna i ein rapport. Vi vil så påverke sentrale aktørar til å lage naudsynte rettleiarar for sektoren.
- Funn frå helsesektoren om formaliserte arbeidsfellesskap vil bli følgt opp i forhold til helsemyndigheitene og bransjeorganisasjonane.
- Vi vil ha dialog med sentraleininga for fylkesnemndene for barnevernssaker og sosiale saker for å betre regelverksetterlevinga hos alle nemndene.
- Vi vil ha dialog med bransjeforeiningar om muleg utarbeiding av ein bransjenorm for privat kontrollverksemd.
- Funn frå tilsyn innan helseforsking, skal kommuniserast tilbake til dei Regionale Etiske Komiteer (REK) og aktørane i sektoren.
- I meldingsåret sendte Datatilsynet eit brev til alle statlege verksemder med informasjon om krava til internkontroll og informasjonssikring. Dette var ei oppfølging av tidlegare tilsyn.

- Fem av tilsyna var felles, nordiske initiativ. Desse tilsyna vil bli følgde opp i samarbeid mellom dei nordiske datatilsyna, spesielt når det gjeld korleis vi samarbeider mellom ulike land når internasjonale aktørar vert kontrollert. Når personvernregelverket vert modernisert innan få år, vil behovet for koordinering mellom dei ulike nasjonale tilsynsmyndigheitene auke. Dei nordiske landa har gått saman om å førebu seg på dette gjennom felles koordinering av nokre tilsyn.

Juridisk saksbehandling

Datatilsynets mål er at det juridiske arbeidet skal kjenneteiknast av god metode, klarleik og høg kvalitet. Dette skal gå igjen i alle svara vi gir på spørsmål og i saker, uansett om det er store sakskompleks eller om det er svar av rettleiande karakter til publikum. Sjølv om vi ikkje behandlar alle saker som kjem inn med full saksbehandling, skal dei som spør oss få eit svar. Målsetjinga er at svaret skal utformast på ein måte som blir opplevd som nyttig for dei som spør.

Spesielle saker og problemstillingar

Vi bruker meir tid på nokre saker enn tidlegare. Dette kjem av at vi tek fleire større og meir komplekse saker til grundig behandling enn før, samtidig som vi nedprioriterer nokre saker. I tillegg til dei sakene som er omtala andre stader i meldinga, er det somme saker og problemstillingar frå saksbehandlinga som er verdt å nemne.

«Big Data» i Coop

Vi ser eksempel på at aktørar samlar inn større mengder data om kundane sine til marknadsføring. Datatilsynet har i meldingsåret motteke fleire klager frå kundar som hadde fått tilbod frå Coop tilpassa kjøpsmønsteret deira – såkalla skreddarsydd marknadsføring. Coop registrerer kjøpsdata kvar gong ein kunde bruker medlemskortet sitt. Desse kjøpsdataa er mellom anna tid og stad for handelen, samt varer og pris. Dataa blir så analyserte ved hjelp av avanserte analyseverktøy for å avdekkje preferansar og behov, slik at marknadsføringstiltaka kan tilpassast desse.

Vi hadde ein god dialog med Coop som viste både vilje og evne til å gjere endringar. Hovudproblemstillinga var krava til samtykke for å kunne analysere og bruke kjøpsdata slik Coop gjer, samt korleis Coop skal informere om kva dei gjer. Datatilsynet meinte i utgangspunktet at Coop informerte kundane for dårleg og at samtykket Coop baserte seg på, var problematisk.

Rutinane er no lagt om slik at den som teiknar medlemskap skal gi eit aktivt samtykke til Coop for analyse av kjøpsdata – såkalla *opt in* (i motsetning til ei løysing der kundane sjølv må gi melding om at dei ikkje ønskjer dette – *opt out*). Dette er den mest personvernvennlege løysinga. I tillegg har Coop gjort omfattande forbetringar i informasjonen som vert gitt til kundane, både via personvernerklæringa og medlemsblada. Datatilsynet er svært tilfreds med den innsatsen Coop la ned for å styrkje sjølvråderetten til den einskilde når det gjeld bruk av kjøpsdata til individuelt tilpassa marknadsføring.

Ny teknologi – nye utfordringar

Ny teknologi er, som vi har peikt på mange gonger, ei drivkraft for nye løysingar – noko som òg ofte reiser juridiske spørsmål. Det er eit ønske om å automatisere tradisjonelle, manuelle system, og ein vanleg konsekvens er at *alle* som nyttar ei teneste eller oppheld seg i nærleiken, risikerer å bli registrert i ei automatisk løysing. Eit eksempel frå årets saksbehandling er ei rekkje saker om automatisering av parkering ved bruk av automatisk kjenneteiknavlesing *(Automatic number plate recognition* – ANPR).

Trondheim Parkering bad om ei vurdering av ei løysing der kundar skulle kjennast att via bilens registreringsnummer ved innkøyringa til eit parkeringshus. For å identifisere parkeringsselskapet sine kundar måtte nødvendigvis registreringsnummera til *alle* køyretøy verte lest av ved innkøyringa. Vi konkluderte med at parkeringsselskapet hadde høve til dette, forutsett at berre kundane sine registreringsnummer blei lagra, mens dei andre numra blei sletta raskt. Dei som ikkje har valt å bli kundar betalar for seg på tradisjonelt vis – anten ved bruk av kort eller kontantar.

Dette ønskjer dei no å automatisere ytterlegare, ved at alle transaksjonar for parkering skal basere seg på attkjenning av registreringsnummeret. Alle som køyrer inn på den aktuelle parkeringsplassen blir då registrert. Dei som har teikna abonnement blir registrert i forhold til den avtalen som ligg bak, mens alle andre blir registrerte, og systemet skal så produsere ein faktura til bileigarane. Desse blir då registrert *fram til dei betalar* saman med at dei oppgjev registreringsnummeret – det kan dei også gjere der og då – samt at systemet registrerer at dei forlèt parkeringsplassen.

Det blir med andre ord stadig vanskelegare å ferdast anonymt i samfunnet. Kvar einskild registrering er kanskje ikkje så inngripande, men ser ein alle registreringar samla, er mengda opplysingar som blir lagra om oss formidabel samanlikna med få år tilbake.

Rekneskapslovgivinga er (framleis) ei utfordring for personvernet

Gode intensjonar om kontrollmekanismar har i denne samanhengen òg ein konsekvens for personvernet. Reglar om bokføring og revisjon krev i dag at alle som køyrer gjennom ein bomstasjon skal identifiserast. Betalinga av bompengar skal registrerast sidan det blir sett på som betaling for ei teneste. Kravet er at partane i avtalen skal identifiserast, og tidspunktet for leveringa av tenesta skal meldast saman med art og mengd. Konsekvensen er at folk sitt høve til å påverke kva dei legg igjen av spor etter seg er svært liten, sjølv når det gjeld hendingar som kvar einskild karakteriserer som trivielle. Datatilsynet jobbar med desse og tilgrensande problemstillingar, både i enkeltsaker og i ei arbeidsgruppe under Samferdselsdepartementet.

Registerstudiar

Innan helseforsking har det ei stund vore ei utvikling der det er ønskjeleg med ei kopling mellom stadig fleire opplysingar på individnivå. Slike registerstudiar ser vi no også på andre område innan forsking, ikkje berre innanfor helsesektoren. Vi har i år til dømes hatt saker om forsking knytt til arbeidslivet. Her blir det òg store samlingar med opplysingar knytte til arbeidstakarar, og problemstillinga blir også her kor grensa skal gå for kva ein arbeidstakar må tole, med andre ord kvar personvernet står i arbeidslivet. Rapporten om Big Data kan tene som illustrasjon for kor kompleks denne problemstillinga kan bli i forholdsvis nær framtid. Nye metodar for analyse og samanstilling vil kunne utfordre personvernet på måtar Datatilsynet hittil ikkje har sett. Dette vil vi naturlegvis følgje nøye med på når vi handterer framtidige saker.

Overføring til utlandet

I meldingsåret har det vore ein auke i søknader om overføring av personopplysingar til utlandet - også utanfor EØS/EU-området. Auken var der også i 2012. Datatilsynet har hjelpt til med det juridiske, i samband med ein frihandelsavtale mellom EFTA og India.

Seint i 2013 kom det eit forslag om endring i personopplysingsregelverket. Endringa gjeld ei forenkling av prosessen med overføring av opplysingar basert på EUs standardavtalar, og vil *også*

kunne forenkle sakshandteringa hos oss. I praksis skal det svært mykje til for å kunne nekte ei overføring internt i EU/EØS i medhald av personverndirektivet, så førehandskontrollen vår hadde i realiteten liten verdi anna enn på det formelle; å sjå at avtalen var riktig fylt ut og at dei riktige vedlegga var med.

Ytringsfridom og internettnettpublisering – Min lærer og Legelisten

Datatilsynet har motteke ei rekkje klager på to tenester som tillèt at ein anonymt kan publisere vurderingane og oppfatningane sine av namngitte lærarar og legar (www.minlarer.no og www.legelisten.no). Vi har lagt til grunn at dei som opprettar og driftar eit slikt forum ikkje har eit behandlingsansvar etter personopplysingslova, og at det er den einskilde ytrar som eventuell må stå ansvarleg for ytringar som ikkje er verna av ytringsfridomen. Vi har også lagt til grunn at det er den einskilde ytringa som må vurderast opp mot ytringsfridomen, ikkje eksistensen av forumet.

Vi fekk to klager som gjaldt konkrete ytringar i meldingsåret – ei på kvart forum. I begge tilfella kom vi til at ytringane var verna av ytringsfridomen, og at reglane i personopplysingslova derfor ikkje gjeld ved publiseringa. Det blei lagt vekt på at fråsegnene etter ei objektiv vurdering, ikkje var særleg negative eller av krenkjande art. Det blei òg lagt vekt på at fråsegnene var knytte til personane si yrkesutøving, og ikkje gjaldt personlege forhold. Dessutan blei det vurdert at både legar og lærarar er vist ein særleg tillit gjennom offentleg autorisasjon og tilsetjing, og at ein derfor må forvente og tillate at det blir diskutert om desse gjer oppgåvene sine i tråd med føresetnadene.

Prioriteringar av saker og førespurnadar

Det kjem inn mange ulike førespurnadar til Datatilsynet, og vi har ikkje kapasitet til å undersøkje alle klager og spørsmål i full breidde. Vi har i fleire år jobba med å prioritere kva vi skal ta tak i for å oppnå best mogeleg personvern med dei ressursane vi har. Ei typisk vurdering vi gjer, er å sjå på om spørsmålet i ei sak har aktualitet ut over den konkrete saka. Om ei sak ikkje har det, har vi vore strengje på prioriteringa i meldingsåret. Nedprioriteringa av enkeltsaker har blitt klaga til Personvernnemnda, der vi har fått stønad til vurderinga vår.

Parallelt med ei streng prioritering av kva for nokre saker vi skal ta opp til full behandling, og ei vurdering av om vi skal følgje opp med ein form for kontroll, har vi styrkt arbeidet vårt med å rettleie publikum og verksemder ytterlegare, sjå nedanfor om juridisk rettleiingsteneste. Ved å prioritere på denne måten, har vi fått høve til å ta tak i meir komplekse problemstillingar og større sakskompleks, noko vi meiner har større verdi for borgarane sitt personvern.

Dokument og saker

Det blei journalført til saman 5 059 dokument i 2013, noko som er ein liten auke frå året før. Mengda med dokument og saker vi opprettar, er ganske stabil over tid.

Alle journalførte **dokument** (ikkje interne dokument):

	2010	2011	2012	2013
Dokument inn	3 111	2 740	2 646	2 814
Dokument ut	3 184	2 138	2 212	2 245
Totalt	**6 295**	**4 878**	**4 858**	**5 059**

Alle nye journalførte **saker:**

	2010	2011	2012	2013
Nye saker	1 580	1 345	1 218	1 405

Innsynskrav

Datatilsynets postjournalar er tilgjengelege via Offentlig Elektronisk Postjournal (OEP), som er ei samordning av offentlege postjournalar på Internett.

	2012	2013
Innsynskrav via OEP	2 029	2 502
Direkte innsynskrav	797	772
Totalt	**2 826**	**3 274**

I meldingsåret handterte tilsynet 2 502 innsynskrav via OEP. Dette er ein auke på 473 krav frå i fjor. I tillegg fekk arkivtenesta 772 innsynskrav direkte. Til saman har vi dermed behandla 3 274 innsynskrav i 2013. Det ser ut til at talet på innsynskrav aukar, noko som er naturleg etter endringane i offentleglova. Vi har etablert eit godt system for handtering av slike krav, ved at arkiv og saksbehandlar samarbeider om å effektuere sakene. Vi har òg etablert eit system der same dokument berre blir vurdert ein gong, slik at neste gong nokon ønskjer innsyn, blir det fort ekspedert direkte frå arkivet.

Tall for OEP	2012	2013
Antall dokument med innsynskrav	2 029	2 502
Antall sladda dokument sendt ut	251	250
Antall avslag på innsyn	137	112

Klagebehandling

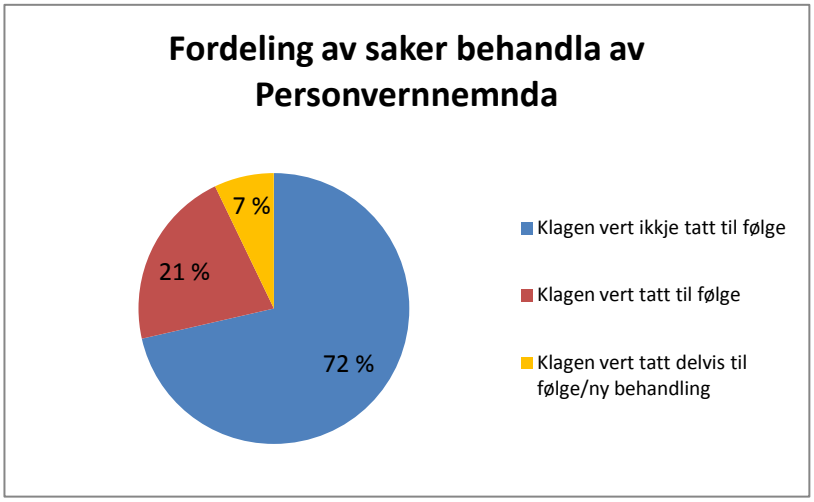
I 2013 blei det registrert 50 klager på vedtaka våre, ein auke samanlikna med året før, då vi registrerte 35 klager. Sakene omfattar klager på forvaltingsvedtak og avslag på innsyn etter offentleglova og forvaltingslova.

Ti av klagene gjaldt behandling av innsynskrav, og åtte av dei blei sende til klageinstansen som var Fornyings-, administrasjons- og kyrkjedepartementet (FAD). Berre ei av sakene der Datatilsynet opphavleg gav avslag på innsyn, blei heilt omgjort av FAD. 20 av klagene er framleis til behandling hos Datatilsynet, mens resten blei sende til Personvernnemnda.

Personvernnemnda

I meldingsåret sende vi over fleire saker til klagebehandling i Personvernnemnda enn tidlegare, til saman 30 saker (nokre av dei på grunnlag av klager som kom inn i 2012). Heile 13 av sakene blei sende over i perioden oktober-desember.

Nemnda hadde ved årsskiftet rokke å behandle 14 av sakene. I tre av sakene har klagaren fått medhald, mens ei sak er send tilbake til Datatilsynet for ny behandling. I dei andre ti støtta nemnda våre vurderingar:



Seks saker dreia seg om same forhold, dei såkalla GE-sakene. Desse er omtala nærmare i kapittel 3 under *Helse og* velferd, mens andre enkeltsaker vi har lyst til å dra fram er omtala under sine respektive område i same kapittel.

Dei sakene som blir gjort om i nemnda, er saker som ikkje har noko klart svar, og der Datatilsynet òg synest det er greitt med ei avklaring rundt tolkinga av regelverket. Delen som blir omgjord er uansett svært låg i forhold til den mengda saker som blir behandla i løpet av eit år.

Avklaring av prioriteringar
Personvernnemnda tok i meldingsåret mellom anna stilling til ei sak der klaga var retta mot avgjerda vår om ikkje å forfølgje ei sak vidare på grunn av prioritering.

Ein bebuar i eit sameige hadde montert eit skilt med «videoovervaking» i fellesarealet. Det var berre sett opp eit skilt, og bebuaren håpa at dette skulle vere tilstrekkeleg for å skremme eventuelle gjerningspersonar. Datatilsynet korresponderte med partane, men valte å ikkje dra på tilsyn på grunn av avgrensa ressursar. Personvernnemnda kom til at vi hadde oppfylt utgreiingsplikta og rettleiingsplikta vår etter forvaltingslova. Saka var blitt utgreidd på ein tilfredsstillande måte, og nemnda fann ikkje grunnlag for å kritisere prioriteringa.

Sjå fullstendig oversikt over alle sakene vi sende til Personvernnemnda i 2013 i *Vedlegg C.*

Konsesjonsplikt

Eit spørsmål som går igjen når verksemder tek kontakt, er om handteringa deira av personopplysingar krev konsesjon frå Datatilsynet. Det gjeld både i den formelle sakshandteringa og i førespurnadene som kjem via telefon og e-post. Vi freistar å avklare dette med råd og rettleiing over telefon og i møte.

Det blei i meldingsåret søkt om 173 konsesjonar frå Datatilsynet, og vi gav 155 konsesjonar:

	2010	2011	2012	2013
Gitte konsesjonar	324*	143	132	155

**av desse var 215 bankkonsesjonar*

Datatilsynet har i meldingsåret sett på grensene for når vi kan og bør gi konsesjon til helseregister, samt kva som bør vere forskriftsregulert eller på annan måte knytt opp til ein meir demokratisk prosess enn ei forvaltingsavgjerd frå oss. Vi har i nokre saker ikkje gitt konsesjon etter søknad, då vi meiner det gjeld så sensitive opplysingar at det bør ha ei anna rettsleg forankring (til dømes HIV-registeret som er omtala under *Helse og velferd* i kapittel 3). Det blei òg gitt avslag til registeret *«Norsk kvalitetsregister for biologiske lækjemiddel»* (NOKBIL) som vi meinte var for stort, og ikkje nok tidsavgrensa, til at konsesjon var eit riktig rettsleg grunnlag.

Trenden med at konsesjonar innan forsking går igjen i form av søknader om endringar og utvidingar, held seg som dei føregåande åra. Sakene blir med andre ord meir og meir kompliserte ettersom det kjem ønske om endringar og utvidingar. På dette området vil vi i nær framtid bli stilte overfor nye utfordringar med innføring av ny lovgiving på helseregisterområdet (les meir under *Helse og velferd* i kapittel 3). Vi reknar derfor med at vi kjem til å bruke ein del ressursar på konsesjonssaker også i framtida.

Meldeplikt

Alle som vil setje i gong med behandling av personopplysingar har meldeplikt. Meldinga skal sendast til Datatilsynet seinast 30 dagar før verksemda startar behandlinga. Alle meldingar som kjem inn blir lagt inn i ein database som er offentleg tilgjengeleg via heimesidene våre. Meldinga som blir send inn, gjeld i tre år. Deretter må det sendast ei ny melding dersom verksemda framleis handterer personopplysingar. Det er gitt unnatak frå meldeplikta for verksemder som har personvernombod.

	2010	2011	2012	2013
Nye meldingar	3 693	4 010	2 954*	8 912**
Meldingar per 31.12 – totalt	10 055	11 211	10 909	15 979

** Det kom inn over 5 000 meldingar frå ein og same leverandør i 2012, men vi rakk ikkje å registrere alle same år som dei kom inn*
*** I dette talet ligger mange av meldingane som kom inn i 2012*

Sjølv om vi ser bort frå den store mengda meldingar vi fekk inn frå *ein* leverandør av elektroniske køyrebøker i 2012, er trenden framleis at talet på aktørar som behandlar personopplysingar, aukar. Vi har dessutan framleis grunn til å tru at det er ein del verksemder som ikkje melder inn behandlinga si av personopplysingar til Datatilsynet. Funn frå kontrollar om kameraovervaking er med på å underbyggje dette synspunktet. Som tidlegare år reknar vi med at dette kjem av at verksemdene ikkje er klare over denne plikta.

Høyringar

Ein viktig del av ombodsrolla vår, er å gi svar på høyringar. Vi fekk til saman 134 invitasjonar til å vere høyringsinstans i 2013. Til 52 av desse høyringane hadde vi konkrete merknader. Dei resterande sakene har vi frå og med 2012 valt å dele i to kategoriar; dei sakene vi ikkje hadde merknader til og dei vi tek til etterretning. Forskjellen er at i dei sakene der vi svarer at vi ikkje har nokon merknader, har vi vurdert eventuelle konsekvensar for personvernet. Dei sakene vi tek til etterretning, har vi

vurdert som klart utan konsekvensar for personvernet, og vi har ikkje hatt saka til saksbehandling eller sendt skriftleg svar til avsendaren. Vi meiner dette er ei meir effektiv utnytting av ressursane våre.

Oversikt over høyringssakene:

	2010	2011	2012	2013
Med merknadar	51	58	58	52
Utan merknadar	72	64	47	29
Tatt til etterretning	-	-	58	53
Totalt	**123**	**122**	**163**	**134**

Høyringar der Datatilsynet har hatt kommentarar, blir omtalte under sine respektive område i kapittel 3. For ei fullstendig liste over saker der vi har sendt merknader eller sagt at vi ikkje har merknader, sjå *Vedlegg B.*

Som tidlegare år er Helse- og omsorgsdepartementet, samt Justis- og beredskapsdepartementet, dei to største leverandørane av nytt regelverk som vil ha tyding for personvernet. Situasjonen har vore slik i mange år. På justissektoren ser vi dessutan at det er fleire saker som heng saman med rapporten etter terroraksjonen 22. juli 2011.

Avsendar av høyringa	TOPP 5 – tall på høyringsinvitasjonar
Helse- og omsorgsdepartementet	17
Justis- og beredskapsdepartementet	16
Finansdepartementet og Finanstilsynet	10
Fornyings-, administrasjons- og kyrkjedepartementet	6
Barne-, likestillings- og inkluderingsdepartementet	4

Datatilsynet har som tidlegare år lagt vekt på klare reglar i dei tilfella der reglane skal danne grunnlag for kontroll eller overvaking av personar. Vi meiner det er viktig med klare og balanserte reglar slik at den einskilde har god moglegheit til å vite kva staten gjer. Vi meiner også at det er viktig med god balanse mellom inngrep for den einskilde, og samfunnet sine interesser og behov.

Lovbrotsgebyr og tvangsmulkt

Vi freistar å bruke dei verkemidla vi har på ein god og balansert måte for å sikre at regelverket vert følgt. Lovbrotsgebyr og tvangsmulkt skal ikkje vere det primære verktøyet vårt for å sikre dette, men noko vi bruker i dei mest alvorlege sakene. I meldingsåret blei det gitt lovbrotsgebyr i sju saker, to av dei er til behandling i Personvernnemnda.

Tabellen viser ei oversikt over gebyra:

Verksemd	Gebyr	Merknadar
Teletopia Gruppen AS	Kr 200 000,-	Er til behandling i Personvernnemnda
Personal Utvelgelse Oslo AS	Kr 50 000,-	
Retura Sør-Trøndelag AS	Kr 100 000,-	
Folkehelseinstituttet – SRI-data	Kr 350 000,-	
Gjensidige Forsikring BA	Kr 600 000,-	
AS Skan-kontroll	Kr 600 000,-	Er til behandling i Personvernnemnda
Securitas	Kr 75 000,-	

Sakene i tabellen er stort sett omtala under sine respektive område i kapittel 3.

Juridisk rettleiingsteneste

Den juridiske rettleiingstenesta i Datatilsynet, svarar på fleire tusen telefonar og e-postar frå publikum kvart år. Tenesta blir kontakta av både privatpersonar og verksemder, og det er stor variasjon i spørsmåla som kjem inn. Rettleiingstenesta er eit viktig lågterskeltilbod for publikum. Eit viktig mål med tenesta er å gjere borgarar og verksemder i stand til å ta vare på personvernet sjølve.

Det har vore eit overordna mål i Datatilsynet at fleire saker skal handterast via rettleiingstenesta, og som ein konsekvens av dette er det tilsett tre nye medarbeidarar i denne faggruppa. Hovudforskjellen frå dei andre faggruppene, er at primæroppgåva til denne gruppa er å yte juridisk rettleiing, mens dei andre faggruppene har saksbehandling som primæroppgåve.

Oversikt over omfanget av spørsmål til tenesta:

	2010	2011	2012	2013
Telefonar	7 309	5 196	4 645	5 032
E-post	2 727	2 632	2 175	2 546
Totalt	**10 036**	**7 828**	**6 820**	**7 578**

I løpet av 2013 har rettleiingstenesta svara på til saman 7 578 spørsmål via e-post og telefon. Dette er ein oppgang frå 2012, men samanlikna med tidlegare år, synest trenden likevel å vere at vi får færre spørsmål på telefon, mens tala for e-post er nokså stabile.

Når nokon tek kontakt med denne tenesta, får dei ei rettleiing om regelverket. Det blir alltid presisert at svara berre er av rådgivande karakter, og at dei ikkje må oppfattast som eit formelt løyve eller forvaltningsrettsleg vedtak. Det blir likevel gjort ei løpande vurdering av om ei sak skal underleggjast saksbehandling og dermed journalførast. Rettleiingstenesta tek òg imot anonyme tips, noko som i løpet av meldingsåret har resultert i kontrollar frå Datatilsynet.

Kva lurer dei som tek kontakt på?

Rettleiingstenesta lagar kvart år ein intern rapport, der e-postar og telefonsamtalar blir analyserte. Rapporten skal gi oss ei betre oversikt over kva slags spørsmål vi får, samt fange opp trendar og liknande.

Prosentfordeling mellom telefon og e-post (avrunda tal):

Tema	Telefon	E-post
Arbeidsliv/ skule	25 %	22 %
Kamera	18 %	16 %
Register	14 %	16 %
Melding/ konsesjon	10 %	8 %
Internett	7 %	14 %
Fødselsnummer	5 %	5 %
Anna	25 %	18 %

Vårt hovudinntrykk er at det er den registrerte som tek kontakt. Innan kategorien arbeidsliv, er for eksempel heile 76 prosent av spørsmåla på e-post frå arbeidstakarar. Det ser ut til at det er dei «nære ting» som opptek folk. Det vil seie personvernrettslege spørsmål som får direkte innverknad på folk sin kvardag. Det kan for eksempel vere ein arbeidstakar som kjenner seg overvakt på jobb, ein privatperson som meier at ein nabo overvaker han med kamera eller som kjenner seg uthengt på Internett, skuleelevar som har spørsmål om kva skulen kan gjere og så vidare. Vi hadde forventa eit oppsving i spørsmål av meir prinsipiell karakter om staten si overvaking etter all mediemerksemda Snowden-saka har fått. Dette har ikkje skjedd.

Arbeidsliv/skule: Arbeidsliv/skule utgjer ein stor del av spørsmåla som rettleiingstenesta får inn. Dei fire største underkategoriane innanfor arbeidsliv, er spørsmål knytte til GPS-sporing av arbeidstakarar, innsyn i/sletting av arbeidstakarane sine e-postkasser og ulike former for kontrolltiltak slik som kameraovervaking. Generelt kan vi seie at temaet overvaking i arbeidslivet er aukande.

Når det gjeld skule/barnehage utgjer dette om lag fire prosent av alle spørsmåla. Fleire spørsmål er knytte til informasjonstryggleik, som for eksempel bruk av læringsplattformer, lagring i skytenester, bruk av SMS og liknande. Andre spørsmål gjeld lovlegheita rundt foto og filming av elevar, utlevering av elevlister og overvaking av elevane sin PC-bruk. Dei fleste spørsmåla her er knytte til grunnskulen.

Kameraovervaking: Kameraovervaking i burettslag og i nabosituasjonar er tema som går igjen, og som har auka samanlikna med 2012. Andre spørsmål gjeld bruk av webkamera og lovlegheita av ulike kamera. I meldingsåret har vi også fått ein del spørsmål om bruk av dashbord-kamera. Dette er ein ny trend, og vi har på bakgrunn av dette trekt opp retningslinjer for slik bruk. Desse retningslinjene er også kommuniserte på Datatilsynets nettsider.

Register: Spørsmåla rundt register gjeld eit breitt spekter, slik som helse-, kreditt-, kunde-, medlems- eller offentlege register. Mange av spørsmåla gjeld kva som kan registrerast i eit register, kor lenge det kan registrerast, kven som har tilgang til opplysingane og korleis ein får retta eller sletta opplysingar i eit register.

Internett: Spørsmål i denne kategorien er i hovudsak fordelt på følgjande hovudområde; Facebook og andre sosiale medium, publisering av bilete/film, nummeropplysningsaktivitet, offentleg journal på nett, ytringsfridom og informasjonstryggleik på Internett. Facebook og andre sosiale medium

utgjer den største delen, og gjeld sletting av profil eller annan informasjon, publisering av bilete utan samtykke og falske profilar. Fleire av desse spørsmåla blir vist vidare til tenesta slettmeg.no.

Fødselsnummer: Det er nesten berre privatpersonar som spør om bruk av fødselsnummer. Det er gjerne uroa menneske som kjenner ubehag ved å måtte gje frå seg fødselsnummeret sitt. Ein stor del av desse spørsmåla gjeld bruk av fødselsnummer i møte med offentlege etatar, og ein noko mindre del gjeld private verksemder og bruk av kredittvurdering ved fakturakjøp. Mange spørsmål lèt seg ikkje så lett kategorisere, då det er eit stort sprik i innhald.

Melding og konsesjon: Det kjem mange spørsmål om ei konkret behandling er melde- eller konsesjonspliktig. Dessutan er det mange som tek kontakt om endring og oppfølging av melding og konsesjon.

Anna: Denne kategorien er ganske stor, men har blitt vesentleg mindre samanlikna med 2012. Dette skuldast at vi er blitt flinkare til å sortere desse inn i dei andre kategoriane. Omtrent halvparten av spørsmåla fell utanfor personopplysingslova, spørsmål knytte til offentleglova eller spørsmål om brot på teieplikt (som ofte fell innunder forvaltingslova). Anna som hamnar i denne samlekategorien er spørsmål om lydopptak, databehandlaravtale, overføring av personopplysingar til utlandet og informasjonstryggleik.

Personvernombod

Ved utgangen av 2013 har Datatilsynet registrert 210 personvernombod. Personvernomboda representerer 420 verksemder.

	2010	2011	2012	2013
Personvernombod	173	193	203	210
Verksemder	350	370	390	420

Datatilsynet har brukt omtrent eitt årsverk på arbeidet med personvernomboda, fordelt på fleire medarbeidarar. Arbeidet består stort sett av å arrangere faglege tilbod slik som kurs og konferansar, rettleiing over telefon og e-post, sende ut nyhetsbrev til omboda, behandling av søknader om nye ombod og å drifte sidene for personvernomboda på www.datatilsynet.no.

Datatilsynet har laga fem forskjellige kurs for personvernomboda; eit grunnkurs for nye ombod, to juridiske påbyggingskurs og to kurs i informasjonstryggleik og internkontroll. Grunnkurset har vore halde på både vår- og hausthalvåret. I tillegg blei den årlege fagdagen for alle personvernomboda arrangert i april. Både kursa og fagdagen har vore fullteikna og får gode tilbakemeldingar.

Deltakelse i arbeidsgrupper og 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 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, samt holde kontakt med fagmiljøet.

Tilsynet deltar nå i tre komiteer:

SN/K 171 arbeider i hovedsak relatert til ISO/IEC JTC 1/SC 27 IT Security techniques
SN/K 175 Intelligente Transportsystemer (ITS)
SN/K 188 Person-ID, kortsystemer, biometri, sikre signaturer, borgerkort

NAFAL

Datatilsynet er oppnevnt med en representant i nasjonalt råd for Facilitation (NAFAL), sivil luftfart. Rådets mandat er å fremme forslag til fastsettelse av standarder for effektiv gjennomstrømming av personer, bagasje og varer på lufthavner. Luftfartstilsynet koordinerer gruppen, som har medlemmer fra tolv ulike myndigheter og virksomheter i sivil luftfart.

Biometri Forum

Datatilsynet deltar i Biometri Forum, som er et uformelt forum for presentasjon og diskusjon innenfor området bruk av biometri. Det er lagt stor vekt på å få inn nye ideer, samtidig som møtet benyttes til orientering om pågående prosjekter innenfor offentlig og privat sektor.

I prinsippet er forumet åpent for alle interesserte innen offentlig sektor, næringsliv og forskning. Forumet møter omtrent to ganger i året og har deltakere fra departementer, direktorater og en del private bedrifter, samt Høgskolen i Gjøvik. Forumet arrangeres i tett samarbeid med *Forum for Research and Innovation in Security and Communications* (FRISC) og European *Association for Biometrics* (EAB).

ITS-rådet (ITS-Intelligente Transport Systemer)

En representant fra Datatilsynet er oppnevnt som medlem av ITS-rådet. Rådets overordnede formål er å bidra til implementering av ITS-løsninger i Norge, og å bygge opp under de norske transportpolitiske målene om trafikksikkerhet, fremkommelighet, miljø og tilgjengelighet for alle. ITS-rådet skal også fremme samarbeid og medvirkning i nasjonale og internasjonale prosesser og markeder for ITS. Rådet ledes av vegdirektøren, og har 14 faste medlemmer. I tillegg inviteres deltakere etter behov.

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 ny forordning. Tilsynet har blant annet gitt bistand til Fornyings-, administrasjons- og kirkedepartementet. Vi har også deltatt i Justis- og beredskapsdepartementets 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.

Arbeidsgruppe under Arbeidsdepartementet

Datatilsynet har deltatt i en referansegruppe nedsatt av Arbeidsdepartementet. Gruppen har hatt som oppgave å kartlegge omfanget av kontroll og overvåking i arbeidslivet og å belyse de rettslige utfordringene på området. Gruppen skulle vurdere personvern- og arbeidslivsutfordringer som følge av kontroll og overvåking. Deltakelsen i gruppen har ført til bedret kontakt med relevante personer innen departement og organisasjonene i arbeidslivet.

På oppdrag av arbeidsgruppen har forskningsstiftelsen FAFO dessuten forfattet en gjennomgang av den forskningen som er gjort på området.

Gruppen ble avsluttet i meldingsåret.

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.

Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren

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 Datatilsynet også i grupper knyttet til utarbeidelse av faktaark og veiledninger etter normen. I meldingsåret gjaldt dette bruk av video-opptak i helsetjenesten og bruk av portalløsninger, SMS og e-post.

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 mulighet til å ivareta egne rettigheter etter helselovgivningen og personopplysningsloven. Datatilsynet mottar en rekke spørsmål om dette, og det er viktig for oss å være med på å påvirke arbeidet.

Arbeidsgruppe i Samferdselsdepartementet – helautomatiske bomstasjoner

Prosessen rundt helautomatiske bomstasjoner er fortsatt ikke 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 Samferdselsdepartementet og Statens Vegvesen som de andre

hovedaktørene. Statens vegvesen og Datatilsynet har i løpet av det siste halve året dessuten utarbeidet en rapport om vilkår for og konsekvenser av en mulig obligatorisk bombrikke for lette kjøretøyer. Et arbeid som skal legges frem for denne arbeidsgruppen i Samferdselsdepartementet.

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

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. Arbeidet ble avsluttet i 2013 med implementeringen av SIS II.

KINS

Datatilsynet har deltatt som samarbeidspartner i Kommunal informasjonssikkerhet (KINS). Dette innebærer å delta på styremøter som observatør/bidragsyter og delta i planleggingen av KINS sine arrangementer. Vi er også fast bidragsyter med foredrag eller som paneldeltakere på disse arrangementene.

Du Bestemmer – et samarbeidsprosjekt

DuBestemmer er et samarbeidsprosjekt mellom Senter for IKT i utdanningen, Teknologirådet og Datatilsynet. Datatilsynet hadde prosjektledelsen ved etableringen i 2007, men dette ble overført til Senter for IKT i utdanningen for et par år siden.

Det at vi har klart å utvikle DuBestemmer på en slik måte at det fortsatt oppfattes et viktig tilskudd til undervisningen på norske skoler, seks år etter lanseringen, må kunne karakteriseres som en suksess, og et godt eksempel på vellykket statlig samarbeidsprosjekt.

Norsk senter for Informasjonssikring – NorSIS

Datatilsynet er representert i styret til NorSIS ved direktøren.

Internettvalgstyret

Datatilsynet var i forbindelse med Stortingsvalget høsten 2013 representert i internettvalgstyret ved direktør Thon. Styret skulle se etter at stemmegivningen via Internett og opptelling av internettstemmene ble gjort i henhold til regelverket.

Kommunikasjonsvirksomheten

Personvernlovgivningen legger i stor grad ansvaret på den enkelte når det gjelder å ivareta sitt eget personvern. Samtidig er alle som behandler personopplysninger, enten det er offentlige etater eller private virksomheter, pålagt vesentlige plikter for å etterleve lovgivningen på området.

I strategien for perioden frem til 2016 har Datatilsynet som to av våre overordnede mål at vi skal sette borgeren i stand til å ivareta sitt eget personvern og at vi skal ha stor synlighet i personverndebatten. Vi har også som strategisk satsing at vi skal bidra til økt kunnskap om, og interesse for personvern, og jobbe aktivt for at andre aktører skal legge vekt på personvernhensyn. I tillegg er det slik at en målrettet kommunikasjonsvirksomhet er helt avgjørende for å få mest mulig effekt av de øvrige virkemidlene saksbehandling, tilsynsvirksomhet, utredning og analyse.

Kommunikasjon brukes derfor som et aktivt virkemiddel både ved utøvelse av Datatilsynets ombudsrolle, og i rollen som forvaltningsorgan.

Foredrag, konferanser og seminarer

Det å være til stede på ulike arenaer hvor representanter for virksomheter, interesseorganisjoner og andre aktører møtes er høyt prioritert fra Datatilsynets side. Ved siden av å delta med foredragsholdere i regi av andre, har vi også etablert våre egne møteplasser for de som er interesserte i personvern. I tillegg til våre kurs- og seminarer i regi av personvernombudsordningen, gjennomførte vi tre seminarer i egen regi i løpet av 2013:

I anledning den internasjonale personverdagen 28. januar arrangerte Datatilsynet og Teknologirådet et seminar der vi presenterte statusen for personvernet i Norge, samt trender fremover på feltet. I tilknytning til seminaret ble det publisert en egen rapport, *«Personvern 2013 – tilstand og trender»*. Seminaret ble vist stor interesse og ble vurdert som så vellykket at det blir gjentatt i 2014.

I mai 2013 ble det arrangert et frokostseminar om innebygd personvern. Seminaret ble åpnet av daværende statsråd Rigmor Aasrud, som også deltok i den påfølgende debatten. Seminaret ble fulltegnet, med over 60 eksterne deltakere. Les mer om dette i kapittel 3, under *Innebygd personvern*.

Samme måned gjennomførte vi også seminaret *«Hvem eier våre gener?».* Her presenterte vi en rapport der personvernutfordringer knyttet til viderebruk av genetiske opplysninger ble beskrevet. Ellen Økland Blinkenberg, overlege ved Senter for medisinsk genetikk og molekylærmedisin ved Haukeland Universitetssykehus i Bergen, holdt et innlegg om utfordringer knyttet til gentester, med utgangspunkt i sin nyutgitte bok *«Min DNAgbok. Personlig og forståelig om genetikk».* Også dette seminaret hadde god deltakelse.

Det ble i meldingsåret holdt 149 foredrag på eksterne arrangementer, mot 118 året før:

	2009	2010	2011	2012	2013
Antall	110	136	129	118	149

Forespørsler om foredrag har blitt vurdert ut fra satsingsområder i virksomhetsplanen for 2013 og er gitt prioritet ut fra bransje, antall deltakere, tema og kapasitet på aktuelt tidspunkt. Vi har et mål om å holde mellom 120 og 150 eksterne foredrag i løpet av året. Selv om vi har hatt et høyt aktivitetsnivå på området i 2013, har vi likevel måttet takke nei til rundt 35 forespørsler om å stille med foredragsholder.

Foruten generelle foredrag om personvern og Datatilsynets oppgaver har etterspurte temaer for foredrag vært informasjonssikkerhet/internkontroll, Big Data og skytjenester, samt temaer relatert til offentlig sektor og helseområdet.

Hjemmesiden

For å møte publikums informasjonsbehov på en helhetlig måte, samarbeider juridisk veiledningstjeneste og informasjonsavdelingen om å produsere og revidere informasjonsmateriell. Basert på analyser av telefonhenvendelser og bruk av nettsidene, har samarbeidet resultert i brukertilpasset informasjon på nettsidene. Dette gjelder blant annet spørsmål og svar på prioriterte fagområder, veiledning om kameraovervåking, lydopptak av telefonsamtaler og ikrafttredelse av åndsverkloven. I tillegg til rent veiledningsmateriell blir også nyheter, tilsynsrapporter og høringsuttalelser publisert fortløpende.

Vi har i meldingsåret etablert retningslinjer for forvaltning av innholdet på nettsidene. Dette innebærer at vi på en mer systematisk måte enn tidligere jobber med å forbedre og kvalitetssikre innholdet, i tråd med både brukernes behov og våre egne målsetninger. Vi har også jobbet med å forbedre søkefunksjonaliteten og spørsmål og svar-funksjonen.

Andelen brukere som benytter mobil når de besøker våre nettsider er på 13 prosent. Vi vil i tiden fremover jobbe videre med å ytterligere tilpasse nettsidene til mobile flater, ettersom dette i økende grad blir en foretrukket kanal.

Personvernbloggen

I februar 2013 lanserte vi www.personvernbloggen.no, i tråd med vår strategi for sosiale medier. Målet med bloggen er blant annet at våre budskap skal komme tydeligere fram i personverndebatten, at vi skal vise bredden i de sakene vi jobber med og at den skal generere trafikk til hjemmesiden vår. Etter lanseringen har vi publisert 41 om ulike tema. Statistikken viser at bloggen hadde 8 198 besøk i 2013, og antall faste følgere øker jevnt. De mest leste innleggene omhandlet de nye cookie-bestemmelsene, googlebriller og forslaget om opprettelse av elevregister. Vi erfarer at innleggene deles i sosiale medier og i noen grad skaper medieomtale. Personvernbloggen skal evalueres i løpet av første halvår 2014.

Twitter

I 2013 har vi vært noe mindre aktive på twitterkontoen @datatilsynet enn året før:

	2009	2010	2011	2012	2013
Antall meldinger	135	168	275	391	220
Antall følgere	1 000	3 000	4 900	7 500	10 065

Imidlertid har direktør Bjørn Erik Thon benyttet sin twitterkonto aktivt også på Datatilsynets vegne. Hans konto hadde ved årsskiftet 3 620 følgere.

Mediekontakt

Mediene vurderes som en svært viktig kanal for Datatilsynets budskap, og det er jevn pågang og interesse fra disse. Vi legger stor vekt på å ha et profesjonelt forhold til mediene. Dette innebærer at vi skal ha god tilgjengelighet og et høyt servicenivå overfor journalistene. Dette mener vi å ha lykkes godt med også i 2013.

I løpet av året har Datatilsynet registrert 850 besvarte mediehenvendelser:

	2009	2010	2011	2012	2013
Antall henvendelser	1 293	1 432	1 120	876	850

Som det går frem av oversikten har vi håndtert noen færre mediehenvendelser enn tidligere år. Årsaken til dette er nok sammensatt. En del av nedgangen fra 2011 skyldes at debatten om datalagringsdirektivet preget tiden frem til Stortinget gjorde sitt vedtak våren 2011. I tillegg er det slik at noen flere henvendelser enn tidligere nå går direkte til ledere og fagpersoner, slik at disse ikke alltid blir fanget opp av informasjonsavdelingens statistikk. Henvendelser om å få tilgang til offentlige dokumenter blir dessuten i hovedsak håndtert via arkivet og den elektroniske postjournalen, og fanges heller ikke opp av statistikken.

Flere av de sakene som har fått medieomtale har kommet som følge av aktive utspill til mediene fra vår side. Vi har videre deltatt i 13 debattprogrammer, hovedsakelig i radio.

Følgende saker har fått særlig oppmerksomhet i meldingsåret:

- Den amerikanske overvåkingsskandalen – Snowdens avsløringer
- Ytterligere kriminialisering av forberedelse til terrorhandlinger
- Ny åndsverklov mot fildeling
- Opptak av telefonsamtaler i finansforetak
- Tilsyn med Gjensidige forsikring
- Folkehelseinstituttet pålagt å slette DNA-opplysninger
- Politiets bruk av pass- og førerkortregistre
- Big Data, blant annet Coops individorienterte markedsføring
- Overvåking i arbeidslivet, bruk av kamera og GPS
- Ulovlig bruk av pasientdata til forskning
- Kameraovervåking i drosjer, og bruk av såkalte dashkameraer i biler
- Lagring av elevopplysninger (forslag om elevregister, og lagring av elevopplysninger hos Riksarkivet)
- Manglende informasjonssikkerhet, Dagbladets avsløringer i serien «null-ctrl»
- Ulovlig publisering av opptak fra kameraovervåking
- Forslag om gjeldsregister

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

	2009	2010	2011	2012	2013
Antall innlegg	16	13	6	10	8

Bruk av kronikker må også sees i sammenheng med etablering av personvernbloggen, der vi har publisert over 40 innlegg siden lanseringen i februar.

Brukerundersøkelse/omdømme

Datatilsynet har ikke brukt ressurser på omdømmeundersøkelser. For å få til naturlige sammenligningsgrunnlag mellom private og offentlige virksomheter blir Datatilsynet likevel med jevne mellomrom gjort til gjenstand for målinger fra ulike selskapers side. I en kåring i regi av rekrutterings- og konsulentselskapet Universum, fikk Datatilsynet i mai 2013 prisen for «årets nykommer» på listen over de mest attraktive arbeidsgiverne for IT-studenter.

Klart språk

I 2012 ble det satt i gang ekstra klarspråktiltak i Datatilsynet, med bistand fra Direktoratet for forvaltning og IKT (Difi). Klarspråksatsingen fortsatte i 2013 med gjennomføring av følgende tiltak:

- Alle ansatte har deltatt på en fagdag i klarspråkarbeid, der våre forbedringspunkter i klarspråksammenheng ble gjennomgått. Fagdagen var tilpasset våre behov med bakgrunn i resultatene fra kartlegging av ulike tekster, og ble avholdt med ekstern ekspertbistand.
- Vi har utviklet en egen språkprofil for Datatilsynet
- Ordlisten på datatilsynet.no er kvalitetssikret med bistand fra Språkrådet

Klarspråkarbeidet fortsetter også i 2014.

Samisk språk

Innenfor forvaltningsområdet for samisk språk skal virksomhetene følge opp språkreglene i sameloven. Vi vurderer behovet for oversetting fortløpende og har følgende materiale tilgjengelig på samisk:

- Personopplysningsloven (datatilsynet.no)
- Personvernprinsippene (datatilsynet.no)
- Informasjonen «Hva er personvern?» (datatilsynet.no)
- Undervisningsopplegget Du Bestemmer

Det er ikke blitt gjort nye oversettelser i meldingsåret.

Budsjett, organisasjon og administrasjon

Bevilgning

Datatilsynet fikk i meldingsåret 37 753 000 kroner til disposisjon. Dette var en økning på 7,82 prosent i forhold til 2012. I tillegg ble 1 292 000 kroner overført fra 2012. Disse midlene var øremerket påbegynte IKT-investeringer. Det ble videre gitt en tilleggsbevilgning på 366 000 kroner som kompensasjon for økte utgifter som fulgte av det sentrale lønnsoppgjøret i mai 2013. Til sammen disponerte Datatilsynet dermed 39 411 000 kroner i meldingsåret

Datatilsynets lønnsutgifter var i meldingsåret på 71 prosent, mens øvrige driftsutgifter var på 29 prosent. I 2012 var fordelingen 69 prosent til lønn og 31 prosent til drift.

	2009	2010	2011	2012	2013
Bevilgning	Kr 29 020 000,-	Kr 30 989 000,-	Kr 32 051 000,-	Kr 35 015 000,-	Kr 37 753 000,-

Organisasjon

Datatilsynet ledes av direktør Bjørn Erik Thon, og er organisert i fire avdelinger; en juridisk avdeling, en kommunikasjonsavdeling, en administrasjonsavdeling og en tilsyns- og sikkerhetsavdeling. Hver av avdelingene ledes av en avdelingsdirektør. Sammen med direktøren utgjør disse Datatilsynets ledelse.

I 2013 har Datatilsynet hatt 41 faste stillinger. Av disse var 54 prosent kvinner og 46 prosent menn. I løpet av året har tre medarbeidere sluttet i Datatilsynet mot ni i 2012.

	Totalt	Kvinner	Menn
Direktør	1	-	1
Informasjonsavdelingen	4	3	1
Juridisk avdeling	17	9	8
Tilsyns- og sikkerhetsavdelingen	12	3	9
Administrasjonsavdelingen	7	7	-
Totalt	**41**	**22**	**19**

Administrasjon og kompetanse

Det er viktig at Datatilsynets medarbeidere har god kompetanse og spesielt viktig er kompetanse på personvernområdet. Vi erfarer at kompetansen til våre medarbeidere, er etterspurt i både offentlig og privat sektor. Det har derfor vært viktig å satse på kompetansebygging, og legge til rette for at hver enkelt medarbeider får utfordringer og utviklingsmuligheter faglig og i samspill med andre.

I 2013 er mye ressurser benyttet til planlegging og implementering av ny infrastruktur for IKT og oppgradering av arkiv- og saksbehandlersystem. Dette arbeidet vil fortsette også i 2014. Vår målsetting er å ha effektive og gode arbeidsverktøy som er tidsriktige og tilpasset dagens oppgaveløsning. Det er blant annet behov for ekstra ressurssatsing og midler til nødvendige investeringer for digital kommunikasjon. Det er derfor i 2013 fremmet et eget satsningsforslag til budsjettbehandlingen 2014. Forslaget skisserer et behov for generell tilrettelegging for digital

kommunikasjon til og fra etaten, og ivaretakelse av Datatilsynets forpliktelse til å ha en offentlig oversikt over innmeldte behandlinger av personopplysninger. Dette er i dag ivaretatt av et meldesystem som er utrangert, og Datatilsynet ser ikke en investering i en ny dedikert meldeløsning som hensiktsmessig. Dagens meldesystem er ikke et nyttig verktøy, hverken for melder, Datatilsynet eller for de som ønsker å bruke det til å skaffe seg oversikt over hvilke behandlinger av personopplysninger som gjøres.

Datatilsynet har som målsetting å være organisert på en hensiktsmessig måte i forhold til oppgaveløsning og effektivitet. For å ivareta dette, jobbes det strukturert etter en detaljert virksomhetsplan som alle i tilsynet er med på å utforme.

Datatilsynet er omfattet av avtalen om inkluderende arbeidsliv og har spesiell oppmerksomhet på forebygging og oppfølging av sykefravær. Sykefraværet i meldingsåret er tre prosent, mot to prosent i 2012. Det er en økning på en prosent. Det har ikke vært behov for å iverksette spesielle tiltak utover tett oppfølging. Datatilsynet har allikevel valgt å tilby ansatte en helsesjekk hos bedriftshelsetjenesten med fokus på arbeidshelse. 22 medarbeidere fikk dette tilbudet høsten 2013. Samme tilbud gis til de øvrige tilsatte våren 2014.

Vi har som målsetting å hindre at søkere med redusert arbeidsevne blir diskriminert. Målsettingen om mangfold med tanke på etnisk bakgrunn, funksjonsevne, kjønn og alder vektlegges derfor i våre stillingsutlysninger. Vi ønsker også å bidra til å heve den generelle pensjonsalderen. Vi tilbyr blant annet medarbeidere som vurderer pensjon, profesjonell pensjonsrådgivning.

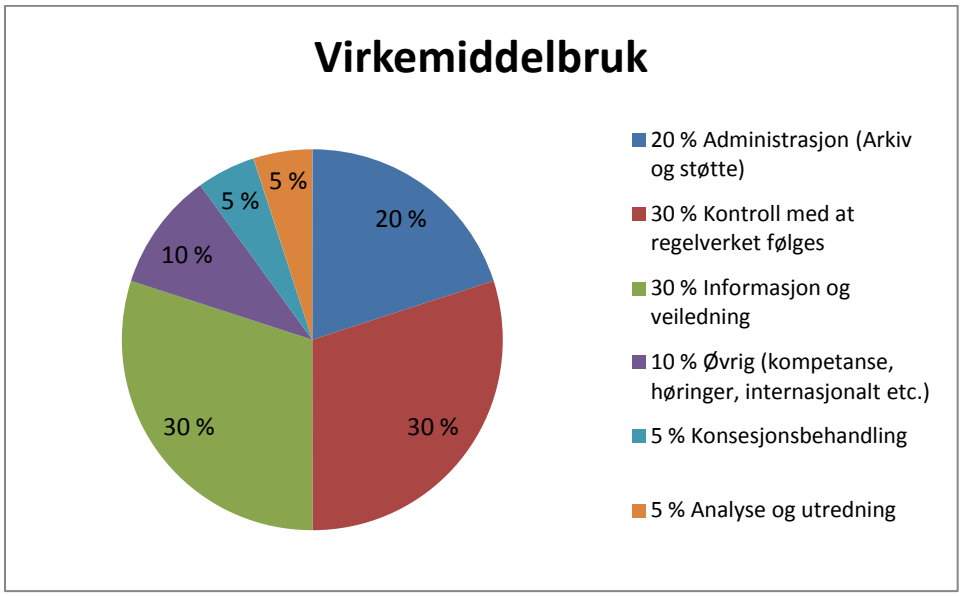
Med utgangspunkt i samfunnskontrakten for 2013-2015, skal statsforvaltningen øke antallet lærlinger. Datatilsynet har i meldingsåret vurdert å ta inn lærlinger, og har ved årsskiftet gitt tilbud om en praksisplass innen IKT.

Virkemiddelbruk

Datatilsynet innhenter kunnskap gjennom tilsyn, saksbehandling, dialog med publikum, dialog med samarbeidende myndigheter nasjonalt og internasjonalt, gjennom veiledningsarbeid, utredningsarbeid, interne og eksterne evalueringer, samt gjennom problemstillinger relatert til personvern og som kommer frem i den offentlige debatten. Fakta og erfaring gir grunnlag for å vurdere virkemiddelbruk, om det er nødvendig å gjennomføre videre tiltak, og i så fall hvilke.

Bruk av virkemidler balanseres og ses i sammenheng. Tilsyn kan være et sentralt virkemiddel innen enkelte sektorer, mens det på andre områder er informasjonsvirksomhet eller deltagelse i samarbeid som fremmer personvernfremmende teknologi, og som vil gi best effekt.

Vi har beregnet at tidsbruken fordeler seg på ulike aktiviteter etter følgende modell (det er tatt utgangspunkt i det totale antall årsverk):


Virkemiddelbruk
20 %
30 %
30 %
10 %
5 %
5 %
20 % Administrasjon (Arkiv og støtte)
30 % Kontroll med at regelverket følges
30 % Informasjon og veiledning
10 % Øvrig (kompetanse, høringer, internasjonalt etc.)
5 % Konsesjonsbehandling
5 % Analyse og utredning

5. Vedlegg

Vedlegg A. Gjennomførte tilsyn

	Saksnummer	Kontroll	Område
1	13/00579	Brevkontroll – e-post 1	Arbeidsliv
2	13/00588	Brevkontroll – e-post 2	Arbeidsliv
3	13/00468	Brevkontroll – e-post 3	Arbeidsliv
4	13/00104	Brevkontroll – e-post 4	Arbeidsliv
5	13/00711	Brevkontroll – e-post 5	Arbeidsliv
6	13/00204	Brevkontroll - Brødbakerne AS avdeling Gjelleråsen – Kameraovervåking	Arbeidsliv
7	13/00775	Brevkontroll – e-post (tipstilsyn kontrolltiltak 1)	Arbeidsliv
8	13/00908	Brevkontroll – e-post (tipstilsyn kontrolltiltak 2)	Arbeidsliv
9	13/01059	Brevkontroll – e-post (tipstilsyn kontrolltiltak 3)	Arbeidsliv
10	13/00210	Kontroll hos Securitas – Rusmiddeltesting	Arbeidsliv
11	13/00213	Kontroll hos Aleris Helse AS – Rusmiddeltesting	Arbeidsliv
12	13/00226	Kontroll hos Sporveien Oslo AS – Tidligere Kollektivtransportproduksjon AS – Rusmiddeltesting	Arbeidsliv
13	13/00392	Kontroll hos Yummy Heaven	Arbeidsliv
14	13/00512	Uanmeldt kontroll hos Ryanair – Kameraovervåking	Arbeidsliv
15	13/01329	Kontroll hos Illums Bolighus Oslo – Kameraovervåking i butikklokaler	Arbeidsliv
16	13/00438	Brevkontroll – forsterket tilsyn med Hjerte og karregisteret	Helse
17	10/00264	Brevkontroll – forsterket tilsyn med Norsk Pasientregister	Helse
18	13/00674	Brevkontroll ved Spesialistsenteret på Straume – Informasjonsplikt	Helse
19	13/00675	Brevkontroll ved Huddoktoren – Informasjonsplikt	Helse
20	13/00676	Brevkontroll ved Oppdal medisinske senter – Informasjonsplikt	Helse
21	13/00677	Brevkontroll ved Martin Schuster – Informasjonsplikt	Helse
22	13/00678	Brevkontroll ved Årdal psykologsenter – Informasjonsplikt	Helse
23	13/00679	Brevkontroll ved Helgelandssykehuset HF – Informasjonsplikt	Helse
24	13/00680	Brevkontroll ved Helse Nord-Trøndelag HF – Informasjonsplikt	Helse
25	13/00681	Brevkontroll ved Helse Fonna – Informasjonsplikt	Helse
26	13/00682	Brevkontroll ved Sykehuset Innlandet HF – Informasjonsplikt	Helse
27	13/00683	Brevkontroll ved Sykehuset Telemark HF – Informasjonsplikt	Helse
28	13/00684	Brevkontroll ved Sinsenklinikken – Informasjonsplikt	Helse
29	13/00685	Brevkontroll ved Stovner legesenter - Informasjonsplikt	Helse
30	13/00686	Brevkontroll ved Ringerike Medisinske Senter – Informasjonsplikt	Helse
31	13/00687	Brevkontroll ved Nytorget legesenter – Informasjonsplikt	Helse
32	13/00688	Brevkontroll ved Fenring Legesenter – Informasjonsplikt	Helse

	Saksnummer	Kontroll	Område
33	13/00748	Brevkontroll med Folkehelseinstituttet – oppfølging av rapport om personvernutfordringer ved genetiske undersøkelser	Helse
34	13/00749	Brevkontroll med Kreftregisteret – oppfølging av Datatilsynets rapport om personvernutfordringer ved genetiske undersøkelser	Helse
35	13/00091	Kontroll hos Universitetet i Nordland – Helseforskning	Helse
36	13/00093	Kontroll hos Universitetssykehuset Nord-Norge HF – Helseforskning	Helse
37	13/01093-1	Formaliserte arbeidsfellesskap – Holtet legesenter	Helse
38	13/01089-1	Formaliserte arbeidsfellesskap–- Byhagen legesenter	Helse
39	13/01092-1	Formaliserte arbeidsfellesskap – Follo legevakt	Helse
40	13/01091-1	Formaliserte arbeidsfellesskap – Øyeblikkelig hjelp	Helse
41	13/01088-1	Formaliserte arbeidsfellesskap –Alta helsesenter	Helse
42	13/01090-1	Kontroll av Drammen geriatriske kompetansesenter – virksomhetsovergripende pasientjournal	Helse
43	13/01268	Kontroll hos Helsedirektoratet – reseptformidlerforskriften § 4-3	Helse
44	13/01309	Kontroll hos Human Etisk forbund	IK IS
45	13/00170	Kontroll hos Ambassaden i Kiev – Utenriksstasjon/ Utenriksdepartementet – Visumsøknadsprosessen – Tilgang til SIS	Justis
46	13/00327	Kontroll hos AS Scan Detect – Privat etterforskningsvirksomhet	Justis
47	13/00328	Kontroll hos Gjensidige Forsikring BA – Privat etterforskningsvirksomhet	Justis
48	13/00329	Kontroll hos Securitas – Privat etterforskningsvirksomhet	Justis
49	13/00330	Kontroll hos Skan-kontroll – Privat etterforskningsvirksomhet	Justis
50	13/00979	Kontroll hos Fylkesnemnda barnevern HedOp	Offentlig
51	13/00977	Kontroll hos Fylkesmannen HedOp	Offentlig
52	13/01156	Kontroll hos Kunnskapsdepartementet	Offentlig
53	13/01157	Kontroll hos BLD	Offentlig
54	13/00200	Kontroll hos Fiskeri- og kystdepartementet – Internkontroll og informasjonssikkerhet	Offentlig
55	13/00201	Kontroll hos Fiskeridirektoratet – Internkontroll og informasjonssikkerhet	Offentlig
56	13/00451	Kontroll hos Vega kommune – Internkontroll og informasjonssikkerhet	Offentlig
57	13/00452	Kontroll hos Brønnøy kommune – Internkontroll og informasjonssikkerhet	Offentlig
58	13/00454	Kontroll hos Sømna kommune – Internkontroll og informasjonssikkerhet	Offentlig
59	13/00455	Kontroll hos Bindal kommune – Internkontroll og informasjonssikkerhet	Offentlig
60	13/00456	Kontroll hos Vevelstad kommune – Internkontroll og informasjonssikkerhet	Offentlig

	Saksnummer	Kontroll	Område
61	13/00457	Kontroll hos Nesna kommune – Internkontroll og informasjonssikkerhet	Offentlig
62	13/00903	Kontroll hos Molde kommune – Internkontroll og informasjonssikkerhet	Offentlig
63	13/00904	Kontroll hos Averøy kommune – Internkontroll og informasjonssikkerhet	Offentlig
64	13/00906	Kontroll hos Kristiansund kommune – Internkontroll og informasjonssikkerhet	Offentlig
65	13/01040	Kontroll stedlig – Volvo (Nordisk kontroll, vi gjennomfører kontrollen, Sverige er invitert til å være med som observatører)	Samferdsel
66	13/00933	Kontroll ved Borgen ungdomsskole – Asker kommune	Skole
67	13/00934	Kontroll ved Bygdøy skole – Oslo kommune	Skole
68	13/00935	Kontroll ved Foss videregående skole i Oslo fylkeskommune – Internkontroll og informasjonssikkerhet	Skole
69	13/00936	Kontroll ved Malakoff videregående skole i Østfold fylkeskommune – Internkontroll og informasjonssikkerhet	Skole
70	13/00937	Kontroll hos Harestad skole i Randaberg kommune – Internkontroll og informasjonssikkerhet	Skole
71	13/00938	Kontroll ved Nordfjordeid skole – Eid kommune	Skole
72	13/00939	Kontroll ved Elverum ungdomsskole – Elverum kommune	Skole
73	13/00940	Kontroll ved Steinerskolen i Oslo	Skole
74	13/00941	Psykososialt arbeidsmiljø 1 – Møhlenpris skole i Bergen kommune	Skole
75	13/00942	Psykososialt arbeidsmiljø 2 – Aronsløkka skole i Drammen kommune	Skole
76	13/00929	Nordisk kontroll med Spotify (Finland gjennomfører og bygger spørsmål. Vi spør norske Spotify.)	Telekom

Vedlegg B. Høringer

	Dok.nr.	Tittel	Avsender/Mottaker
1	13/01203-2	Høringsuttalelse – Retningslinjer for brukergrensesnitt i formelle nettskjema – ELMER 3	Brønnøysundregistrene
2	13/01315-2	Høringsuttalelse - Referansekatalogen 4.1 - Nye anbefalte IT-standarder i offentlig sektor	Direktoratet for forvaltning og IKT
3	13/00982-2	Høringsuttalelse - Endringer i forskrift om Norsk overvåkingssystem for antibiotikaresistens hos mikrober - Etablering av et nasjonalt overvåkningssystem for resistens mot antivirale midler hos virus - RAVN - Ingen merknader	Helse- og omsorgsdepartementet
4	13/00983-2	Høringsuttalelse - Forslag til endringer i opplæringsloven privatskoleloven og folkehøyskoleloven	Kunnskapsdepartementet
5	13/00963-2	Høringsuttalelse - Forslag til endringer i MSIS-forskriften for å overvåke effekt av HPV-vaksine	Helse- og omsorgsdepartementet
6	13/00769-2	Høringsuttalelse - Forslag til ny pasientjournallov og ny helseregisterlov	Helse- og omsorgsdepartementet
7	13/00812-2	Høringsuttalelse - Forslag til endringer i universitets- og høyskoleloven	Kunnskapsdepartementet
8	13/00716-2	Høringsuttalelse - Forskriftsfesting av gjennomgående dokumentasjonsordning for enkelte yrkesfaglige utdanningsprogram	Utdanningsdirektoratet
9	13/00987-2	Høringsuttalelse - NEK 399 tilknytningspunkt for el og ekom - Norsk Elektroteknisk Komite	Norsk Elektroteknisk Komite
10	13/00723-3	Høringsuttalelse - Forslag til forskrift om IKT-standarder i helse- og omsorgssektoren	Helse- og omsorgsdepartementet
11	13/00803-2	Høringsuttalelse - EU-kommisjonens forslag til Entry/Exit System - EES og Registered Traveller Programme - RTP	Justis- og beredskapsdepartementet
12	13/00882-2	Høringsuttalelse - NOU 2013:9 Ett politi - rustet til å møte fremtidens utfordringer	Fornyings-, administrasjons- og kirkedepartementet
13	13/00654-2	Høringsuttalelse - Endringer i eForvaltningsforskriften - Digital kommunikasjon som hovedregel	Fornyings-, administrasjons- og kirkedepartementet
14	13/00715-2	Høringsuttalelse - Forslag til endring i tinglysingsloven - Ingen merknader	Miljøverndepartementet
15	13/00737-2	Høringsuttalelse - Lovfesting av rett til behandling av sensitive personopplysninger i forbindelse med autorisasjonsordning for ansatte i verdipapirforetak - Ingen merknader	Finansdepartementet
16	13/00603-2	Høringsuttalelse - Utredning om fjernvarmereguleringen - Ingen merknader	Olje- og energidepartementet
17	13/00620-2	Høringsuttalelse - Forslag til endringer i trygdeloven og enkelte andre endringer som følge av henvisning fra psykologer - Ingen merknader	Helse- og omsorgsdepartementet
18	13/00587-2	Høringsuttalelse - Forslag til direktiv om bankkontoer - Justis- og beredskapsdepartementet	Justis- og beredskapsdepartementet

	Dok.nr.	Tittel	Avsender/Mottaker
19	13/00776-2	Høringsuttalelse - Forslag til forskriftsendring - krav om lokalpolitisk behandling av kvalitetskrav i helse- og omsorgstjenesten	Helse- og omsorgsdepartementet
20	13/00207-3	Høringsuttalelse - NOU 2013:1 Det livsåpne samfunn	Kulturdepartementet
21	13/00338-2	Høringsuttalelse - Anvendelse av helselovgivningen for Svalbard og Jan Mayen - Ingen merknader	Helse- og omsorgsdepartementet
22	13/00347-2	Høringsuttalelse - Endringer i pasient- brukerrettighetsloven - rett til brukerstyrt personlig assistanse - BPA - Helse-og omsorgsdepartementet - Ingen merknader	Helse- og omsorgsdepartementet
23	13/00746-2	Høringsuttalelse - Endringer i sprøyteromsloven og forskriften for å åpne for inhalering av heroin i sprøyterom - Ingen merknader	Helse- og omsorgsdepartementet
24	13/00657-2	Høringsuttalelse - Forslag til endringer i kommunikasjonskontrollforskriften - Forskrift om kontrollutvalget for tiltak mot hvitvasking og til enkelte deler av politiregisterforskriften	Justis- og beredskapsdepartementet
25	13/00533-2	Høringsuttalelse - Forslag til endringer i førerkortforskriften - Ingen merknader	Fornyings-, administrasjons- og kirkedepartementet
26	13/00630-2	Høringsuttalelse - Om datalagring - forslag til regler om kostnadsfordeling nødrettssituasjoner og taushetsbelagte data	Samferdsels-departementet
27	13/00439-2	Høringsuttalelse - Om gjennomføring av avtale mellom Norge og USA om FACTA og generell innføring av tilsvarende opplysningsplikter	Finansdepartementet
28	13/00490-2	Høringsuttalelse - Gjennomføring av direktiv 2011/62/EU om bekjempelse av forfalskede legemidler - Ingen merknader	Statens legemiddelverk
29	13/00514-2	Høringsuttalelse - Forslag om styrket hjemmel for PST sin søketilgang i utlendingsforvaltningens datasystemer	Justis- og beredskapsdepartementet
30	13/00525-3	Høringsuttalelse - Forskrift om forsøk internettvalg og elektronisk avkryssing i manntallet ved stortingsvalget 2013	Kommunal- og regionaldepartementet
31	13/00174-2	Høringsuttalelse - Endringer i straffeloven 1902 og straffeloven 2005 - personforfølgelse - voldtekt og andre seksuelle overgrep - formidling av prostitusjon - forberedelse til tvangsekteskap - foreldelsesregler mv - Ingen merknader	Justis- og beredskapsdepartementet
32	13/00485-2	Høringsuttalelse - Kjønnsnøytrale premier og ytelser i livsforsikringskontrakter - Ingen merknader	Finansdepartementet
33	13/00363-2	Høringsuttalelse - Ny forskrift til fagskoleloven - Ingen merknader	Kunnskapsdepartementet, Fornyings-, administrasjons- og kirkedepartementet
34	13/00305-2	Høringsuttalelse - Obligatorisk gjennomføring av lærlingeundersøkinga - Forslag til ny regel i forskrift	Utdanningsdirektoratet

	Dok.nr.	Tittel	Avsender/Mottaker
		til opplæringslova § 2-3a	
35	13/00275-4	Høringsuttalelse- Forslag til lov- og forskriftsendringer som følge av a-opplysningsloven	Skattedirektoratet
36	13/00348-2	Høringsuttalelse - Gjennomføring av kommisjonsforordning EU nr. 712/2012 i norsk rett	Helse- og omsorgsdepartementet
37	13/00255-2	Høringsuttalelse - Alkolås som alternativ til tap av førerrett som en del av program mot ruspåvirket kjøring	Justis- og beredskapsdepartementet
38	13/00119-2	Høringsuttalelse - Endring i utlendingsforskriften - tjenesteutsetting av mottak av søknader om oppholdstillatelse	Justis- og beredskapsdepartementet
39	13/00260-2	Høringsuttalelse - Forslag til endringsforskrift til yrkessjåførforskriften - Ingen merknader	Statens vegvesen - Vegdirektoratet
40	13/00277-2	Høringsuttalelse - Forslag til forskrift om prioritet i mobilnettet.	Post- og teletilsynet
41	13/00138-2	Høringsuttalelse - Inntak til videregående opplæring - Utdanningsdirektoratet	Utdanningsdirektoratet
42	13/00375-2	Høringsuttalelse - Endringer i EØS-høringsloven og forskrifter som gjennomfører IMI-forordningen og forordning om europeisk standardisering - Ingen merknader	Nærings- og handelsdepartementet
43	13/00336-2	Høringsuttalelse - Utkast til forskrift om behandling av personopplysninger i kriminalomsorgen	Justis- og beredskapsdepartementet
44	13/00116-2	Høringsuttalelse - Forslag til forskrift om nasjonal kjernejournal	Helse- og omsorgsdepartementet
45	13/00362-2	Høringsuttalelse - Endring i våpenforskriften - Endring angående registrering av løp - Ingen merknader	Justis- og beredskapsdepartementet
46	13/00216-2	Høringsuttalelse - Rapport om Avhør av særlig sårbare personer i straffesaker	Justis- og beredskapsdepartementet
47	13/00284-2	Høringsuttalelse - Endringer i forskrift til introduksjonsloven	Barne-, likestillings- og inkluderings-departementet
48	12/01210-2	Høringsuttalelse - Ny forskrift om internkontroll etter energiloven	Norges vassdrags- og energidirektorat
49	13/00256-2	Høringsuttalelse - Forslag til endringer i utlendingsloven § 108 - Heving av strafferammen ved brudd på innreiseforbudet - Ingen merknader	Justis- og beredskapsdepartementet
50	13/00292-2	Høringsuttalelse - Tvungen etterregistrering av hagler - endring av forskrift - Ingen merknader	Justis- og beredskapsdepartementet
51	13/00072-2	Høringsuttalelse - Hindre for digital verdiskapning - Rapport fra utvalg som har vurdert muligheter og hindringer for digital verdiskapning	Fornyings-, administrasjons- og kirkedepartementet - Statsråden
52	13/00126-2	Høringsuttalelse - Endring i reseptformidlerforskriften	Helse- og omsorgsdepartementet
53	13/00161-2	Høringsuttalelse - Forslag om nye lovbestemmelser for tollkontroll	Finansdepartementet

	Dok.nr.	Tittel	Avsender/Mottaker
54	13/00224-2	Høringsuttalelse - Forslag til endringer i passloven og passforskriften - utvidet adgang for politiet til å benytte opplysninger fra passregisteret	Justis- og beredskapsdepartementet
55	13/00060-2	Høringsuttalelse - Forslag om unntak i advokaters taushetsplikt på skatte- og avgiftsområdet	Finansdepartementet
56	13/00140-2	Høringsuttalelse - Forslag om ratifikasjon av konvensjoner mot terrorhandlinger til sjøs og etablering av bordingsregime - Ingen merknader	Justis- og beredskapsdepartementet
57	13/00208-2	Høringsuttalelse - Forslag til endring i politiloven - Adgang til å pålegge meldeplikt for pengeinnsamling og til å regulere pengeinnsamling på offentlig sted	Justis- og beredskapsdepartementet
58	13/00066-2	Høringsuttalelse - NOU 2013:3 Pensjonslovene og folketrygdreformen III og Finanstilsynets høringsnotat 8. januar 2013 om håndtering av levealderisiko i ny lov om kollektiv tjenestepensjonsforsikring - Ingen merknader	Finansdepartementet
59	13/00177-2	Høringsuttalelse - Forslag til endring av taushetspliktbestemmelsene i finanstilsynsloven sentralbankloven og folketrygdfondloven	Finansdepartementet
60	12/01137-2	Høringsuttalelse - Forslag til endringer i kommuneloven og offentleglova - innbyggerinitiativ - revisors taushetsplikt - utsatt offentlighet - Ingen merknader	Kommunal- og regionaldepartementet
61	13/00134-2	Høringsuttalelse - Arbeidsgrupperapport om forsikringsskjønn - Ingen merknader	Finansdepartementet
62	13/00159-2	Høringsuttalelse - Endringer i forskrift om fastsettelse av tariffer mv for bestemte innretninger - Ingen merknader	Olje- og energidepartementet
63	12/01213-2	Høringsuttalelse - Utvidelse av pasientskadelovens virkeområde til å omfatte barneboliger kommunale rusinstitusjoner og aldershjem - Ingen merknader	Helse- og omsorgsdepartementet
64	13/00031-2	Høringsuttalelse - Nye retningslinjer for registrering i DNA-identitetsregisteret	Riksadvokaten
65	12/01198-2	Høringsuttalelse - Registrering av enkeltpersoners kreditt til bruk ved kredittvurdering	Barne-, likestillings- og inkluderings-departementet
66	12/01204-3	Høringsuttalelse - Endringer i Lov om avleveringsplikt for allment tilgjengelige dokumenter	Kulturdepartementet
67	12/01175-2	Høringsuttalelse om ny prosessordning i sikkerhetssaker etter utlendingsloven - Ingen merknader	Justis- og beredskapsdepartementet
68	12/01181-2	Høringsuttalelse - Nytt regelverk på securityområdet	Luftfartstilsynet
69	12/01097-2	Høringsuttalelse - Regulering av epikriseutsending og utlevering av taushetsbelagte opplysninger i lærings- og kvalitetssikringsøyemed	Helse- og omsorgsdepartementet
70	12/01224-2	Høringsuttalelse - Funksjonelle krav - kravspesifikasjon sikker digital postboks	Direktoratet for forvaltning og IKT
71	12/01046-4	Høringsuttalelse - Forslag til forskrift om universell	Fornyings-,

	Dok.nr.	Tittel	Avsender/Mottaker
		utforming av IKT-løsninger - Ingen merknader	administrasjons- og kirkedepartementet
72	12/01209-2	Høringsuttalelse - Styrking av pasienters brukeres og pårørendes stilling i tilsynssaker mm - Ingen merknader	Helse- og omsorgsdepartementet
73	12/01221-2	Høringsuttalelse - Forslag til endringer i kreftregisterforskriften	Helse- og omsorgsdepartementet
74	12/01211-2	Høringuttalelse - Åpenhet om lønn - lønnsstatistikker og opplysningsplikt - forslag om endringer i diskrimineringslovene	Barne-, likestillings- og inkluderings-departementet
75	12/01155-2	Høringsuttalelse - Om fremlegg til endringer i lov 21 juni 2002 nr. 45 om yrkestransport med motorvogn og fartøy	Samferdsels-departementet
76	12/01073-2	Høringsuttalelse - Forslag til endringer i adopsjonsloven	Barne-, likestillings- og inkluderings-departementet
77	12/01034-2	Høringsuttalelse - NOU 2012:17 - Om kjærlighet og kjøletårn - strafferettslige spørsmål ved alvorlige smittsomme sykdommer - Helse og omsorgsdepartementet - Datatilsynet har ingen merknader	Helse- og omsorgsdepartementet
78	12/01129-2	Høringsuttalelse - Forslag til endring i forskrift om krav til innretning av datasystemer for medlemmer av Bankens sikringsfond - Ingen merknader	Finanstilsynet
79	12/00953-2	Høringsuttalelse - Digital kommunikasjon som hovedregel - Endringer i Forvaltningsloven	Fornyings-, administrasjons- og kirkedepartementet
80	12/00613-3	Høringsuttalelse - Forslag til nye felles bevarings- og kassasjonsbestemmelser for statsforvaltningen	Riksarkivet
81	12/00876-2	Høringsuttalelse - Forslag om å gi adgang til å gi innsyn til bruk for forskningsformål i opplysninger som er omfattet av verdipapirregisterets taushetsplikt	Finansdepartementet

Vedlegg C. Saker oversendt til Personvernnemnda

Klager		Tittel	Dato for oversendelse til nemnda	Dato for vedtak i nemnda	Saksnr. hos nemnda	Resultat
1	Folkehelseinstituttet	Klage på vedtak om pålegg mot Folkehelseinstituttet vedrørende sletting av personopplysninger fra oppdragsvirksomheten	30.01.2013	19.06.2013	PVN-2013-01	Klagen tas ikke til følge
2	Privatperson	Klage på vedtak om omgjøring av vedtak om sletting av personopplysninger i journal ved barneverntjenesten i Tysnes kommune	18.01.2013	16.04.2013	PVN-2013-02	Klagen tas til følge
3	GullAdam	Klage på vedtak om opphør av kameraovervåking av den delen av forretningens lokaler som kun er tilgjengelig for ansatte	06.02.2013	15.10.2013	PVN-2013-03	Klagen tas til følge
4	NTNU/HUNT	Klage på delvis avslag om søknad om forlengelse av konsesjon knyttet til et underprosjekt som bruker data fra HUNT 2 og HUNT 3	14.02.2013	14.05.2013	PVN-2013-04	Klagen tas til følge
5	Diakonhjemmet sykehus AS	Klage på vedtak om pålegg - Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	13.12.2013	PVN-2013-05	Klagen tas ikke til følge
6	Stavanger universitetssykehus	Klage på vedtak om pålegg - Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	20.12.2013	PVN-2013-10	Klagen tas ikke til følge
7	Helse Bergen HF	Klage på vedtak om pålegg – Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	20.12.2013	PVN-2013-09	Klagen tas ikke til følge
8	Haraldsplass Diakonale Sykehus	Klage på vedtak om pålegg - Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	20.12.2013	PVN-2013-08	Klagen tas ikke til følge
9	Oslo universitetssykehus	Klage på vedtak om pålegg - Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	20.12.2013	PVN-2013-11	Klagen tas ikke til følge
10	Curato Røntgen	Klage på vedtak om pålegg - Uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang – GE Healthcare Systems	03.04.2013	20.12.2013	PVN-2013-12	Klagen tas ikke til følge
11	Privatperson	Klage på vedtak om avslutning av sak – Krav om sletting av personopplysninger i barnevernjournal - Eiker kommune	22.05.2013	11.09.2013	PVN-2013-06	Klagen tas ikke til følge

Klager		Tittel	Dato for oversendelse til nemnda	Dato for vedtak i nemnda	Saksnr. hos nemnda	Resultat
12	Helse Bergen HF	Klage på avslag på søknad om endring av konsesjon til å behandle helseopplysninger i Det Norske Nyrebiopsiregisteret	02.07.2013		PVN-2013-07	
13	Privatperson	Klage på avvisningsvedtak	16.08.2013	19.12.2013	PVN-2013-13	Saken sendes tilbake for ny behandling
14	Oslo universitetssykehus – Ullevål	Klage på vedtak om avslag på konsesjonssøknad - Opprettelse av helseregisteret Norwegian Farmers Biobank	29.08.2013		PVN-2013-14	
15	Oslo universitetssykehus – Ullevål – Privatperson	Klage på avslag på kobling av personidentifiserbar informasjon fra Reseptregisteret - Forskningsprosjektet Anti-androgen behandling med eller uten definitiv strålebehandling ved lokalavansert prostatakreft	29.08.2013		PVN-2013-15	
16	Privatperson	Klage på avslutning av sak - Uriktige opplysninger i Folkeregisteret	19.09.2013	20.12.2013	PVN-2013-16	Klagen tas ikke til følge
17	Folkehelseinstituttet	Klage på delvis avslag på forlengelse og utvidelse av Nasjonalt tvillingregister	25.09.2013		PVN-2013-17	
18	Privatperson	Klage på avvisning av sak - Kameraovervåking i sameie	18.10.2013	13.12.2013	PVN-2013-18	Klagen tas ikke til følge
19	SpareBank 1 Markets	Klage på vedtak om lydopptak	22.10.2013		PVN-2013-19	
20	Teletopia Gruppen AS	Klage på vedtak og ileggelse av overtredelsesgebyr	21.10.2013		PVN-2013-20	
21	DNB Bank ASA	Klage på vedtak - kameraovervåking i bank i butikk	06.11.2013		PVN-2013-21	
22	Privatperson	Klage på vedtak om avslutning av sak - Sletting av rettspsykiatrisk erklæring	05.11.2013		PVN-2013-22	
23	Privatperson	Klage på vedtak om avvisning av sak - Kameraovervåking av hytteeiendom i Sauda kommune	20.11.2013		PVN-2013-23	
24	Privatperson	Klage på vedtak om avvisning av sak	06.11.2013		PVN-2013-24	
25	Universitets-sykehuset Nord-Norge	Klage på vedtak om pålegg - Informasjonsplikt i medhold av helseforskningsloven	20.11.2013		PVN-2013-25	
26	Advokat	Klage på vedtak om avvisning av sak - Klage på nettstedet Mittoppdrag.no	13.12.2013		PVN-2013-26	
27	Oslo	Klage på avslag på søknad om konsesjon til nasjonalt	18.12.2013		PVN-2014-	

Klager		Tittel	Dato for oversendelse til nemnda	Dato for vedtak i nemnda	Saksnr. hos nemnda	Resultat
	universitetssykehus	kvalitetsregister for HIV - NORHIV			02	
28	Gjensidige Forsikring ASA	Klage på vedtak etter kontroll hos Gjensidige Forsikring ASA – Privat etterforskningsvirksomhet	18.12.2013		PVN-2013-27	
29	Helse Midt-Norge regionale helseforetak	Klage på avslag på søknad om konsesjon til å opprette Norsk kvalitetsregister for biologiske legemidler – NOKBIL	19.12.2013		PVN-2013-28	
30	AS Skan-kontroll	Klage på vedtak etter kontroll hos AS Skan-kontroll – Privat etterforskningsvirksomhet	20.12.2013		PVN-2014-01	

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: Pb 8177 Dep, 0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

www.datatilsynet.no