ÅRSMELDING FOR 2016

Hva skjer på personvernfeltet, og hvilke utfordringer ser vi fremover?

Datatilsynet

Innhold

LEDERS BERETNING

Ny giv for personvernet – eller to skritt fram og ett tilbake

Datatilsynets årsmeldingen skal oppsummere året som nettopp er over. Her kan man lese om viktige tilsyn, hvor mange som henvender seg til oss, hvor mange mediehenvendelser vi har mottatt og hva som skjer i de viktigste sektorene vi jobber med.

Men det er to temaer som er særlig viktig for personvernet akkurat nå. Det ene er allerede vedtatt, nemlig personvernforordningen som trer i kraft i mai 2018. Det andre er digitalt grenseforsvar, som et utvalg har foreslått å innføre i Norge. Begge disse vil, på ulikt vis, ha stor betydning for norske borgeres personvern i mange år framover.

Det finnes i dag knapt noen grense for hva som kan samles inn av opplysninger om oss, og hva de kan brukes til. Den teknologiske utviklingen går rasende fort, og det er svært krevende for lovgivningen å henge med i svingene. Tross dette, eller kanskje nettopp derfor, er det veldig bra at det kommer et nytt, modernisert personvernregelverk. Kort fortalt er det tre grunnpilarer i det nye regelverket:

- Forhåndskontroll vil i stor grad erstattes av etterkontroll.
- Virksomhetene får en sterkere forpliktelse til å lage rutiner, få på plass avtaler og jobbe systematisk for å følge regelverket.
- Borgernes rettigheter styrkes.

I tillegg får Datatilsynet mulighet til å utstede langt større overtredelsesgebyrer, men minst like viktig er at vi også skal legge vekt på å utvikle bransjenormer og gi rådgivning til virksomhetene, for å nevne noe.

Norske virksomheter har en stor oppgave foran seg før de kan si seg klare til å følge lovens bestemmelser. Vår erfaring er nemlig at det står relativt dårlig til i en del sektorer, og dette inkluderer så absolutt også offentlig sektor. Dette bekreftes gjennom de mange tilsynene vi har gjennomført hos norske kommuner de siste årene. Samtidig opplever vi svært stor interesse fra nær sagt alle om det nye regelverket. Viljen til å etterleve regelverket er stor. Det er evnen, og kjennskap til regelverket, som er utfordringen. Det gjør at vi i Datatilsynet også har en oppgave for oss. Det er selvsagt slik at det er den enkelte virksomhet som skal sørge for å følge reglene. Dette understrekes enda tydeligere i det nye regelverket enn i dagens. Men mange vil være avhengige av god veiledning fra Datatilsynet. Norge har svært mange små og mellomstore bedrifter. Mange bedrifter i oppstartsfasen har nettopp som forretningside å bygge tjenesten på personopplysninger, og det vil utvilsomt være krevende å helt på egen hånd finne ut hvordan man skal følge regelverket.

Dette til tross, vi ser optimistisk på framtida. Det nye regelverket vil få stor betydning for norske borgeres personvern, og heldigvis hører vi stadig flere si at skikkelig behandling av folks personopplysninger er en konkurransefordel. Og i en tid der dette opptar stadig flere kan det omdømmemessig bli kostbart å trå feil.

Forslaget til digitalt grenseforsvar, som ble laget av et utvalg høsten 2016, har derimot motsatt fortegn. I korthet går forslaget ut på at all kabelkommunikasjon som går ut og inn av Norge (i realiteten svært mye av vår daglige kommunikasjon) bli registrert i ulike registre. Lengst lagringstid, på hele 18 måneder, har det såkalte metadataregisteret. Slike metadata avslører hvordan vi lever livet vårt, for eksempel hvor vi er, hvem vi omgås, hva vi kommuniserer om og hvem vi kommuniserer med. Det foreslås filtreringsmekanismer og domstolskontroll, men tross dette vil

mesteparten av dataene som lagres omfatte vanlige folk som ikke utgjør noen trussel mot samfunnet.

Datatilsynet advarer mot å innføre et digitalt grenseforsvar slik det er foreslått av utvalget. I lys av rettsutviklingen i European Court of Justice (EU-domstolen) de siste årene, er det etter vår mening ikke tvil om at forslaget strider med både Den Europeiske Menneskerettighetskonvensjonens (EMK) artikkel 8, og Grunnlovens § 102. Domstolen sier at det må være en sammenheng mellom de dataene som lagres og den konkrete trusselen som tiltaket har til hensikt å avverge. Videre uttaler domstolen at det er et krav at lagringen må være avgrenset med hensyn til tid, sted og ikke minst personkrets. EU-dommen er usedvanlig klar – den stenger helt enkelt døra for generell masselagring av borgernes data. Det digitale grenseforsvaret oppfyller ikke dommens krav til avgrensning, og vil innebære masselagring av informasjon om uskyldige mennesker

Vi advarer også mot formålsutglidning, nemlig at data brukes til nye formål. Utvalget selv advarer også mot dette, og forsøker å forhindre det ved stram lovregulering og forbud mot å bruke dataene som bevis i konkrete straffesaker. De konkluderer faktisk med at deres eget forslag vil være i strid med EMK og Grunnloven dersom formålsutglidning skjer. Både Kripos og Riksadvokaten argumenterte i høringsrunden for nettopp utvidet bruk, blant annet i konkrete saker. Dette sier noe om det presset som her vil komme fra mange hold om å bruke dataene til nye formål, et press som etter vår mening vil være svært krevende å stå imot, og som i realiteten vil føre til at forslaget utgjør et enda mer kvalifisert brudd på de nevnte bestemmelsene.

Vårt råd er derfor klart: Legg bort forslaget til et digitalt grenseforsvar, nedsett et nytt utvalg med bredere sammensetning, blant annet med personvernrepresentanter, og gi det i oppdrag å utarbeide et forslag som ligger godt innenfor EMK og Norges Grunnlov. Slik unngår vi at digitalt grenseforsvar lider samme skjebne som datalagringsdirektivet, som ble kjent ugyldig av EU-domstolen fordi det kunne gi folk en følelses av å være under kontinuerlig overvåking.

Bjørn Erik Thon
Direktør

INTRODUKSJON OG HOVEDTALL

Datatilsynet ble opprettet i 1980 og er et uavhengig forvaltningsorgan under Kommunal- og moderniseringsdepartementet (KMD). Vårt hovedmål er å bidra til at personvernlovgivningen etterleves, og at alle skal ha beskyttelse i tråd med gjeldende personopplysningsregelverk. Vi skal også fremme personvern som en sentral verdi i samfunnet. I dette arbeidet bruker vi ombudsrollen vår ved å ta i bruk ulike formidlingskanaler og ved å delta aktivt i det offentlige ordskiftet om personvern.

Personvern handler enkelt sagt om retten til et privatliv og retten til å bestemme over egne personopplysninger. Personvern er en menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet, men det er også en ideell interesse og er svært viktig for å sikre felles goder i et demokratisk samfunn.

Det vil for eksempel være uheldig dersom enkeltpersoner begrenser sin deltagelse i den åpne meningsutvekslingen og politiske aktiviteten fordi de frykter at opplysninger om personlige forhold vil bli trukket frem og gjort til allmenn oppmerksomhet. Det vil også være uheldig og undergrave demokratiet dersom de setter begrensninger på seg selv fordi de er redde for at myndighetene registrerer og lagrer opplysninger om deres kommunikasjon med andre, om ferdselsmønster, interesser eller uttrykk for holdninger. Datatilsynet må derfor jobbe aktivt for å oppnå en god ivaretagelse av personvernet i avveiingen mot andre samfunnsinteresser.

Hovedaktiviteter

For å realisere hovedmålet om en best mulig beskyttelse av folks personvern har Datatilsynet hatt følgende målsetninger i 2016:

- At virksomheter og borgere kjenner og anvender personvernregelverket.
- At innebygd personvern blir ivaretatt i utviklingen av nytt regelverk og nye tekniske løsninger.
- God kjennskap til rettigheter og plikter i EUs personvernforordning.
- At vi er ombud for personvern nasjonalt og et effektivt talerør for personvern internasjonalt

Vi har i meldingsåret valgt å fokusere særlig på personvern i justissektoren, helse- og velferdssektoren og det omfattende digitaliseringsarbeidet som skjer i offentlig sektor. Vi brukte også mye kapasitet på å følge opp rapporten om kommersiell utnyttelse av personopplysninger.

Virkemidler

For å nå hovedmålet vårt har vi i hovedsak fem ulike virkemidler til disposisjon. Vi prøver til enhver tid å kombinere disse virkemidlene der det er mulig for å oppnå en best mulig effekt.

Saksbehandling som virkemiddel

Gjennom saksbehandling tilegner vi oss erfaring og kunnskap om hvordan personvernhensyn ivaretas i praksis, og vi skal særlig ha oppmerksomheten rettet mot å identifisere systemfeil i virksomheter og bransjer.

Saksbehandling som virkemiddel har særlig vært brukt på områder der vi mottar mange henvendelser og klager. Som offentlig etat er vi naturlig nok bundet av forvaltningsrettslige regler og normer. Det gjøres derfor mye saksbehandling også innenfor områder som ikke er hovedprioritet.

Tilsynsvirksomhet som virkemiddel

Gjennomføringen av tilsyn gir oss et faktabasert grunnlag for kommunikasjon til ulike bransjer og relevante aktører. Tilsyn skal benyttes aktivt for å undersøke og avklare praksis, og til å følge opp konkrete problemstillinger i enkeltsaker. En aktiv tilstedeværelse gir signal om at regelverket skal etterleves og at etterlevelsen blir kontrollert. Tilsynsvirksomheten inkluderer også bruk av kontrollhjemler i saksbehandlingen, som for eksempel når vi følger opp enkeltklager gjennom krav om redegjørelse.

Ved å gjennomføre tilsyn når nye løsninger tas i bruk, men før en praksis har satt seg, kan tilsyn også medvirke til å forme et område videre.

Noen ganger benyttes kontrollene dessuten for å få bedre oversikt over et område eller en sektor, og for å skaffe et bedre grunnlag for å ta i bruk de andre virkemidlene. Andre ganger benyttes de for å holde oppe et trykk på en bestemt sektor – gjerne innenfor et bestemt tema.

Kommunikasjon som virkemiddel

Datatilsynet skal veilede og informere om personvernlovgivning og forvaltningspraksis. Kommunikasjon som virkemiddel benyttes derfor i stor grad for å spre informasjon om personvernets tilstand, samt til å skape debatt og gi uttrykk for synspunkter vi måtte ha som forvaltnings- og tilsynsorgan og i rollen som ombud. Ombudsrollen brukes blant annet ved utspill og kommentarer overfor mediene, foredragsvirksomhet og blogginnlegg.

Kommunikasjon som virkemiddel benyttes stadig mer integrert med de øvrige virkemidlene. En del av kommunikasjonen og dialogen vår skjer derfor gjennom veiledningstjenesten, veiledningsmøter og annen dialog med rammesettere og beslutningstakere.

Organisatoriske, tekniske og økonomiske virkemidler

Deltagelse i ulike råd og utvalg er et godt virkemiddel for å best mulig kunne påvirke aktører til å etablere god praksis. Det samme gjelder deltagelse i arbeid knyttet til personvernfremmende teknologi og regelverksutvikling. Disse virkemidlene egner seg særlig på områder der det pågår større reformer og utviklingsarbeid, særlig dersom de er teknologidrevne. Stortingsmeldingen «Personvern – utsikter og utfordringer», Meld. St. 11 (2012-2013), fastsetter for eksempel et prinsipielt mål om innebygd personvern i alle sektorer. Det har derfor vært viktig å minne beslutningstagere om dette prinsippet i viktige prosesser.

Personvernombudsordningen er også et utpreget organisatorisk virkemiddel.

Når det gjelder overtredelsesgebyr og tvangsmulkt, er dette økonomiske virkemidler som er blitt tatt stadig mer i bruk.

Forsknings-, utviklings- og utredningsarbeid

Gjennom nær kontakt med miljøer i inn og utland som driver med forsknings- og utviklingsarbeid, setter vi oss selv bedre i stand til å sette personvernhensyn inn i en samfunnsmessig kontekst, og til å fange opp trender og utviklingstrekk på et tidlig stadium. Vår kontakt med forskningsmiljøer kan stimulere til forskning på personvern, samtidig som personvernhensyn også blir ivaretatt i annen forskning.

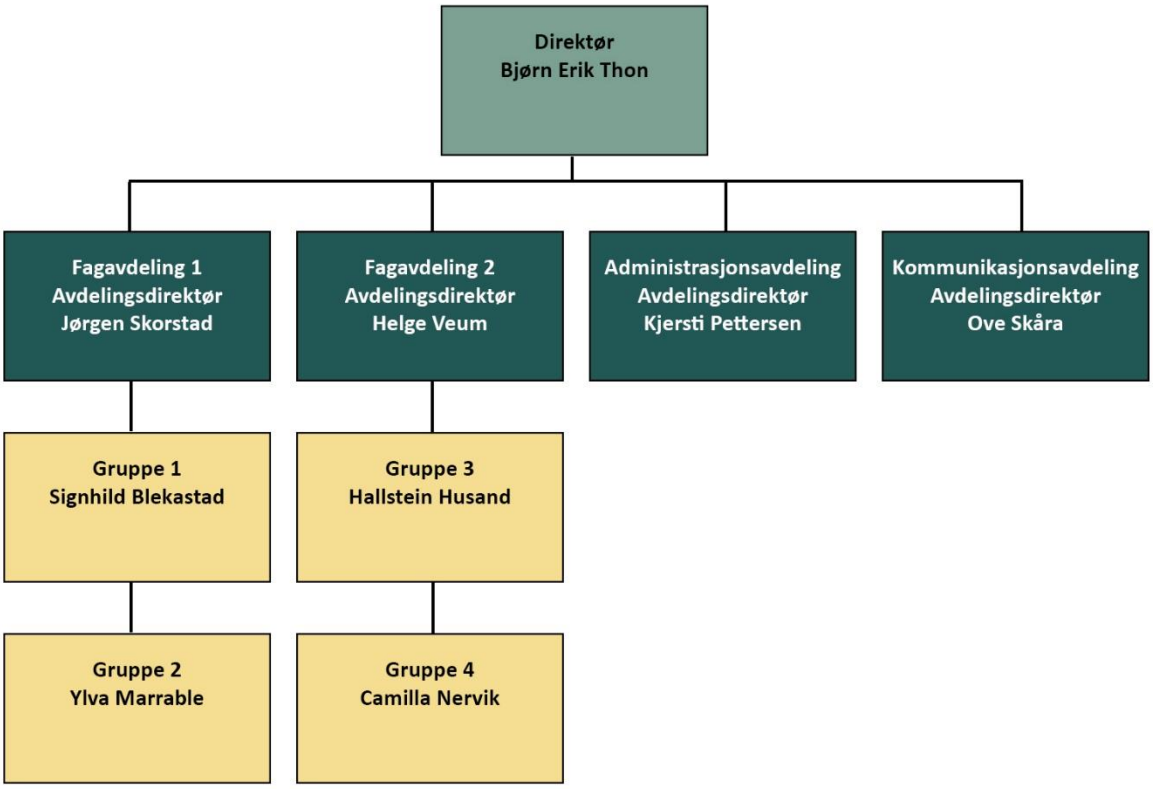
Vårt eget utredningsarbeid og kartlegginger utgjør også en viktig kilde til kunnskap. De gir dybde til ulike temaer vi jobber med og er med på å skape oppmerksomhet om personvernspørsmål. Resultater fra vårt forskning-, utviklings- og utredningsarbeid legges naturlig nok også til grunn ved bruk av de øvrige virkemidlene.

Organisasjon og budsjett

Datatilsynet ledes av direktør Bjørn Erik Thon. Han ble i april 2016 utnevnt som direktør for en ny åremålsperiode. Ledergruppen består av fire menn og en kvinne.

I 2016 har Datatilsynet hatt 47 årsverk til disposisjon (57 prosent kvinner og 43 prosent menn). Av disse årsverkene er 40 faste stillinger. Fem årsverk er engasjementer opprettet for å forberede gjennomføring av nytt personvernregelverk og to årsverk er knyttet til andre oppgaver. I 2016 har vi også hatt to studenter og en lærling tilsatt deler av året.

Organisasjonskart per januar 2017:



Budsjett

Datatilsynets budsjett dekker drift og tilsynets løpende oppgaver. I 2016 ble Datatilsynet tildelt 45 587 000 kroner. Dette var en økning på 5 495 000 kroner fra 2015. Økningen dekker kostnader til arbeidet med å forberede innføringen av nytt personvernregelverk. Når overføringene fra 2015 var gjort og tilleggsbevilgning var lagt til, hadde vi totalt 48 084 000 kroner til disposisjon i 2016. Fordelt på lønn og drift, utgjorde lønnsutgiftene 32 347 000 kroner (70,9 prosent). Driftsutgiftene utgjorde 13 240 000 kroner (29,1 prosent). Lønn per årsverk var i gjennomsnitt 688 000 kroner.

Oversikt over bevilgninger de siste årene:

År	Bevilgning
2013	37 753 000,-
2014	38 264 000,-
2015	40 092 000,-
2016	45 587 000,-

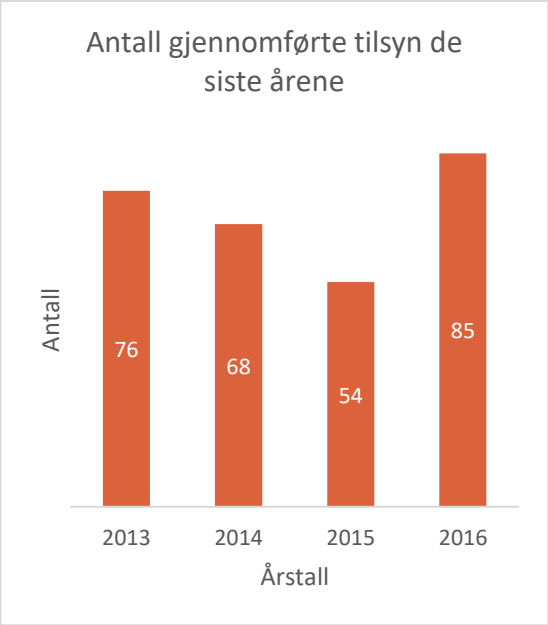
Tilsynsvirksomheten

Gjennomføring av tilsyn/kontroll er viktig for å nå målene våre. Vi skal gjennomføre tilsyn på prioriterte områder basert på risikoanalyse, vi skal systematisere og kommunisere funnene, og vi skal følge opp etterlevelsen av pålegg. Hvilke virksomheter vi faktisk velger å kontrollere, faller normalt i to kategorier; virksomheter hvor vi antar at det er en særskilt risiko, og representative virksomheter hvor vi ønsker å avdekke status innenfor en sektor eller et tematisk område.

I 2016 gjennomførte vi totalt 85 tilsyn (se fullstendig oversikt under *Vedlegg*). De mest sentrale tilsynene er nærmere beskrevet under sine respektive områder i *Årets viktigste aktiviteter*.

Generelle kommentarer

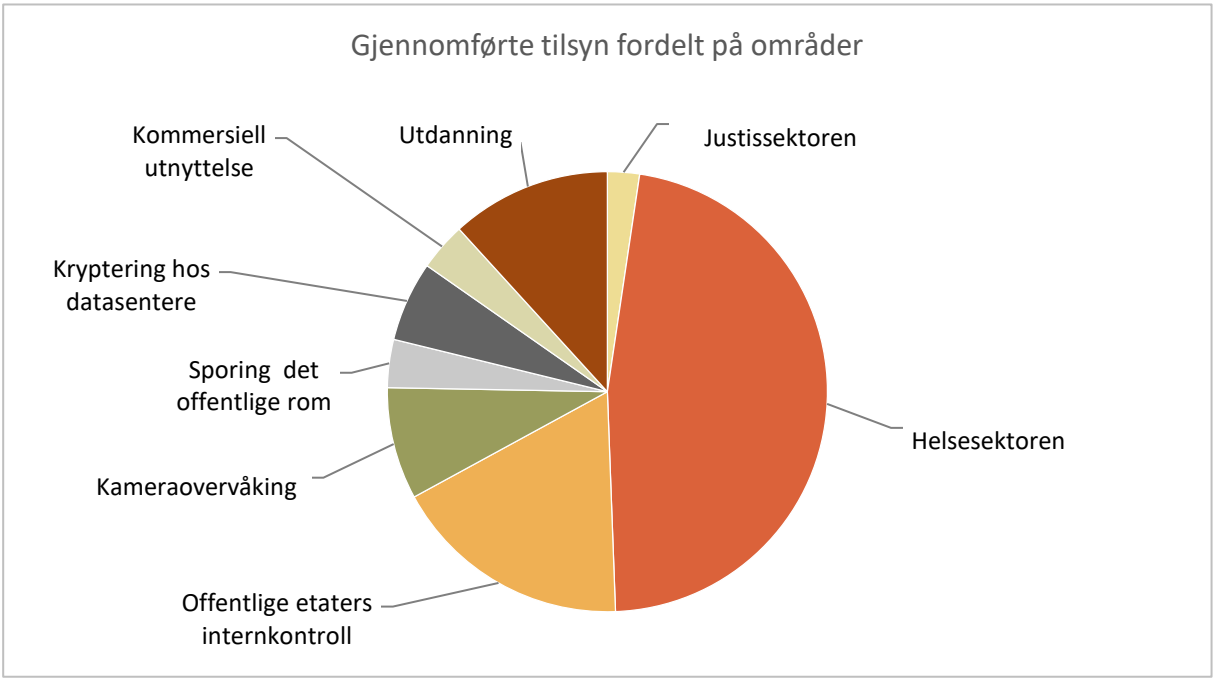
Det vi her regner som tilsyn, er våre kontroller med om regelverket er fulgt, og der det normalt blir utarbeidet en rapport i etterkant. Et tilsyn eller en kontroll blir vanligvis gjennomført ved at to eller tre medarbeidere fra Datatilsynet besøker en virksomhet.



I mange tilfeller gjennomføres planlagte kontroller som en skriftlig prosess, uten at vi er på fysisk besøk hos virksomheten. Dette er i tilfeller der det vi ønsker å undersøke er egnet å få avklart uten et stedlig oppmøte.

I 2016 ble 15 av tilsynene gjennomført hos virksomhetene (stedlig tilsyn), mens 70 ble gjennomført via brev (brevlig tilsyn).

De brevlige tilsynene skiller seg fra bruk av de samme kontrollhjemlene i øvrig saksbehandling ved at de er en planlagt undersøkelse av konkrete forhold i virksomhetene. I 2016 ble brevlige tilsyn særlig vurdert som hensiktsmessig for den oppfølgingen vi hadde innen helsesektoren, kryptering i datasentre, og autentisering i utdanningssektoren.



Oversikt over kontrollene vi gjennomførte i 2016, fordelt på stedlige og brevlige tilsyn:

Bransje/sektor/område	Stedlig	Brevlig	Totalt
Helsesektoren	1	39	**40**
Justissektoren	2	0	**2**
Kameraovervåking	6	1	**7**
Kryptering hos datasentre	0	5	**5**
Offentlige etaters internkontroll	4	11	**15**
Sporing i det offentlige rom	1	2	**3**
Kommersiell utnyttelse	1	2	**3**
Utdanning	0	10	**10**
Sum	**15**	**70**	**85**

Det har blitt gjennomført flere tilsyn i 2016 enn i de foregående årene, og dette er i samsvar med planene våre. Økningen skyldes særlig at vi har gjennomført grupper av brevkontroller, blant annet på helseområdet. Vi fører også kontroll med om regelverket følges gjennom enkeltsaksbehandlingen utover det som fremgår som enkelttilsyn her.

En oppsummert oversikt over områdene vi har gjennomført tilsyn på i 2016:

- Vi gjennomførte et stort antall tilsyn med helsesektoren. Dette innbar rekker av brevkontroller med sentrale helseregistre, kvalitetssikring i helseforetakene, og avtaleregulering mellom virksomheter som har etablert felles pasientjournal.
- Vi har fulgt opp arbeidet med internkontroll og informasjonssikkerhet i kommuner, primært gjennom brevkontroller.
- Innen justissektoren har vi fortsatt kontrollene med politiregistre etter politiregisterloven ved å føre stedlig tilsyn med Politiets utlendingsregister, samt at vi har gjennomført et tilsyn med Kripos etter loven om Schengen informasjonssystem (SIS-loven).

- Innen utdanning har vi gjennomført tematiske brevkontroller med informasjonssikkerheten ved pålogging til skolenes fagsystemer.
- Vi har gjennomført kontroller på to områder som må ses i sammenheng med vårt utredningsarbeid:
    - Det ene gjaldt sporing i det offentlige rom. Dette kom som følge av en rapport vi skrev i 2016 der vi så på de tekniske mulighetene og de rettslige kravene når det tas i bruk sporingsteknologi på for eksempel kjøpesentre.
    - Det andre området var en del av vår prioriterte satsning på kommersialisering av personopplysninger og hvor vi så på behandling av personopplysninger i fordelsprogram og ved annonsering på nett.
- I 2015 gjorde vi tilsyn med kryptering av kommunikasjonen hos store datasentre, og i 2016 fulgte vi opp dette med ytterligere fem tilsyn med samme tema.

Funn fra tilsyn - avvik

Funn som blir gjort under tilsyn, kategoriseres som avvik. Det vil si at vi har vurdert praksisen hos den kontrollerte virksomheten til å være et avvik fra krav i regelverket. Hvilke avvik vi finner avhenger naturligvis av hva som ble kontrollert, noe som varierer med tema for kontrollen.

Spesielle funn fra enkelttilsyn er som nevnt omtalt under *Årets viktigste aktiviteter*. Vi vil likevel fremheve at vi fremdeles ser vesentlige avvik i offentlig sektor knyttet til internkontroll, informasjonssikkerhet og etablering av databehandleravtaler. Kontrollene av kommuner viser imidlertid noe bedring.

Kommunikasjon av funn

Funn fra våre tilsyn blir samlet og systematisert i kontrollrapporter. Foreløpige rapporter blir først sendt til tilsynsobjektet, tilbakemeldinger blir vurdert og så utformes det til slutt en endelig rapport.

De fleste rapportene publiseres på datatilsynet.no slik at andre aktører i tilsvarende bransje kan lese om funn og hva vi er opptatt av. Videre stadfester rapportene vår forvaltningspraksis innen de aktuelle feltene.

Rapportene gjøres også tilgjengelig via Offentlig elektronisk postjournal (OEP) og får derfor ofte også medieomtale, både i lokale, regionale og nasjonale medier.

Utover dette brukes funnene i dialog med bransjeforeninger, sektormyndigheter og andre sentrale aktører som tar utfordringene videre. Funn fra tilsyn presenteres også på relevante foredrag.

Noen gjennomførte og planlagte aktiviteter for å følge opp tilsynene som ble gjennomført i 2016:

- Kontroller med kommuner gjennom flere år har vært et viktig faktagrunnlag i dialogen med sektoren, særlig med Kommunenes arbeidsgiver-, interesse- og medlemsorganisasjon (KS) og organisasjonen Kommunal informasjonssikkerhet (KINS) om hvordan det kan legges bedre til rette for kommuners regelverksetterlevelse.
- Etter tilsyn med kameraovervåking i regi av lokalt politi har det vært kontakt med Politidirektoratet for å koordinere rammene og omfanget av slik overvåking.
- I forbindelse med kontroll av kryptering av datasentertrafikk i 2015 og 2016, er vår veiledning på området oppdatert i samråd med Nasjonal sikkerhetsmyndighet (NSM), og våre beslutninger vil gjøres kjent for sektoren i den grad det ikke eksponerer sårbarheter hos de kontrollerte virksomhetene.
- Funn og avgjørelser etter tilsynene med virksomheter som driver med samfunnsforskning, blir kommunisert tilbake til sektoren.

- Funn og avgjørelser etter tilsyn med helsevirksomheters avtaler om samarbeid vil bli brukt aktivt i dialogen med sektoren om veiledning og mulige forskrifter.
- Funn fra tilsyn med fordelsprogram er en del av informasjonsgrunnlaget vårt i arbeidet med kommersialisering av personopplysninger.
- Informasjon til utdanningssektoren om krav om sterk autentisering og synliggjøring av at dette blir håndhevet.

Etterkontroller

Ett av tilsynene vi gjennomførte i 2016 var en etterkontroll med gjennomføring av pålegg fattet i en sak om avvik i en kommune. Videre legger vi fremdeles negative svar om etterlevelse av internkontrollplikten fra kommuneundersøkelsen vår i 2010 og 2011 til grunn ved utvelgelsen av tilsynsobjekter i kommunesektoren. Tilsyn med Kripos om Schengen informasjonssystem etter SIS-loven gjennomføres regelmessig, og inkluderer slik sett en etterkontroll. I kontrollene med sentrale helseregistre er et av temaene kryptering av identitet som har vært kontrollert tidligere.

Saksbehandlingen

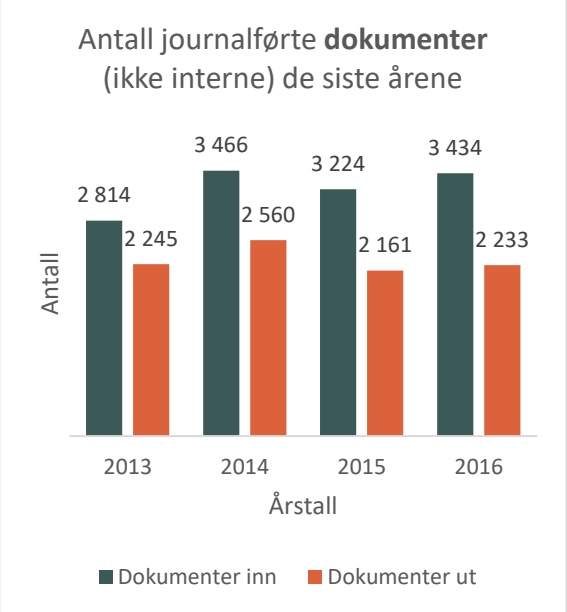
Saksbehandling er en av Datatilsynets viktigste oppgaver. Publikum har ofte en forventning om at vi skal behandle alle sakene vi mottar i sin fulle bredde, men mange av henvendelsene som kommer inn blir tatt hånd om i veiledningssporet.

I 2016 har vi fortsatt arbeidet med å effektivisere saksbehandlingen vår. Vi har særlig sett på hvilke muligheter vi har for å prioritere saker opp mot hverandre, og for øvrig på hvordan vi jobber med de ulike sakene. Prioriteringskriteriene våre er revidert. Dessuten har vi gjennomført et tverrfaglig prosjekt om effektivisering av arbeidsmetodikken vår.

På slutten av året kom det nye regler i personopplysningsforskriften som reduserer omfanget av konsesjonspliktige og meldepliktige databehandlinger. Dette gjelder blant annet for kameraovervåking, varsling i arbeidslivet og adgangskontrollsystemer, i tillegg til bruk av «flåtestyring» og elektronisk kjørebok. Disse regelverksendringene er resultatet av et initiativ fra oss, og de bidrar til å redusere antallet saker som vi må behandle.

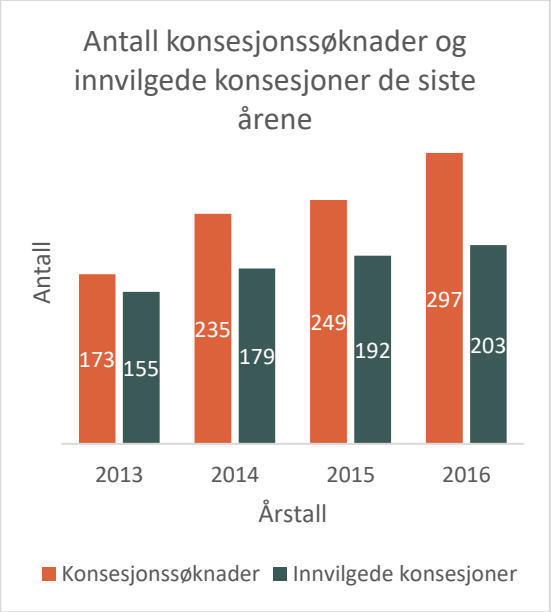
Antall saker og saksdokumenter

I løpet av 2016 er det registrert 1 745 nye saker i vårt elektroniske saksbehandlingssystem. Gjennomsnittstallet for de siste fem årene er på omtrent 1350 nye saker i året. Vi opplevde altså en



betydelig oppgang i antallet sakshenvendelser i 2016.

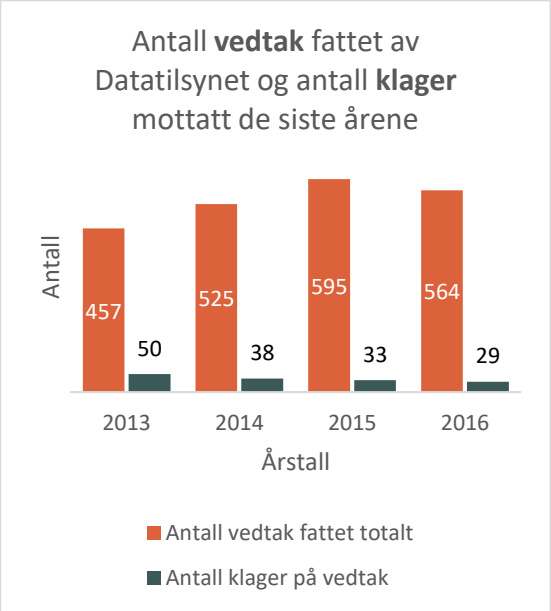
Noe av økningen i 2016 kan trolig forklares med at det kom inn langt flere saker enn tidligere om overføring av personopplysninger til USA. Dette har trolig sammenheng med at Safe Harbor-ordningen ble kjent ugyldig av EU-domstolen i oktober 2015, noe som førte til at det kanskje viktigste rettslige grunnlaget for å overføre personopplysninger til USA falt bort. I stedet ble det nødvendig å forhåndsvarsle Datatilsynet om, eller søke om Datatilsynets forhåndsgodkjenning av, denne typen dataoverføringer.



Antallet innkomne **dokumenter** i løpet av året er 3 434. Dette er på linje med de siste årene.

Konsesjoner

En av Datatilsynets lovpålagte oppgaver er å behandle og ta stilling til konsesjonssøknader. I 2016 har vi til sammen behandlet 297 konsesjonssaker. 203 søknader er innvilget og 90 av sakene gjelder endringsvedtak. Kun fire søknader er avslått.



De fleste konsesjonssøknadene gjelder forskning eller opprettelse av registre i helsesektoren. Vi ser også et økende antall saker som gjelder tillatelser til utstrakt behandling av personopplysninger for å kunne tilby personaliserte tjenester, særlig i forsikringsbransjen.

Arbeidet med konsesjoner er blant de mest tidkrevende oppgavene vi har. Behandling av konsesjonssøknader er en forhåndskontroll av om søkerens planlagte databehandlinger oppfyller regelverkets krav. Det er ofte nødvendig med kontakt mellom søker og Datatilsynet for å få avklart diverse spørsmål i løpet av denne godkjennelsesprosessen. Aktuelle spørsmål kan gjelde det rettslige grunnlaget for databehandlingen, internkontroll, eller tiltak for å redusere personvernulempene. Disse sakene er derfor ofte svært tidkrevende.

Vedtak, overtredelsesgebyr og klagesaker

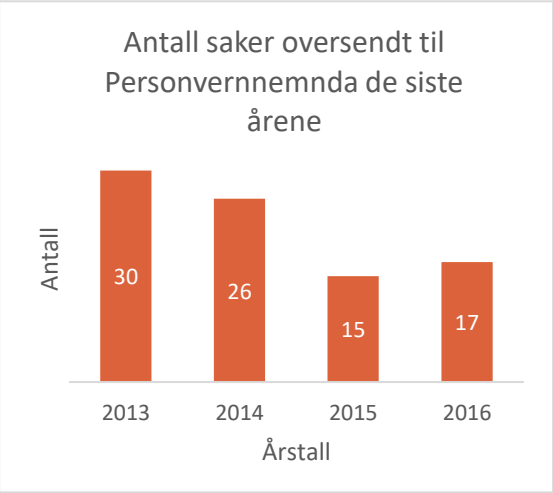
Vi fattet 564 forvaltningsvedtak i 2016. Dette er en liten nedgang sammenlignet med 2015. Antall fattede vedtak i 2016 ligger likevel over snittet for de siste fem årene. Vi mottok bare 29 klager i løpet av året, noe som viser en svak nedgang i antall klager gjennom de siste årene.

I løpet av 2016 ble 17 klagesaker oversendt til Personvernnemnda for endelig klagebehandling der. Samtidig har vi mottatt nemndas vedtak i 26 saker. Kun i fire av sakene har klager fått fullt medhold i sin klage.

Se fullstendig oversikt over antall saker som ble oversendt til Personvernnemda under *Vedlegg.*

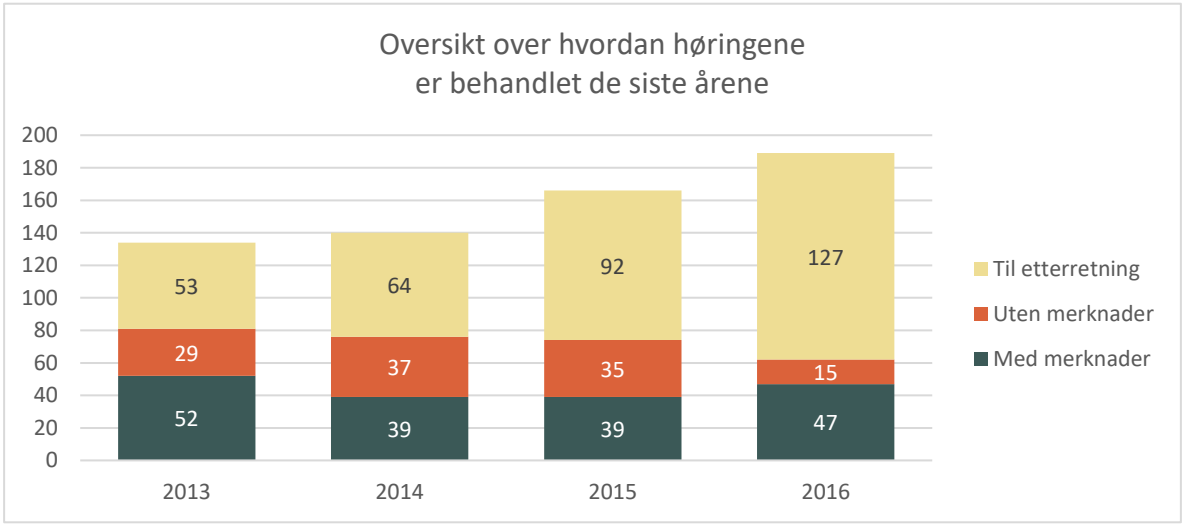
I 2016 fattet vi 22 vedtak om overtredelsesgebyr. Sakene gjelder blant annet ulovlig innsyn i arbeidstakers epostkasse, ulovlig publisering av følsom personinformasjon på internett, ulovlig kameraovervåking og kredittvurderinger som er gjennomført uten at det har vært et saklig behov for det. Det laveste gebyret var på 25 000 kroner, mens det høyeste var på 500 000 kroner.

Se fullstendig oversikt over overtredelsesgebyr under *Vedlegg*.



Høringer

I 2016 mottok vi 189 saker på høring. I samme periode har vi avgitt 47 høringsuttalelser med merknader. Dette er omtrent som normalt. Departementene som mottar flest uttalelser fra oss er Justis- og beredskapsdepartementet og Helse- og omsorgsdepartementet. De mest sentrale høringssakene er omtalt i de ulike kapitlene under *Årets viktigste aktiviteter*.

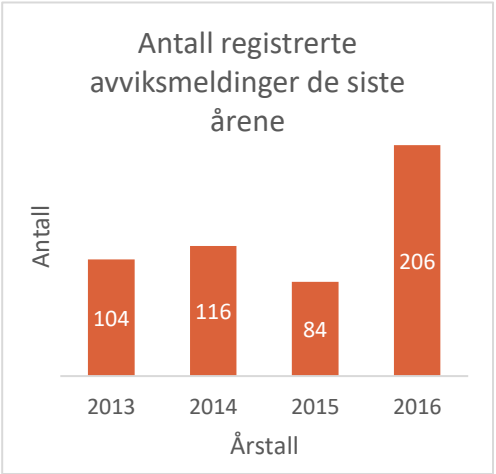


Se fullstendig liste over høringene under *Vedlegg.*

Avviksmeldinger

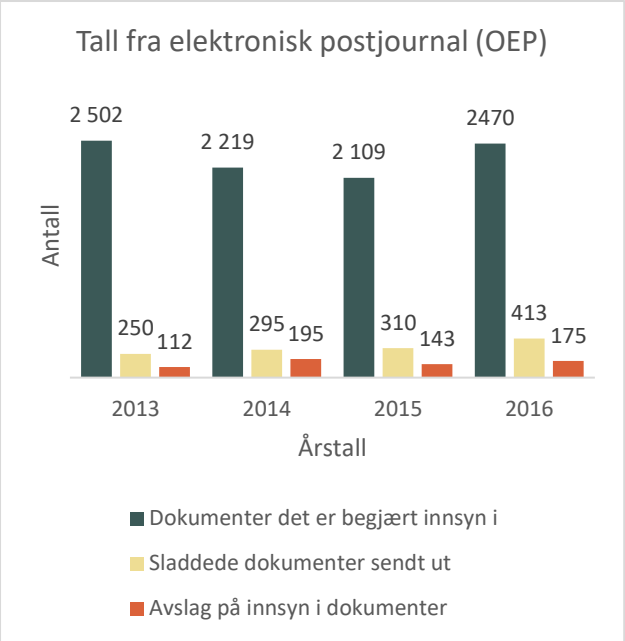
Hendelser som har medført uautorisert utlevering av personopplysninger der konfidensialitet er nødvendig, skal rapporteres til Datatilsynet.

I 2016 mottok vi 206 slike avviksmeldinger. Dette er en markant økning sammenlignet med tidligere år. De fleste meldingene kommer fra bank- og forsikrings-bransjen, i tillegg til fra offentlig sektor, inkludert helsesektoren. Rapporterte avvik er en indikator på hvor godt virksomhetene fanger opp avvik, og hvor godt de kjenner til den forskriftsfestede rapporteringsplikten.



Offentlighetsloven og innsynskrav

I 2016 håndterte Datatilsynet innsynskrav om til sammen 2 470 dokumenter via elektronisk postjournal (OEP), noe som innebærer en økning sammenlignet med året før.



Vi har interne rutiner som sørger for fordeling mellom dokumenter som sendes ut direkte fra arkivet og dokumenter som vurderes av saksbehandler. Når et dokument er vurdert én gang gjenbrukes denne beslutningen dersom opplysningene bes utlevert på nytt. Vi sender naturlig nok ut en del dokumenter hvor bare deler av opplysningene er offentlige.

Vi er svært bevisste på å etterleve offentlighetlovens regler om meroffentlighet. Vi ser en betydelig økning i antallet sladdede dokumenter som vi har sendt ut. Det mener vi er en naturlig utvikling ettersom kompleksiteten i sakene øker og mengden av beskyttelsesverdig informasjon som vi mottar er økende. En stor del av informasjonen som unntas, er av informasjonssikkerhetsmessig karakter, og er beskyttet av bestemmelsen om taushetsplikt i personopplysningsloven § 45.

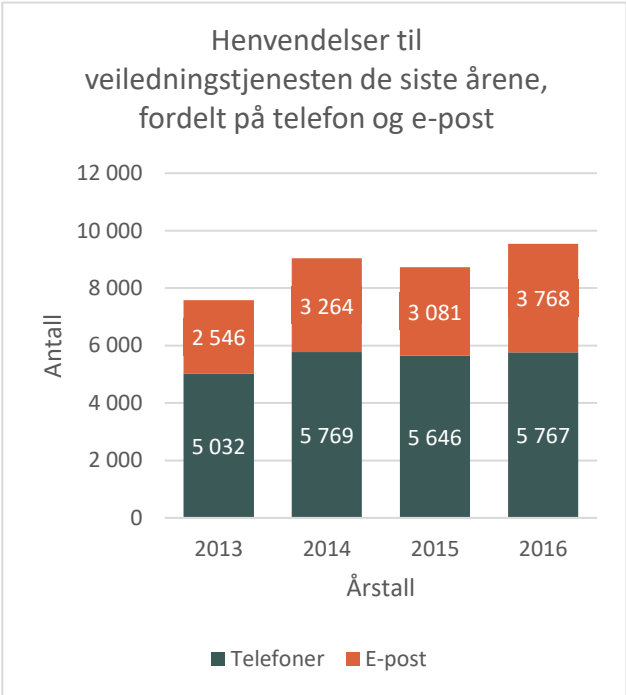
Vi legger ned betydelige ressurser i utførelsen av de oppgavene som offentlighetsloven pålegger oss å utføre.

Veiledningstjenesten

Datatilsynets veiledningstjeneste er et lavterskeltilbud for publikum som har spørsmål om behandling av personopplysninger. Et viktig mål med tjenesten er å gjøre enkeltpersoner i stand til å ivareta egne interesser i saker som gjelder personvern, og bistå virksomheter i å følge pliktene i personvernlovgivningen.

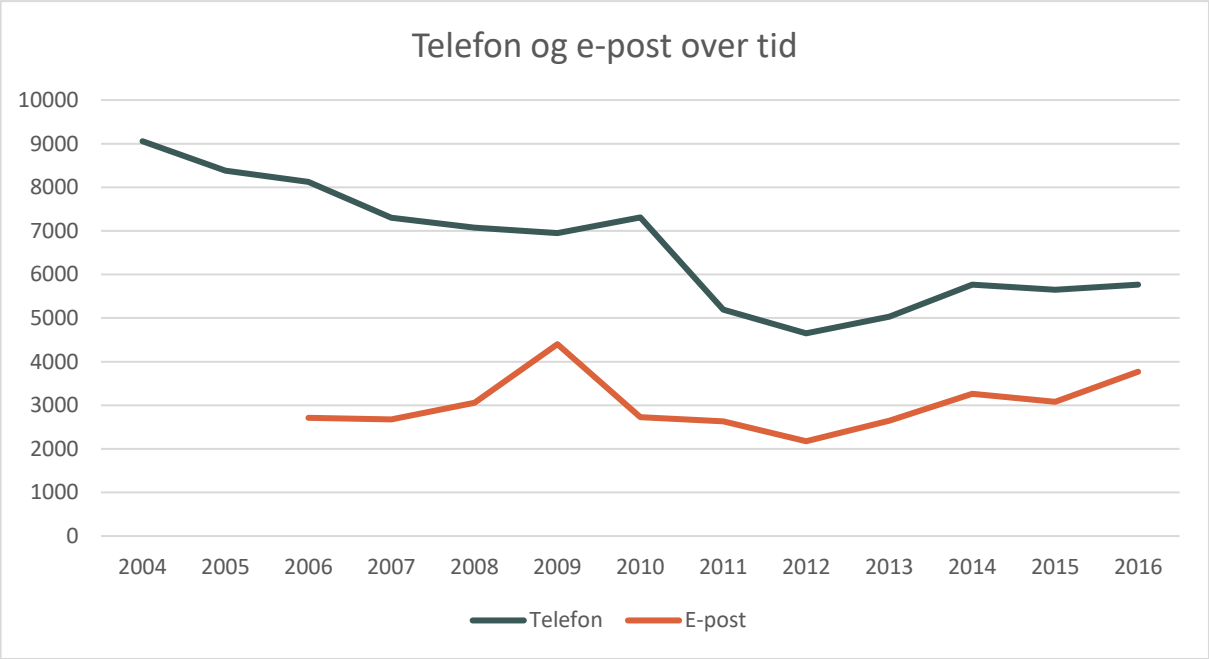
Det er stort spenn i spørsmålene, og de er av både juridisk, teknisk og sikkerhetsmessig art. Svarene vi gir er av veiledende karakter og er ikke bestemmende for rettigheter eller plikter, i motsetning til vedtak som fattes i den mer tradisjonelle saksbehandling.

I løpet av 2016 har veiledningstjenesten besvart 9 535 henvendelser. Dette består av 3 768 henvendelser på e-post og 5 757 per telefon. Sammenlignet med 2015

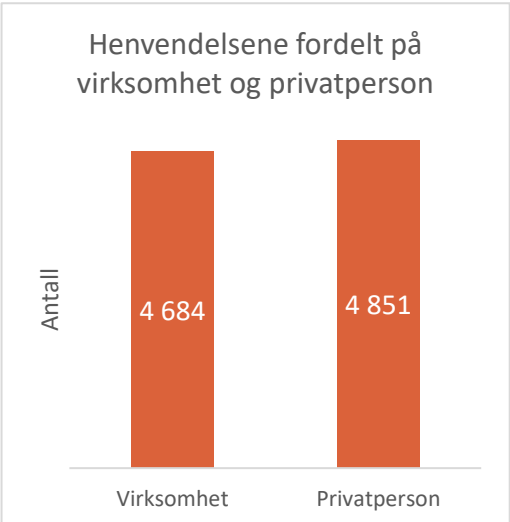


representerer dette en oppgang på 808 henvendelser. Det er e-posthenvendelser som står for størstedelen av økningen.

Det har de siste ti årene i snitt vært en jevn nedgang i antall telefonhenvendelser. Forklaringen kan være stadig mer oversiktlige og utfyllende nettsider, men en redusert telefontid kan nok også forklare noe av nedgangen i telefonhenvendelser og økningen i antall e-posthenvendelser.



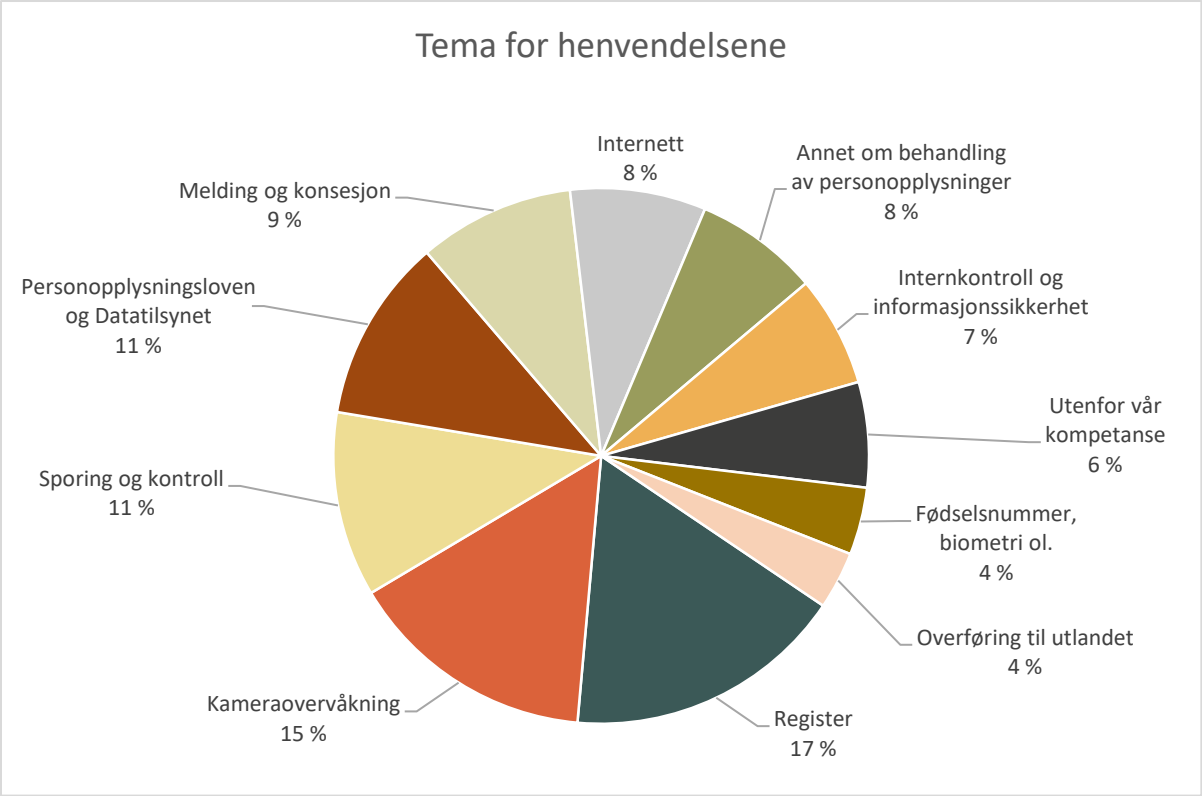
I 2016 har det blitt endret noe på måten henvendelsene til veiledningstjenesten registreres på for å få en bedre oversikt over hva slags type henvendelser vi mottar. En endring i forhold til i fjor, er at vi registrerer om spørsmålet kommer fra en virksomhet eller privatperson. Oversikten viser at fordelingen mellom spørsmål fra virksomheter og privatpersoner er nesten lik.



I tillegg registreres det både hvilken sektor henvendelsen hører under og hva som er tema for henvendelsen. Tidligere er det ikke blitt skilt mellom sektor og tema. Den nye kategoriseringen gjør det derfor noe vanskelig å sammenligne statistikken med tidligere år. Vi kan likevel si noe om prosentfordelingen for de fleste temaene sammenlignet med fjoråret.

Hva handler henvendelsene om?

Her følger en kort oppsummering av de mest sentrale kategoriene. Merk at tallene ikke vil være fullstendig dekkende, da flere av temaene vi får spørsmål om vil kunne plasseres i ulike kategorier.



Register

17 prosent av henvendelsene til veiledningstjenesten var ulike spørsmål knyttet til en eller annen form for register. Dette representerer en liten økning fra 14 prosent i 2015. Spørsmålene dreier seg om hva som kan registreres i ulike registre, når og hvordan man kan kreve å få slettet informasjon og hvem som har tilgang til opplysningene i registrene. Videre får tjenesten en del spørsmål om i hvilken grad det kan utleveres informasjon fra et register til en tredjepart.

Det er flest henvendelser knyttet til kunde- og medlemsregistre, men det er også mange spørsmål knyttet til personalregistre, journalopplysninger og registrering i forbindelse med kredittopplysningsvirksomhet.

Kameraovervåking

Kameraovervåking er en annen stor kategori som utgjorde 15 prosent av henvendelsene. Denne kategorien er nokså stabil sammenlignet med 2015 da kategorien utgjorde tolv prosent.

De fleste henvendelsene gjelder spørsmål om ulike virksomheter har anledning til å iverksette kameraovervåking. Det er mange arbeidstakere som tar kontakt fordi de føler seg urettmessig overvåket. Kameraovervåking i borettslag og i nabosituasjoner er også henvendelser som går igjen. Andre vanlige spørsmål er bruk av webkamera, samt spørsmål om lovligheten av kameraer i for eksempel naturen, i båthavner eller andre offentlige områder.

Internett

Ulike henvendelser om internett sto for åtte prosent av henvendelsene. Dette er samme nivå som i 2015 da det utgjorde sju prosent. Mange av spørsmålene handler om sletting av uønsket informasjon. Dette gjelder både bilder og tekst på ulike plattformer som sosiale medier, blogger og så videre. En god del gjelder retten til å bli glemt, som følge av den såkalte Google-dommen. Denne

dommen gir den registrerte mulighet til å få slettet søketreff med informasjon som er feil, irrelevant eller ikke lengre aktuell.

Tjenesten mottar en god del spørsmål om regler for bruk av sosiale medier, og spørsmål om publisering av bilder på nett går også igjen. Veiledningstjenesten får ellers en del spørsmål om kontroll, sporing og sikkerhet på internett. Mange er bekymret for om deres personopplysninger er trygge på internett og de er redde for identitetstyveri.

Sporing og kontroll

Denne kategorien utgjør elleve prosent av henvendelsene og består hovedsakelig av spørsmål knyttet til kontroll og sporing i arbeidslivet. Dette er et nytt tema og lar seg derfor ikke sammenligne med 2015. En tredjedel av disse henvendelsene gjelder arbeidsgivers innsyn og tilgang til arbeidstakers epostkasse, hjemmeområde og telefon. Et annet stort tema er problemstillinger som gjelder GPS og annen sensorteknologi. Tilgangskontroll og lydopptak går også igjen.

Melding og konsesjon

Ti prosent av henvendelsene gjaldt spørsmål om melding og konsesjon. I fjor sto denne kategorien for ni prosent av henvendelsen. Over halvparten av disse er henvendelser om hvorvidt en behandling er melde- eller konsesjonspliktig. En del av spørsmålene handlet også om endring og oppfølging av melding og konsesjon, og hvordan melding og konsesjon skal leveres.

Internkontroll og informasjonssikkerhet

Spørsmål knyttet til informasjonssikkerhet og internkontroll utgjorde syv prosent av henvendelsene. Det er stor variasjon i disse spørsmålene. Bruk av skytjenester er et gjentagende tema. I tillegg er det mye som handler om sikker lagring, tilgangsstyring og overføring av personopplysninger. Kategorien utgjorde i 2015 også syv prosent av henvendelsene.

Fødselsnummer og biometri o.l.

I likhet med fjor utgjorde denne lille kategorien fire prosent av henvendelsene. Spørsmålene i denne kategorien handler i stor grad om privatpersoner som reagerer på at de i ulike sammenhenger må oppgi fødselsnummer, eller at de melder om at deres fødselsnummer er kommet på avveier. Det er også noen spørsmål fra virksomheter om hvorvidt de har lov til å benytte seg av fødselsnummer. Et fåtall av henvendelsen dreier seg om lovligheten av å bruke fingeravtrykk.

Overføring til utlandet

Kun fire prosent av spørsmålene gjelder overføring av personopplysninger til utlandet. Det er vanskelig å sammenligne med 2015, da dette ikke var et eget tema. Det er imidlertid grunn til å anta at antall henvendelser er nokså stabil sammenlignet med 2015. De fleste spørsmålene kommer fra virksomheter som ønsker råd for hvordan de skal gjennomføre en lovlig og sikker overføring av personopplysninger.

Utenfor vår kompetanse

Seks prosent av henvendelsene knytter seg til spørsmål som faller utenfor Datatilsynets kompetanse. Dette er spørsmål som er regulert av andre lover, slik som spørsmål knyttet til offentlighetsloven eller om brudd på taushetsplikt etter forvaltningsloven. Dette ble ikke kategorisert i 2015.

Annet om behandlinger av personopplysninger

Denne kategorien sto for av åtte prosent av henvendelsene, og består av små temaer som spørsmål om id-tyveri, personvernombud, avvikssaker og spørsmål knyttet til bruk av personopplysninger til journalistiske, kunstneriske eller litterære formål.

En del av henvendelsene som kommer til veiledningstjenesten har tema går på tvers av sektorer og kategorier:

Spørsmål knyttet til arbeidsliv

Spørsmål knyttet til personvern i arbeidslivet har tradisjonelt sett utgjort en stor andel av henvendelsene til veiledningstjenesten. Det sjekkes derfor alltid om henvendelsen gjelder personvern i arbeidslivet. Hele 21 prosent av henvendelsene til veiledningstjenesten faller inn under denne kategorien. Dette er nøyaktig samme prosentandel som ble registrert i 2015, og andelen har holdt seg jevn i flere år. Mange av spørsmålene handler om kontroll og overvåking av ansatte. Det er spørsmål om kameraovervåking på arbeidsplassen, innsyn og sletting av ansattes e-post, samt adgangskontroll og logging av arbeidsinnsats. Vi får også spørsmål om bruk av GPS-sporing og annen sporing av ansatte.

Spørsmål om personvernforordningen

EUs nye personvernforordningen trer i kraft i mai 2018. Vi har derfor valgt å registrere hvor mange av henvendelsene vi får som gjelder spørsmål knyttet til den kommende forordningen. I 2016 dreide kun en prosent av spørsmålene seg om dette. Det blir interessant å se om dette tar seg opp i løpet av 2017.

Brukerevaluering

Høsten 2016 gjennomførte vi en brukerundersøkelse om hvordan brukerne opplever veiledningstjenesten. Personer som fikk svar fra oss på e-post ble bedt om å gjennomføre en undersøkelse for å kartlegge tilfredsheten med svaret de fikk. Resultatene var meget gode. Vi hadde 158 respondenter, hvorav 70 prosent svarte at de i stor grad fikk svar på det de lurte på. Kun tre prosent svarte at de ikke fikk svar på det de lurte på. På bakgrunn av denne kartleggingen har vi vurdert tiltak som kan forbedre tjenesten ytterligere.

Kommunikasjonsvirksomheten

Personvernlovgivningen legger i stor grad ansvaret på den enkelte når det gjelder å ivareta eget personvern. Samtidig har virksomheter som behandler personopplysninger plikt til å etterleve lovgivningen på området. Dette gjelder både offentlige etater, private organisasjoner og næringsdrivende. Fordi privatpersoner, offentlige aktører og private virksomheter har så forskjellige behov, stiller dette store krav til hvordan vi legger opp kommunikasjonsvirksomheten i Datatilsynet.

Vi har som strategisk satsing at vi skal bidra til økt kunnskap om og interesse for personvern. Vi skal også jobbe for at andre aktører tar personvernhensyn. Vi skal sette borgeren i stand til å ta vare på sitt eget personvern, og vi skal ha stor synlighet i personverndebatten.

Kommunikasjonsarbeidet i Datatilsynet skal være basert på statens kommunikasjonspolitikk og gjeldende regelverk, slik som offentlighetsloven og forvaltningsloven. Videre heter det i virksomhetsinstruksen fra Kommunal- og moderniseringsdepartementet at vi skal ha en aktiv

holdning til kommunikasjon, både internt og eksternt. Det er viktig at vi fanger opp signaler som angår Datatilsynet, og at vi bruker dette aktivt i kommunikasjonsarbeidet. Kommunikasjon skjer i første rekke gjennom nettstedet vårt, direkte veiledning overfor publikum, aktiv mediekontakt og gjennom en utstrakt foredragsvirksomhet.

Nettstedet www.datatilsynet.no

Nettstedet er det viktigste verktøyet vårt, og vi legger betydelig vekt på at innholdet skal være relevant, korrekt og godt tilpasset brukerne. Vi arbeider derfor kontinuerlig med å vedlikeholde og strukturere innholdet, samtidig som vi også må videreutvikle nettstedet på en god måte.

Antall besøkende, røkting og organisering av arbeidet

Antallet besøk på nettstedet har gått opp i 2016. Vi opplever stor interesse om det nye personvernregelverket som kommer fra 2018. Vi ser også at bruksmønsteret endrer seg. Stadig flere oppsøker veiledningsmaterialet vårt fra mobil eller nettbrett mens de er på farten. Her er økningen stor, fra 16 prosent til 24 prosent.

I 2016 begynte vi arbeidet med å få til en oppgradering av nettstedet i 2017, som en forberedelse til at mye av innholdet på nettsidene må endres før forordningen trer i kraft i 2018.

Oversikt over nøkkeltall fra nettstatistikken på datatilsynet.no[1]:

	2015	2016
Antall sider på nettstedet (Google site search)	2 360	2 320
Antall besøk til nettstedet	148 000	202 000
Antall sidevisninger	413 000	598 000
Antall sidevisninger pr besøk	2,7	3,5
Gjennomsnittlig besøksvarighet	3 min og 47 sek	3 min 52 sek
Antall søk i søkemotoren på datatilsynet.no	36 300	43 000
Andel besøk fra mobile enheter	16 prosent	24 prosent
Antall publiserte nyhetssaker	58	44

Datatilsynet utførte høsten 2016 også en brukerundersøkelse på nett. Undersøkelsen hadde nærmere 1000 respondenter og var overveiende positiv. Ifølge tallene lykkes 79,4 prosent av de besøkende til datatilsynet.no med å få utført den oppgaven de kom for å gjøre. Et stort flertall kom frem til den informasjonen som er relevant for dem. Undersøkelsen identifiserer også noen problemområder som vi jobber videre med i 2017.

Personvernblogg, sosiale medier og debattinnlegg

Personvernbloggen.no fungerer etter intensjonen og er et rom hvor vi kan reise andre problemstillinger enn vi kan på den ordinære nettsiden. Hele 2 200 personer har bedt om varsling på e-post når det kommer nye innlegg.

Vi følger med på omtale av Datatilsynet og temaet personvern på Twitter, og vi besvarer raskt de fleste spørsmål og kommentarer som kommer via denne kanalen. Vi har i 2016 hatt tre kronikker og debattinnlegg i ulike papirbaserte medier.

[1] På grunn av et problem med statistikkverktøyet vårt, har vi ikke statistikk for de første fire månedene av 2016. Tallene over er for perioden mai-desember 2016.

Oversikt over noen sentrale tall:

	2013	2014	2015	2016
Innlegg på Personvernbloggen	41	50	40	30
Besøk på Personvernbloggen[2]	8 000	20 000	-	-
Twittermeldinger	220	193	177	178
Twitterfølgere	10 065	12 392	14 100	15 000
Kronikker og debattinnlegg i andre medier	8	9	9	3

Mediekontakt

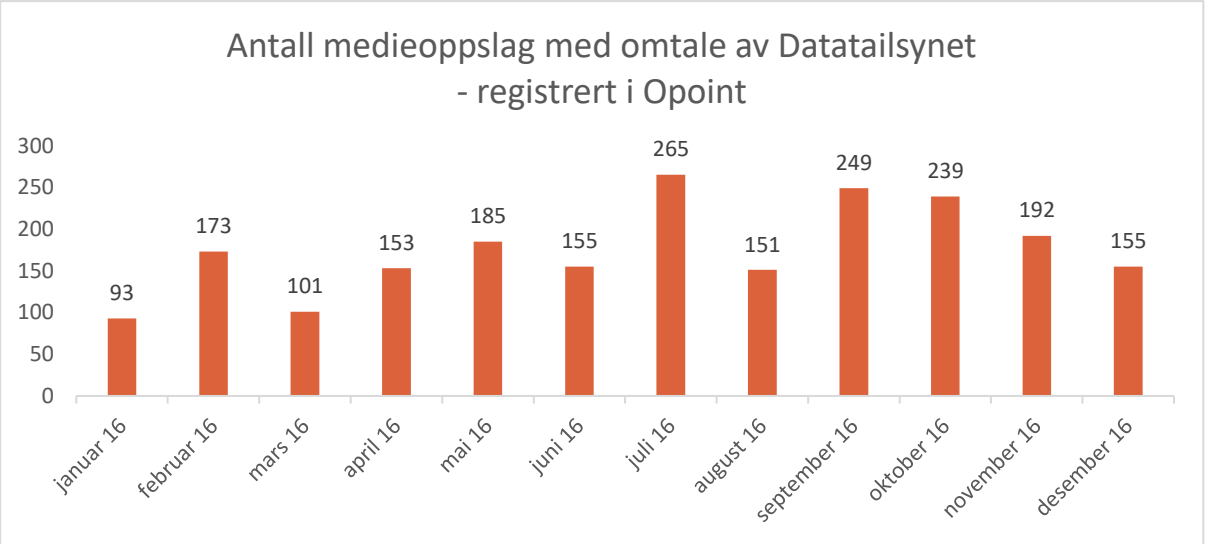
Mediene vurderes som en svært viktig kanal for å få frem budskapene våre, og det er jevn pågang og interesse fra disse. Vi legger stor vekt på å ha et profesjonelt forhold til mediene. Dette innebærer at vi skal ha god tilgjengelighet og et høyt servicenivå overfor journalistene. Dette mener vi å ha lykkes godt med også i 2016.

I løpet av året har vi registrert 618 besvarte mediehenvendelser. Det er noe lavere enn året før, og viser en fortsatt nedgang i antall direkte henvendelser fra medier:

	2013	2014	2015	2016
Mediehenvendelser[3]	850	800	650	618

Medieovervåkingstjenesten Opoint har imidlertid registrert til sammen 2 111 oppslag i internettbaserte medier hvor Datatilsynet er omtalt i løpet av året:

	2013	2014	2015	2016
Medieoppslag[4]	3 632	2 920	1 843	2 111



[2] Vi har ikke besøkstall for Personvernbloggen for 2015 og 2016 på grunn av en feil i statistikkverktøyet.

[3] Registreringssystemet vårt er etablert til bruk av kommunikasjonsavdelingens medarbeidere for å sikre en best mulig oversikt og koordinering i vår kontakt med mediene. I tallene inngår derfor ikke mediehenvendelser som går direkte til andre ansatte. Det reelle antallet er derfor noe høyere enn de registrerte henvendelsene.

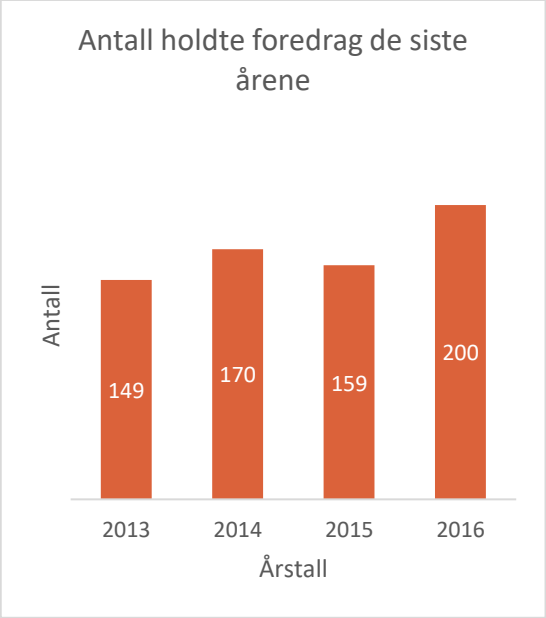
[4] Det varierer noe fra år til år hvordan Opoint rapporter, så tallene er ikke helt nøyaktige.

Dette var noen av de temaene som fikk mest medieomtale i 2016:

- Brukervilkår i mobilapper (treningsapper og pokemon-go)
- Facebook at Work
- Nye politimetoder og digital grensekontroll
- Overvåking av barn og unge
- Personvern i skole og barnehage
- Tollvesenet vil lagre bilder av alle biler som krysser grensen
- Storbank «vippser» kundeinfo til Facebook
- Politiet kan få videokamera på uniformen

Foredragsvirksomheten

Gjennom foredrag oppnår vi en unik synlighet. Vi møter og blir tilgjengelig for virksomheter, interesseorganisasjoner, publikum og ulike sektorer på en helt annen måte enn vi gjøre i andre kanaler. Foredragsvirksomheten vår er derfor en viktig del av vår utadrettede kommunikasjonsvirksomhet.



I 2016 holdt vi 200 foredrag på eksterne arrangementer, mot totalt 159 i hele 2015.

Vi får mange forespørsler om å holde foredrag gjennom hele året. Forespørslene vurderes ut fra kriterier som antall deltagere, om temaet er relevant for våre satsningsområder samt vår kapasitet. Vi har som mål å holde mellom 120 og 150 foredrag per år.

Temaene for foredragene varierer. I tillegg til en rekke generelle innlegg om personvern, personopplysningsregelverket, kameraovervåking og Datatilsynet og våre oppgaver, har vi i år holdt flest foredrag om:

- Ny personvernforordning fra EU
- Kommersiell bruk av personopplysninger – det store datakappløpet
- Informasjonssikkerhet, innebygd personvern og ny teknologi
- Barn og unges personvern

Vi har hatt stor økning både i antall henvendelser om foredrag og hvor mange foredrag vi har holdt. Dette skyldes trolig innføringen av EUs personvernforordning i 2018. Flere av henvendelsene om foredrag har kommet etter at noen har lest eller hørt om den nye forordningen, enten fra oss eller fra andre.

ÅRETS VIKTIGSTE AKTIVITETER

Justissektoren

I justissektoren møter vi tungtveiende hensyn som taler for at staten skal kunne gjøre inngrep i individets rettssfære. Ofte skjer dette uten den enkeltes medvirkning og med begrenset rett til informasjon. Individet kan dermed ha begrensede muligheter til å ivareta sine interesser. På disse områdene er det derfor særlig viktig at tilsynsmyndighetene ser til at enkeltmenneskets rettigheter ivaretas.

Politiregisterloven og politiregisterforskriften trådte i kraft 1. juli 2014. Loven og forskriften regulerer politiets og påtalemyndighetens behandling av personopplysninger, og regelverket gir Datatilsynet en sentral rolle som kontrollør av at regelverket etterleves. Datatilsynet har som mål å bidra til en god implementering og praktisering av politiregisterloven med tilhørende forskrift, samt å ivareta de registrertes rettigheter i møte med politiet.

Gjennomførte aktiviteter

Tilsyn

Kontroll med Politiets utlendingsregister

I juni gjennomførte vi en kontroll med Politiets utlendingsregister. Det er Politiets utlendingsenhet (PU) som er ansvarlig for dette registeret. Datatilsynet har ved overgangen til 2017 ikke trukket noen endelige konklusjoner i saken, men har sendt PU en foreløpig rapport, og samtidig varslet noen pålegg. Påleggene gikk blant annet ut på at PU må sørge for tilfredsstillende rutiner for sletting av personopplysninger fra utlendingsinternat, bedre informasjon til rettighetshaverne, og gjennomføre regelmessige risikovurderinger. PU har ikke hatt anledning til å kommentere faktagrunnlaget som rapporten og påleggene bygger på – og hvis de aktuelle avvikene lukkes før den 10. februar 2017, vil saken bli avsluttet uten at det blir fattet endelige vedtak.

Kontroll med Schengen informasjonssystem

Datatilsynet har også en kontrollerende funksjon etter lov om Schengen informasjonssystem (SIS-loven). I 2016 gjennomførte vi en stedlig kontroll av Schengen informasjonssystem hos Sirene-kontoret ved Kripos. Den foreløpige rapporten hadde ikke blitt sendt ved årsskiftet.

De viktigste høringsuttalelsene

Advokatutvalgets utredning NOU 2015:3 – Advokaten i samfunnet

Advokatutvalgets forslag til nytt regelverk for advokater og andre som yter rettslig bistand (I NOU 2015:3) ble sendt på høring i mai 2015, med høringsfrist 1. januar 2016.

Vi hadde flere merknader. Blant annet var vi enig i at det er behov for avklaringer, og eventuelt særskilte regler, som regulerer advokaters behandling av personopplysninger, samtidig som det er anbefalt å avvente implementeringen av den kommende personvernforordningen. Tilsynet påpekte videre at det var behov for ytterligere avklaringer hva gjelder forholdet mellom forslagets bestemmelse om informasjonssikkerhet og personopplysningslovens krav. I tillegg var vi uenige i forslaget om å innføre taushetsplikt overfor Datatilsynet, idet en slik ordning ville kunne hindre oss i å utføre våre kontrolloppgaver. Vi foreslo i stedet at personopplysningslovens regler om taushetsplikt fortsatt skal gjelde for advokater.

Endringer i straffeprosessloven og politiloven – Utlevering av informasjon fra PST til E-tjenesten

Justis- og beredskapsdepartementet foreslo endringer i straffeprosessloven og politiloven om at PST skal kunne utlevere informasjon innhentet via skjulte tvangsmidler til E-tjenesten, dersom det er nødvendig for E-tjenesten sin utførelse av lovpålagte oppgaver. Lovforslaget innebærer at informasjon som er innhentet av PST, gjennom for eksempel romavlytting og kommunikasjons-kontroll, kan utleveres på lik linje med informasjon innhentet ved bruk av ordinære og betydelig mindre inngripende metoder.

Vi mente forslaget var problematisk, og viste blant annet til at opplysningene det var snakk om allerede er innhentet på en svært inngripende måte, og til ett konkret formål. Om opplysningene tillates videreformidlet, dreier det seg om en form for formålsglidning som lovverket setter strenge skranker mot. Vi mente forslaget også måtte ses i lys av Prop. 68 L (2015-2016), som innførte dataavlesing i straffeprosessloven.

Vi mente videre at de foreslåtte reglene for utlevering burde være tydeligere utformet. Lovteksten burde ha vist til hvilke konkrete og forhåndsdefinerte formål og oppgaver E-tjenesten skal kunne bruke opplysningene som de mottar fra PST. Det er heller ikke tilstrekkelig at PST må gi sitt samtykke dersom E-tjenesten ønsker å utlevere opplysningene de har fått fra PST videre til samarbeidende utenlandske tjenester.

Endringer i politiregisterloven og -forskriften – implementering av direktiv EU 2016/680

Direktiv EU 2016/680 får virkning samtidig med den generelle personvernforordningen, det vil si våren 2018, og Justis- og beredskapsdepartementet sendte sine forslag til endringer i politiregisterloven og -forskriften ut på høring den 11. november, med høringsfrist 15. desember (med senere frist den 1. februar 2017 for forskriftsendringene).

Vi hadde kommentarer om forutgående konsekvensutredninger og forhåndskonsultasjoner med tilsynsmyndigheten, og mente at lovforslaget burde inneholde regler om dette. Vi tok videre til orde for at det tas inn en henvisning til den generelle personvernforordningens bestemmelser om samarbeid mellom de europeiske tilsynsmyndighetene, og understreket dessuten viktigheten av reglene om generell informasjon til de registrerte.

Politiets tilgang til utlendingsmyndighetenes registre

Forslaget gikk ut på å gi politiet tilgang til utlendingsforvaltningens registre for politimessige formål, enten via utlevering eller direkte søk. Vi påpekte at forslaget føyet seg inn i en lang rekke lovforslag som åpner for utvidet tilgang til ulike forvaltningsregistre i løpet av de siste årene. Forslaget er med andre ord nok et eksempel på et register som opprettes for ett formål, men som senere brukes for andre formål – det vil si *formsålsglidning*. Dette er prinsipielt uheldig, og kan også få negative konsekvenser for tillitsforholdet mellom staten og borgerne.

Digital sårbarhet - NOU 2015:13

Det digitale sårbarhetsutvalget leverte sin rapport om digital sårbarhet i samfunnet til Justisdepartementet i slutten av 2015. Rapporten konkluderer blant annet med at kryptering ikke bør reguleres. Vi var enige i dette, ettersom muligheten for å kryptere kommunikasjon er av stor betydning for personvernet. Vi beskrev forbud mot eller regulering av kryptering som et blindspor.

Utvalget pekte på at inngripende metoder ofte foreslås uten forutgående og god utredning av konsekvenser. Dette er også Datatilsynets erfaring. Vi stilte oss bak utvalgets anbefaling om at det i

forbindelse med vurdering av inngripende tiltak, må brukes utredninger og offentlig debatt for å sikre en balanse mellom personvern og et sikrere samfunn.

Vi støtter også utvalgets forslag om en nasjonal kompetansestrategi for IKT-sikkerhet. Vi anbefalte at også Kommunal- og moderniseringsdepartementet (KMD) tas med i dette arbeidet, for å sikre at problemstillinger knyttet til personvern får sin plass i dette arbeidet.

Samlet sett mente vi at rapporten, med dens kartlegging av sårbarheter og hvordan personopplysninger samles inn og benyttes av blant andre politiet i dag, underbygger behovet for en personvernkommisjon for justissektoren.

Øvrige aktiviteter

Samtaler om en personvernkommisjon for justissektoren

I 2016 hadde vi et møte med justisministeren om personvernets kår i justissektoren. Møtet kom i stand etter et initiativ fra vår side i 2015, hvor vi blant annet foreslo å opprette en komite for personvern i justissektoren. Forslaget skulle ifølge ministeren vurderes internt. Senere på året ble et lignende forslag lansert av Venstre i Stortinget, men da med et bredere og mer generelt nedslagsfelt.

Bransjenorm for sikkerhetsbransjen

Vi har også arbeidet med å få i stand en bransjenorm for den private sikkerhetsbransjen, for å legge til rette for en bedre ivaretakelse av personvern i denne voksende sektoren. Blant temaene som er tenkt regulert i normen, er kameraovervåking, bruk av droner og utveksling av informasjon om mulig straffabere mellom ulike aktører i bransjen. Arbeidet med å ferdigstille normen fortsetter i 2017.

Sletting av referanseprofiler

Videre oppsto det debatt om sletting av DNA-referanseprofiler hos Folkehelseinstituttet da Arkivverket anførte at sletting av disse opplysningene – slik Datatilsynet fastslo etter en stedlig kontroll i 2015 – ville være i strid med arkivlovgivningen. Bakgrunnen var motstrid mellom reglene i personregisterlovverket og arkivlovgivningen. Diskusjonen fikk imidlertid sin løsning da Justis- og beredskapsdepartementet mot slutten av året lanserte endringer i det relevante regelverket, slik at det ble brakt i harmoni.

DGF og EU-domstolens avgjørelse i Tele2-saken

En av årets kanskje viktigste hendelser kom 21. desember, da EU-domstolen fastslo at de svenske og britiske datalagringslovene var i strid med menneskerettighetene. Datatilsynet uttalte da at dommen ville få konsekvenser for det digitale grenseforsvaret (DGF) som Lysne II-utvalget hadde lansert i en rapport noen måneder tidligere samme år.

DGF innebærer en generell masseinnsamling av kommunikasjonsdata og overvåking av norske borgere, til tross for at tiltaket er ment å skulle beskytte oss mot internasjonal terrorisme og cyber-angrep fra andre land. DGF-rapporten ble sendt på høring i oktober, med høringsfrist i januar 2017.

Lovforslag om skjulte tvangsmidler (dataavlesing mm.)

Den 11. mars fremmet Regjeringen et lovforslag om å innføre nye, skjulte tvangsmidler til kriminalitetsbekjempelsesformål (Prop. 68 L (2015-2016)). Proposisjonen, som fulgte opp NOU 2009:15, inneholdt blant annet et forslag om å innføre dataavlesing som virkemiddel for politiet og PST, samt utvidet adgang til å benytte andre skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd.

Like etter påske, den 7. april, ble det avholdt en åpen, muntlig høring om lovforslaget i Stortingets justiskomité. Vi ga i et ti minutter langt innlegg vårt syn på lovforslaget der vi blant annet understreket at forslaget atter en gang aktualiserte behovet for en utredning av personvernets kår i justissektoren.

Videre pekte vi på at dataavlesing reiser så mange prinsipielle og vanskelige spørsmål, at bestemmelsene om dataavlesing bør innføres som «solnedgangslovgivning», det vil si med en tidsbegrensning på to til tre år. En slik solnedgangsklausul ville ha sikret at dataavlesing ikke innføres som et virkemiddel med endelig virkning, uten at det er et reelt behov for det, og at personverninngrepet som tiltaket innebærer er nødvendig og proporsjonalt i et demokratisk samfunn, slik menneskerettighetene krever. I tillegg mente vi at kontrollen med bruken av disse virkemidlene burde styrkes.

Lovendringene ble vedtatt 8. juni.

Fremtidige utfordringer

I justissektoren møter vi stadig argumenter om at alvorlig kriminalitet generelt og terrorisme spesielt, nødvendiggjør nye og inngripende tiltak. Vi ser også at justismyndighetene argumenterer for utvidet tilgang til ulike registre som er opprettet for andre formål enn de politimessige. Utviklingen vil neppe stoppe opp i 2017, ikke minst vil DGF bli mye debattert i 2017, tror vi.

Denne utviklingen utgjør uansett en konstant trussel mot vårt personvern. I løpet av 2016 har vi sett flere tiltak og lovforslag som vil innebære store inngrep i den enkeltes rettigheter og frihet. Summen av de mange tiltakene er vanskelig å få øye på og å ta innover seg. Vi vil med andre fortsette å prioritere arbeidet med disse spørsmålene i årene som kommer.

Offentlig sektor

Digitalisering er en samlebetegnelse for overgangen fra analoge, mekaniske og papirbaserte løsninger, prosesser og systemer, til elektroniske og digitale løsninger. Utviklingen er slik at det ikke lenger er et spørsmål *om* forvaltningen skal digitaliseres, men hvor fort og med hvilke prioriteringer.

Regjeringens mål med IKT-politikken er å påvirke utviklingen innen IKT slik at det oppnås forenkling og effektivisering i offentlig sektor, samt fremme innovasjon og verdiskaping i næringslivet. Dette er selvsagt riktige målsettinger som også er viktige for Datatilsynet å bidra til. Når flere tjenester flyttes over på nett, skapes imidlertid nye personvernmessige utfordringer, samtidig som det også gir muligheter for å bygge hensynet til personvern inn i løsningene.

På flere og flere områder er digitaliseringen kommet langt i offentlig sektor, og stadig nye tjenester tilbys i digital form. Likevel er det fremdeles mange av de viktige digitaliseringsprosessene som er i startgropa. Det er derfor viktig at vi er på banen for å påvirke de riktige aktørene. Vi må sørge for å fremme personvern i alle disse prosessene. Vi finner det stadig riktig at vi konsentrerer oss om myndighetsutøverne og beslutningstakerne, idet det er her de viktigste premissene blir lagt. Eksempler på utfordringer vi ser fremover er autentisering av ansatte og virksomheter, og bruk av felleskomponenter, der deling av data og offentlige stordata (Big Data) er sentrale elementer.

Ved deling og gjenbruk av personopplysninger, utfordres prinsippet om formålsavgrensning i personvernlovgivningen. Det er viktig at samtlige offentlige aktører er bevisste i sin produksjon, bruk og deling av offentlige stordata. Her vil blant annet gode, korrekte og konsistente metadata være helt nødvendig for å lykkes, også i en personvernkontekst.

For å sikre et godt personvern ved utveksling og deling av personopplysninger mellom ulike offentlige instanser, og mellom offentlige og private aktører, må ansvarsforholdene være tydelig avklart. For at innbyggerne skal kunne ivareta eget personvern, må de få informasjon om hvilke instanser som lagrer, behandler og utveksler opplysninger om dem, til hvilke formål og hvordan de kan ivareta sin rett til innsyn, retting og sletting.

Offentlig sektor, og særlig kommuner, er storbrukere av alle typer personopplysninger, og bruker disse blant annet for å fastslå hvilke rettigheter og plikter den enkelte innbygger har. Det er derfor i innbyggernes interesse at det offentlige har tilgang på korrekte personopplysninger.

Gjennomførte aktiviteter

Vår «Strategi for godt personvern i digitaliseringen av offentlig sektor» fra 2103 danner fremdeles grunnlaget for mange av de aktivitetene vi prioriterer innenfor dette området.

Vi har gjennomført kontroller med både statlige og kommunale virksomheter som vi over tid har opplevd at har utfordringer med å etterleve kravene til internkontroll og informasjonssikkerhet. Etter vår vurdering er det viktig at virksomhetene først har kommet opp på et akseptabelt nivå med internkontroll og informasjonssikkerhet, før de tar fatt på de store digitaliseringsprosessene.

Vi har gjennomført veiledningsmøter med aktører i sektoren. I tillegg kommer utstrakt veiledning per telefon og e-post.

Vi deltar på flere arenaer der vi ønsker å gjøre Datatilsynets ståsted og holdninger kjent, og vi er tilstede på konferanser med både foredrag og stands.

Vi har også jevnlig møter på toppnivå med alle de sentrale aktørene innenfor digitaliseringen. Vi har heller ikke i 2016 lyktes med å få en fast plass i samarbeidsorganet SKATE (Styring og koordinering av

tjenester i e-forvaltning). Vi mener fortsatt at Datatilsynet er en naturlig deltaker her, og jobber videre for å bli deltaker. Dette mener vi er ytterligere aktualisert med den nye personvernforordningen som vil gjelde fra mai 2018. Kravene i denne til virksomhetene, inklusive offentlig sektor, mener vi er av en slik karakter at vår deltakelse i SKATE ville gavnet hele sektoren.

Tilsyn

I 2016 gjennomførte vi kontroller med 15 forskjellige kommuner. Dette var både stikkprøvekontroller, risikobaserte kontroller og kontroller basert på foregående. For samtlige av kontrollene var etterlevelse og dokumentasjon av internkontroll og informasjonssikkerhet hovedtema.

Selv om det er store variasjoner i hvordan etterlevelsen og dokumentasjon framstår hos de forskjellige kontrollobjektene, kan vi konstatere at det er et gjennomgående problem at mange kommuner ikke har tilfredsstillende rutiner for å oppfylle pliktene i personvernlovgivningen. Dette gjelder særlig pliktene til å:

- ha oversikt over hvilke behandlinger av personopplysninger virksomheten har,
- sørge for at innbyggere blir informert om hvordan opplysninger blir håndtert,
- sørge for at innsyn blir håndtert på riktig måte,
- gjennomføre og dokumentere risikovurderinger og sikkerhetsrevisjoner, og
- ha oversikt over databehandlere og ha tilfredsstillende databehandleravtaler med disse.

Vi har ikke kunnet fastslå at det er signifikante regionale forskjeller eller forskjeller knyttet til størrelse på virksomhetene. Det er gjerne slik at store virksomheter har mer og bredere kompetanse, men det er ikke alltid slik at dette gir seg utslag i bedre ivaretakelse av personvernet og oppfyllelse av pliktene i personopplysningsloven. Imidlertid mener vi å kunne se at virksomheter som har personvernombud, gjennomgående har en bedre ivaretakelse av personvernet og oppfyllelse av pliktene i loven. Dette mener vi viser at ordningen med personvernombud, og opplæringen av disse, har en positiv effekt for personvernet.

Like fullt er det bekymringsfullt at virksomheter som har ansvar for digitaliseringsprosesser, og virksomheter som i økende grad benytter nye digitale løsninger, ikke har tilstrekkelig fokus på å ivareta personvernet og å oppfylle pliktene i personopplysningsloven knyttet til internkontroll og informasjonssikkerhet. Dette gjør at vi også i kommende år vil måtte bruke kontroller for å sikre at nye digitale tjenester ivaretar personvernet, og at de virksomhetene som benytter slike tjenester har god nok internkontroll og informasjonssikkerhet. Vi vil også, sammen med sektoren, vurdere andre tilnærminger for å oppnå dette.

Sentrale høringsuttalelser

Ny kommunelov – Kommunelovutvalget

Datatilsynet støttet i hovedlinjene i forslaget, likevel valgte vi å kommentere enkelte punker i forslaget, blant annet påpekte vi viktigheten av når det er nødvendig med databehandleravtale mellom kommunene når disse danner kommunale oppgavefellesskap, og at dette bør utdypes nærmere i merknadene. Dette er basert på den erfaring vi har fra kontroller med kommunene som viser at det jevnt over er liten kunnskap hos den enkelte kommune om nødvendigheten av databehandleravtaler. Vi valgte også å tydeliggjøre vår støtte til kravet om at kommunen skal ha en strategi for å informere borgerne og hvordan informasjonen skal tilpasses den enkelte gruppe. Dette er særlig viktig i forhold til barn.

Evaluering av offentlighetsloven

Datatilsynet ser positivt på digitaliseringen i offentlig sektor, også når det gjelder meroffentlighet. Men det er viktig at det er gjort tilstrekkelige risikovurderinger og utarbeidet gode nok rutiner, når dokumenter skal legges ut i fulltekstversjon. Da er muligheten for at feil blir gjort erfaringsmessig dessverre ganske stor, blant annet ved at taushetsplikten kan bli brutt. Nettopp fordi det i dag ikke er gode nok rutiner i den enkelte etat for å hindre at dette skjer. Vi erfarer også at det heller ikke gjort tilstrekkelig for å hindre at eksterne søkemotorer fanger opp slik publisering. Disse erfaringene er selvsagt påpekt i vårt høringssvar.

Åpenhet om eiere i aksjeselskap

Formålet med aksjeeierbok er at det skal være mulig for alle å skaffe en oversikt over hvem som eier aksjer i det enkelte aksjeselskap. Vi støttet ikke forslaget om å lage en samlet oversikt over enkeltpersoners aksjeportefølje på tvers av selskaper, fordi dette er mye mer inngripende sett fra et personvernperspektiv. Vi støttet forslaget fra Brønnøysundregistrene som innebærer at den som skal ha innsyn logger seg inn via Altinn. Systemet vil fungere på tilsvarende måte som ved søk i skattelistene. Datatilsynet mener at innlogging er en nødvendig forutsetning for å begrense muligheten for å lage parallelle registre og tilleggstjenester på internett, med krysskopling og supplering av andre personopplysninger.

eID-forordningen

Vi avga høringsinnspill til Nærings- og fiskeridepartementet om gjennomføringen av EUs forordning om elektronisk identifisering (eID-forordningen) og tillitstjenester for elektroniske transaksjoner. Våre viktigste tilbakemeldinger:

- Selvdeklareringsordninger er ikke tilstrekkelig for alle autentiseringsløsninger og krypteringstjenester. Vi mener det kan være direkte uforsvarlig å ikke regulere krav til sikkerhetsnivå for de løsningene og tjenestene som skal ivareta større verdikjeder, slik som for eksempel ID-porten. De bør underlegges et regelverk med tydelige krav til sikkerhetsnivå.
- Regjeringen må sørge for at den statlige delen av de elektroniske leveringstjenestene har en forsvarlig regulering når det gjelder ansvar og sikkerhet. For å få til dette bør det tas inn en hjemmel for forskriftskompetanse for regulering av den statlige delen av Sikker digital post, Altinn, Mitt helsearkiv og eventuelt andre elektroniske leveringstjenester som måtte komme i fremtiden.
- Regjeringen bør kreve at alle tilbydere av elektronisk postkasse skal oppfylle kravene til kvalifisert tjenestetilbyder. Det vil gi bedre forutsigbarhet omkring sikkerhetsnivå og skape den nødvendige tilliten til tjenestene. Det vil også gjøre det enklere for tilsynsmyndigheten, da det i en revisjon vil kunne pekes på spesifikke krav i forordningen.

Saksbehandling og sentrale nemndavgjørelser

Vi har behandlet tips om forhold i offentlig sektor som omhandler personvern. Ut i fra størrelse og omfang har vi prioritert hvilke saker vi skulle følge opp, og på hvilke måter. Vi har ikke gjennomført stedlige tilsyn basert på tips, men vi har fulgt opp innkomne henvendelser ved å be om redegjørelser. Dette har blant annet resultert i at vi har fattet vedtak om endring av rutiner og sikkerhetstiltak.

Vi har mottatt og behandlet en rekke avviksmeldinger fra sektoren der det har vært uautorisert utlevering av personopplysninger om registrerte eller ansatte. Også her har vi i enkelte saker bedt om redegjørelser og hatt påfølgende saksbehandling.

Det har i forbindelse med fire avvik blitt ilagt i alt fem overtredelsesgebyr; fire til kommuner, ett til en fylkeskommune. Samtlige var knyttet til forhold med publisering av sensitive personopplysninger på nett, noe som vi anså som alvorlige brudd på personopplysningslovens bestemmelser om internkontroll og informasjonssikkerhet. Tre av disse gebyrene ble godtatt, mens den siste virksomheten klagde på avgjørelsen til Personvernnemnda. Klagen er nå behandlet i Personvernnemnda og gebyrets størrelse ble redusert.

Bakgrunnen for å ilegge gebyr var at det var forhold vi anså for å være alvorlige brudd på pliktene etter personopplysningsloven. I noen av tilfellene ble ikke avvikene meldt av virksomheten selv, men ble kjent enten via media eller gjennom de berørte. Vi ønsket også å utnytte den allmennpreventive virkningen ved overtredelsesgebyr. Responsen fra sektoren tyder på at dette har hatt effekt. Ønske om samarbeid fra aktører slik som for eksempel kommunenes interesseorganisasjon (KS) har tiltatt, og ønske fra enkeltkommuner eller statlige virksomheter om råd, veiledning og kurs har økt. De fleste er tydelige på at «gebyrsakene» har bidratt til at de nå ønsker å få orden på dette før vi kommer på nye kontroller.

Øvrige aktiviteter

Vi har oppsummert funnene våre og delt denne kunnskapen i ulike sammenhenger. Vi har blant annet deltatt som foredragsholdere på små og store arrangement hvor vi har møtt ansatte i offentlig sektor slik som i kommuner, fylkeskommuner, direktorater og departementer, men også leverandører av IKT-løsninger og andre aktører i sektoren.

Vi har gjennomført en rekke møter med beslutningstakere i offentlig sektor og leverandører av IKT-løsninger for å se på hvordan de best kan bygge og vedlikeholde gode internkontrollsystemer og god informasjonssikkerhet for å ivareta personvernet. Vi forsøker å gjøre aktører i sektoren til gode bestillere av løsninger med innebygd personvern, og vi har gitt råd til leverandører om å ta hensyn til innebygd personvern i deres leveranser til offentlig sektor.

Fremtidige utfordringer

Funn fra kontrollene i sektoren viser at aktørene fremdeles har betydelige mangler og en relativt lang vei å gå før vi kan si at sektoren er på et tilfredsstillende nivå. Riktignok finnes det flere unntak, og mange har kommet langt i etterkant av kontroller eller veiledning fra oss. Like fullt er det bekymringsfullt at sektoren har så betydelige mangler knyttet til internkontroll og informasjonssikkerhet som den har. Dette betyr at vi, sammen med andre aktører, må arbeide for at sektoren bedrer seg i arbeidet med internkontroll og informasjonssikkerhet. Vi må fortsette å bruke våre virkemidler for å høyne nivået i sektoren.

Vi har initiert i et arbeid sammen med KS for å finne andre arenaer og andre virkemidler som kan benyttes for å øke bevisstheten rundt personvern og etterlevelse av personopplysningsloven i kommunal sektor. Dette var et arbeid vi hadde stor tro på at ville materialisere seg tidlig i 2016, dessverre har vi måttet konstatere at KS ikke har kunnet prioritere dette på en slik måte som vi hadde ønsket. Like fullt vil vi fortsette dette samarbeidet og søke å få bedre fart og struktur på dette i 2017.

Datatilsynet har i flere år deltatt i arbeidet med å få på plass gode og sikre eID-ordninger, både for privatpersoner, ansatte og virksomheter. Det gjenstår fremdeles en del arbeid før vi har løsninger som er gode nok for alle disse kategoriene, særlig gjelder dette offentlige løsninger for ansatte og for virksomheter.

Vi deltar også i arbeidet med nytt folkeregister og føler vi er invitert med i dette for å bidra med spisskompetanse på personvern i dette viktige arbeidet.

Helse og velferd

Helse- og velferdsområdet omfatter primær og sekundær bruk av opplysninger innen helse- og omsorgstjenestene, NAV, helseforskning og samfunnsforskning. Opplysningene som behandles i denne sektoren er blant de mest sensitive som finnes, og befolkningen selv anser opplysningene som særlig beskyttelsesverdige. Innen dette ansvarsområdet behandles det opplysninger om befolkningen i alle livsfaser, og bruk og gjenbruk av våre opplysninger til stadig flere formål øker.

Hovedutfordringen innen helsesektoren er at den er gjenstand for store forandringer og at endringene skjer i et raskt tempo. Som eksempel nevnes ny lovgivning, ny forordning, teknologiutviklingen og utviklingen innen e-helse.

Helse- og omsorgstjenesten er preget av mange aktører og flere ulikt organiserte virksomheter med forvaltningsansvar og beslutningsmyndighet. Leverandører og databehandlere har ofte sentrale roller, og ansvarsforholdene kan ofte være uklare.

Endringer i bruken av pasientjournalsystemer, primært for å gi tilgang til pasientinformasjon på tvers av virksomhetsgrenser, stiller nye krav til systemenes evne til å ivareta sikkerheten for at opplysninger ikke gjøres tilgjengelige utover det som er nødvendig og relevant for den helsehjelpen som skal ytes. Informasjonsdeling til beste for den enkelte pasient er utvilsomt et gode. Men det å sørge for at slik informasjonsdeling ikke fører til utilsiktet spredning av sensitive opplysninger, er en vesentlig utfordring når det gjelder å ivareta enkeltindividets krav på beskyttelse av sine egne opplysninger. Ettersom eksisterende journalsystemer er utviklet for en annen og mer begrenset type bruk, byr dette på teknologiske utfordringer.

Vi ser også et økende ønske om og påtrykk for gjenbruk av helseopplysninger, såkalt sekundærbruk av data. Det opprettes stadig nye kvalitetsregistre, og mange av disse er store i omfang og har som formål å være permanente.

NAV har også mange av de tilsvarende utfordringene. Dilemmaet mellom å ha tilgjengelige opplysninger og å sikre tilfredsstillende konfidensialitet, kan gi utfordringer for hensynet til borgernes personvern. En annen utfordring innen NAV-systemet er at det i stor grad benyttes eksterne leverandører for å oppfylle NAV sine oppgaver. En nyere problemstilling er dessuten bruk av datamaterialet NAV besitter i stordataanalyser.

Gjennomførte aktiviteter

Tilsyn

I meldingsperioden har vi arbeidet videre med tilsynene med samfunnsforskning som ble startet i 2015. Foreløpige kontrollrapporter viser alvorlige avvik hos flere av institusjonen vi kontrollerte. Flere har mangler eller lite tilfredsstillende internkontrollsystemer.

Vi gjennomførte i februar kontroll med Oslo Universitetssykehus HF og Janusbanken. Dette helseregisteret har rettslig grunnlag gjennom konsesjon fra Datatilsynet, og vi ønsket å kontrollere om våre konsesjonsvilkår ble etterlevet. Endelig kontrollrapport var ikke klar ved årsskiftet.

Vi har også i 2016 gjennomført elleve brevkontroller med de forskriftsregulerte sentrale helseregistrene. Selv om registrene reguleres hver for seg og ut fra hvert registers formål, er det allikevel mange plikter og rettigheter som er felles for hvordan de behandler personopplysninger. Vi ønsket å undersøke hvorvidt de kravene som stilles til alle disse registrene gjennom deres forskrifter og gjennom de generelle bestemmelsene i helseregisterloven og personopplysningsloven ivaretas. Foreløpige rapporter er under utarbeidelse.

Vi har også sendt ut brevkontroller til alle helseforetakene med krav om redegjørelse over hvordan de behandler data til såkalt intern kvalitetssikring. Vi har mottatt svar, og vil starte arbeidet med å skrive rapporter i løpet av de første månedene i 2017.

Sent høsten 2016 startet vi brevlige tilsyn med virksomheter som deltar i samarbeid om felles pasientjournal. Det er i det vesentlige mindre helsevirksomheter slik som legekontor. En foreløpig vurdering av tilsvarende er at regelverkets krav om å avtale rammene for samarbeidet ikke etterleves i mange av virksomhetene.

Sentrale høringsuttalelser

Endringer i kjernejournal- og reseptformidlerforskriftene

Helse- og omsorgsdepartementet la i en høring fram forslag om endringer i kjernejournal- og reseptformidlerforskriften. De la til grunn at endringene hovedsakelig er av teknisk karakter og ikke har personvernmessige konsekvenser av betydning. Datatilsynet var ikke enig i dette. De foreslåtte endringene vil innebære en økt tilgang til helseopplysninger, redusert kontroll, utvidet lagringstid og større risiko for uautorisert bruk.

Nasjonal strategi for persontilpasset medisin i helsetjenesten

Vi avga også uttalelse i høringen av Nasjonal strategi for persontilpasset medisin. Vi var tilfreds med at Helsedirektoratets utkast til nasjonal strategi for persontilpasset medisin framhever pasientens råderett over egne opplysninger, men ser imidlertid behov for videre utredninger knyttet til blant annet personvernkonsekvenser.

Saksbehandling

Vi har mottatt og behandlet søknader om konsesjon knyttet til behandling av helseopplysninger i forsknings- og kvalitetssikringsprosjekter og i helseregistre, og store deler av våre ressurser på dette feltet har gått til behandling og oppfølging av enkeltsaker. I mange tilfeller medfører søknader om konsesjon behov for omfattende kontakt i form av veiledning og informasjon forut for og underveis i saksbehandlingen.

Vi har gjennom saksbehandlingen sett at eksisterende registre ønskes utvidet, og at opprinnelig avgitte samtykker strekkes langt og tolkes utvidende.

En annen tendens vi ser er at forskningsmiljøene ønsker å samle store datasett i et «hovedprosjekt» eller i en form for forskningsregister, og benytte dataene i flere underprosjekter.

I forbindelse med den nye helseregisterloven, har grensene for Datatilsynets konsesjonskompetanse vært forsøkt klargjort. Av forarbeidene til loven, går det frem at utgangspunktet er at vi kan gi konsesjon til tilnærmet alle typer registre og prosjekter. Vi gir i all hovedsak konsesjoner, i mange tilfeller med vilkår, og det er sjelden Datatilsynet gir avslag på søknader om konsesjon. I de tilfellene vi gir avslag, er dette begrunnet i at personvernulempene anses å være for store i forhold til den positive nytten prosjektet kan ha.

Sentrale nemndsavgjørelser

PVN-2015-10: Sykehuset Østfold

Datatilsynet forutsatte i sitt konsesjonsvedtak at Sykehuset i Østfold informerer pasientene etter helseregisterloven § 24, jf. personopplysningsloven §§ 18 flg., og at informasjonen skal være individuell. Personvernnemnda vurderte om det forelå hjemmel for unntak fra informasjonsplikten etter personopplysningsloven § 20 andre ledd, bokstav b, med begrunnelse i at det var

uforholdsmessig vanskelig å varsle de omlag 3000 deltakerne. Nemnda viste til sin egen uttalelse i sak PVN-2009-07 hvor den bemerket at det kan ikke være slik at hovedregelen ikke skal følges når det gjelder de manges personvern, men bare når det gjelder de få sitt personvern. Det er et prinsipielt viktig poeng nemnda fremhever fordi det stadig oftere argumenteres med at det er «uforholdsmessig vanskelig» å informere når det dreier seg om et større antall personer.

Nemnda kom til at det ikke var umulig eller uforholdsmessig vanskelig å informere disse pasientene.

PVN-2015-12 Universitetet i Oslo – Reseptregisteret

Personvernnemnda vurderte i denne saken om helseregisterloven § 9 og reseptregisterforskriften § 5-3 andre ledd åpner for at Datatilsynet kan gi konsesjon til sammenstilling av helseopplysninger fra Reseptregisteret med helseopplysninger fra andre kilder, til tross for at resultatet av koblingen gjør det mulig å bakveisidentifisere de registrerte. Nemnda kom til at en slik kobling ikke er tillatt etter reseptregisterforskriften.

Øvrige aktiviteter

1. januar 2016 ble Direktoratet for e-helse etablert, og de tidligere oppgavene til Helsedirektoratet ble delt mellom de to etatene. Vi har hatt flere møter med det nye direktoratet og etablert god kontakt med relevante personer og avdelinger. Denne kontakten er helt sentral for å kunne følge de pågående prosessene innen helsesektoren med blant annet velferdsteknologi, Nasjonal kjernejournal, En innbygger – en journal og e-Resept

Vi har videre hatt løpende kontakt med sentrale aktører som Folkehelseinstituttet, de Regionale komiteer for medisin og helsefaglig forskningsetikk (REK), Den nasjonale forskningsetiske komité for medisin og helsefag (NEM), Norsk samfunnsvitenskapelig Datatjeneste (NSD), helseforetakene, Senter for klinisk dokumentasjon og evaluering (SKDE), Helse- og Omsorgsdepartementet og Helsetilsynet.

Vi har også deltatt aktivt i arbeidet tilknyttet Norm for informasjonssikkerhet i helsesektoren (Normen) i arbeidsgrupper og i styringsgruppen. Etter ny lovgivning har det vært behov for oppdateringer av allerede eksisterende materiell.

I tillegg har vi deltatt i referansegruppen i forbindelse med utarbeidelse av ny versjon av Normens veileder for bruk av velferdsteknologi innen helse og omsorgstjenesten i kommunene.

Vi har også i 2016 vært i en rekke møter med KMD og HOD i forbindelse med at det arbeides med forskrifter for regulering av samtykkebaserte befolkningsundersøkelser og kvalitetsregistre. I tillegg har det vært møtevirksomhet knyttet til utarbeidelsen av forskriften til det nye kommunale pasient- og brukerregisteret (KPR), som kommer på høring våren 2017.

Velferdsteknologi og annen helseteknologi

Velferdsteknologi har vært et sentralt tema for Datatilsynet også i 2016. Vi har hatt mye aktivitet på området, både i form av veiledning, møter og foredragsvirksomhet. Vi har også hatt kontakt med Helsedirektoratet vedrørende veilederen til Normen. Datatilsynet mener det fremdeles er sentrale problemstillinger som bør avklares, slik som for eksempel plassering av behandlingsansvar, krav til databehandleravtaler og dokumentering av bruk av velferdsteknologi.

Vi ser også utfordringer knyttet til hvor sterkt dette feltet styres av leverandører, og hvordan kommunene som bestillere har en krevende oppgave med å ha reell kontroll over behandlingen av opplysninger – behandlinger som skjer på deres vegne av leverandører og databehandlere. En rekke av våre veiledningsmøter omhandler dette temaet.

De samme problemstillingene er aktuelle når det stadig utvikles og tilbys nye løsninger innen helseteknologi, både i form av utstyr som brukes til måling og rapportering av helse, og tilhørende apper og elektronisk behandling av data. Vi har hatt en rekke møter med forskjellige aktører som ønsker veiledning.

NAV

En ny utfordring innen NAV-systemet er at det er økende interesse for å ta i bruk stordatanalyser på NAVs registre. Disse registrene inneholder store mengder personopplysninger om så å si alle landets borgere. Vi ser med bekymring på at disse dataene som er samlet inn med spesifikke formål skal kunne benyttes til nye formål som er utenfor den «tradisjonelle sekundærbruken». Vi har hatt flere møter med prosjektet «Big Insight» som er finansiert av Norges forskningsråd, og som har til formål å lage analyseverktøy for å avsløre trygdesvindlere. Dette prosjektet har søkt om konsesjon, og saken er til behandling hos Datatilsynet.

Gendata

Vi møter også i økende grad problemstillinger knyttet til bruk av genetiske opplysninger. Det er stadig billigere å gjøre analyser av våre gener, og det er et økende ønske om å gjennomføre slike analyser. Vi ser utfordringer i at dette er et tema som er komplisert, og det er vanskelig å få god forståelse for konsekvensene av å behandle opplysninger om oss på denne måten. Den tradisjonelle tanken om at samtykkebasert behandling av opplysninger er lite inngripende blir satt på prøve når det kommer til bruk av genetiske data. Vi mener det er riktig å stille spørsmål ved om slike samtykker er tilstrekkelig informerte, og om rekkevidden av konsekvenser ved bruk av genetiske data går mye lenger enn til kun den som faktisk har samtykket, for eksempel til slektninger.

Vi har uttrykt at vi ønsker en bredere utredning knyttet til bruk av genetiske data, og at en slik utredning bør gjennomføres av en bredt nedsatt gruppe som også tar grundig for seg personvernkonsekvensene slik behandling kan medføre.

Vi har i 2016 hatt flere møter med Bioteknologirådet, og vi har blant annet gjennomført et bredt møte med blant annet Helsedirektoratet, REK, Bioteknologirådet og NTNU tilstede hvor gendata og haplotyperegister var særskilte temaer.

Konfidensialitetssikring i spesialisthelsetjenesten - logganalyse

Vern mot snoking i helsektoren handler om god tilgangsstyring, bruk av logger og holdninger hos de ansatte, og arbeid på alle disse områdene er nødvendig. Når det gjelder logganalyse er det erkjent at dagens regime med stikkprøver og mistankebasert gjennomgang av logg ikke er tilfredsstillende. Det har vært kjørt et stort pilotprosjekter på avansert logganalyse som ga gode resultater, men dette er avsluttet. Da logganalyse i spesialisthelsesektoren synes å mangle fremdrift, tok Datatilsynet senhøsten 2016 kontakt med sektoren for å avklare status på nasjonale tiltak før vi eventuelt fulgte opp spørsmålet overfor de enkelte helseforetakene. Status er på rapporteringstidspunktet ikke avklart, men det synes rimelig klart at konfidensialitetssikring ikke har vært nevneverdig prioritert av sektoren etter pilotprosjektet. Området krever videre oppfølging.

Fremtidige utfordringer

Som beskrevet over ser vi store fremtidige utfordringer knyttet til velferdsteknologi, genetiske data og konfidensialitetssikring ved logganalyse.

Utover bruk av logg ser vi også at etter ny lovgivning har det blitt lettere å kunne gi tilgang til pasientopplysninger på tvers av virksomhetsgrensene og å samarbeide om små og store felles

journalsystem. Vi mener at reguleringen rundt disse løsningene ikke er gode nok på forskriftsnivå. Våre kontroller over tid viser at pasientjournaler mangler den nødvendige strukturen som skal til for å kunne sikre at det ikke gis tilgang til mer enn nødvendig. Vi er derfor bekymret for at den adgangen pasientjournalloven gir, kan føre til unødvendig og utilsiktet spredning av pasientopplysninger.

Innen helsetjenesten skjer det en omfattende behandling av helseopplysninger som regnes som intern kvalitetssikring. Slik behandling av opplysninger er ansett å være lovhjemlet etter blant annet helsepersonelloven § 26, og dermed unntatt fra konsesjonsplikt. Denne hjemmelen er imidlertid svak og uklar etter vår oppfatning, og den er strukket langt med tanke på hvilke former for behandling av opplysninger den anses å gi hjemmel til.

Pasientjournallovens åpning for samarbeid om pasientjournaler mellom virksomheter, medfører også at det åpnes for at intern kvalitetssikring med den svake hjemmelen i helsepersonellovens § 26 utvides til å dekke alle innen slike samarbeid.

Stortinget har vedtatt at det skal opprettes et nytt register for kommunale helse og omsorgstjenester, KPR. Dette registeret skal forskriftsreguleres, og arbeidet med forskriften vil være et viktig personvernarbeid. Vårt inntrykk er at ønsket om å ha et omfattende og detaljert KPR er stort, og det skal tjene mange og tilnærmet ubegrensede formål.

Vi mener også at det er gode grunner til å tro at det etablerte screeningprogrammet for nyfødte vil foreslås endret. Det er sterke ønsker om å oppbevare data og materiale fra disse undersøkelsene utover det forskriften som regulerer ordningen tillater, og utover det som har vært forutsetningen ved etableringen av dette screeningprogrammet.

I tillegg ser vi tendenser til at det er ønskelig å gå bort fra den klare hovedregelen om samtykke fra registrerte innen sekundærbruk av helseopplysninger. Nye forskrifter vil aktualisere disse problemstillingene, og vi ser det som en utfordring å sikre at det også i fremtiden er samtykke som er det sentrale rettslige grunnlaget ved slik bruk av personopplysninger.

Det er en meget positiv personverntrend innen helsetjenesten at borgerne skal gis størst mulig grad av selvbestemmelse i egne opplysninger med nye innbyggertjenester. Dette ser vi som en styrking av den enkeltes rett til personvern. Samtidig er det enkelte utfordringer knyttet til at dette krever stadig større bevissthet og kunnskap hos den enkelte.

Helse- og omsorgstjenesten og NAV besitter enorme mengder data om oss. De er meget interessante for gjennomføring av stordataanalyser. Slike analyser utfordrer den tradisjonelle praksisen knyttet til sekundærbruk av data, og den reiser nye personvernproblemstillinger som vi mener kan være utfordrende for den enkelte og for de som skal vurdere om denne bruken av data skal tillates eller ikke.

Kommersiell utnyttelse av personopplysninger

Personopplysninger har i dag stor kommersiell verdi. Innsamling og analyse av forbrukerdata er viktig for å utvikle personaliserte tjenester og løsninger basert på kunstig intelligens.

Det er utfordrende for forbrukerne å få oversikt over hvilke opplysninger som samles inn, hvem som har tilgang til dem og hvordan de brukes. Ikke minst er det utfordrende å overskue hvilke konsekvenser den tiltagende kundeprofileringen har for den enkelte av oss, på kort og på lang sikt.

Markedet er i dag i ubalanse. Kommersielle virksomheter henter ut store inntekter fra analyse av personopplysninger, mens vi som avgir våre opplysninger har mangelfull innsikt i og kontroll med hvordan opplysninger brukes. Dette setter enkeltindividet i en sårbar posisjon. Undersøkelser har blant annet vist at prisdiskriminering på bakgrunn av profilering er utbredt på nett. Denne typen diskriminering er vanskelig å oppdage når praksisen foregår i det skjulte.

Datatilsynet har i 2016 fulgt opp problemstillingene vi reiste i rapporten «Det store datakappløpet». Vi har jobbet for å øke åpenheten rundt hvordan personopplysninger samles inn og brukes til profilering og målretting. Vi har også arbeidet for at enkeltindividet skal få bedre mulighet til selv å velge hvorvidt de ønsker å dele sine personopplysninger eller ikke når de tar tjenester i bruk.

Gjennomførte aktiviteter

Tilsyn

Vi igangsatte tilsyn med datamegleren InsightOne og dagligvarekjeden Trumf i 2016. Tilsynene vil bli sluttført i 2017.

Sentrale høringsuttalelser

Høring om kommunikasjonsverndirektivet (ePrivacy-direktivet)

EU kommisjonen har etter vedtakelsen av ny personvernforordning ansett det som nødvendig å evaluere det nåværende kommunikasjonsverndirektivet for å sikre harmonisering mellom de to lovverkene. Kommisjonen sendte en evaluering av kommunikasjonsverndirektivet ut på høring våren 2016. Datatilsynet ga i sitt høringssvar uttrykk for at det fortsatt er nødvendig med særlovgivning for beskytte sikkerheten til elektronisk kommunikasjon, selv etter innføringen av ny personvernforordning. Dette arbeidet er fulgt opp ved at kommisjonen har lagt frem et forslag til en ny forordning.

Øvrige aktiviteter

Møter med Schibsted

Schibsted er en betydelig medieaktør i Europa og selskapet investerer tungt i utviklingen av en plattform for personalisering av innhold og annonser. Schibsted har signalisert at hensynet til brukernes personvern har høy prioritet i utviklingen av den nye løsningen. Ettersom Schibsted er en ledende medieaktør, og når ut til svært mange brukere, er det av stor betydning å sikre at løsningene deres tilfredsstiller kravene i nåværende og kommende personvernlovgivning.

Datatilsynet har gjennomført flere møter med Schibsted i 2016. Formålet med møtene har vært å få større innsikt i hvordan selskapet håndterer personopplysninger i forbindelse med målretting av annonser og innhold til brukerne. Møtene har hatt tre hovedfokus:

- Schibsteds samarbeid med teknologileverandøren og annonsebørsen Appnexus.

- Schibsteds innsamling, lagring og bruk av data til profilbygging og segmentering av brukerne.
- Schibsteds håndtering av tredjeparter på deres nettjenester og utvikling av privacy dashboard-løsning.

Datatilsynet har etter møtene med Schibsted fått relativt god innsikt i hvilke personopplysninger selskapet samler inn og hvordan de behandles. Schibsted investerer store ressurser i utviklingen av et «privacy daschboard», der brukerne via personverninnstillinger kan bestemme hvilke opplysninger de ønsker at skal samles inn eller ikke. Dette er positivt. Vi anser imidlertid ikke arbeidet vårt som avsluttet og vil følge opp Schibsteds annonseplattform også i 2017.

Samarbeid med norske forbrukermyndigheter

Personvern og forbrukervern henger tett sammen. I den digitale økonomien er stadig flere forretningsmodeller basert på forbrukerdata. Vi har etablert tett dialog med Forbrukerombudet for å diskutere og avklare de respektive tilsynsmyndighetenes rolle når personvern og forbruker-beskyttelse møtes, slik at forbrukerne sikres et effektivt vern etter både personvern- og forbrukervernlovgivningen. Vi samarbeider også med Forbrukerombudet om klagesakene vi begge har mottatt fra Forbrukerrådet i 2016.

Vi har også tett kontakt med Forbrukerrådet. Forbrukerrådet har i 2016 kjørt en kampanje kalt Appfail, der de har undersøkt personvernvilkårene til apper, treningsarmbånd og internettbaserte leketøy. I forbindelse med undersøkelsene har de oversendt tre klager til Datatilsynet på tjenester de mener ikke overholder bestemmelsene i personopplysningsloven:

- **Run keeper:** Datatilsynet mottok en henvendelse om at Run keeper hadde sporet brukere mens appen ikke var i bruk. Dessuten ble personopplysninger delt med tredjeparter og ikke slettet rutinemessig. Da Datatilsynet mottok henvendelsen, hadde allerede Fitnesskeeper Inc rettet opp i førstnevnte feil. Dessuten var vår daværende vurdering at norsk lov ikke kom til anvendelse ettersom selskapet er hjemmehørende i USA. Vi valgte likevel å sende Fitnesskeeper anbefalinger siden selskapet viste endringsvilje og ville unngå mer negativ presse.
- **Treningsarmbånd:** I november 2016 klagde Forbrukerrådet fire produsenter av treningsarmbånd inn for både Datatilsynet og Forbrukerombudet. Det var tre amerikanske produsenter (Fitbit, Jawbone og Garmin) og en kanadisk (Mio). Etter innledende undersøkelser av de påklagde forhold besluttet vi å følge opp saken overfor Garmin, som er det eneste selskapet som er etablert i Norge. For de øvrige selskapene ble det besluttet å anmode om bistand fra de landene hvor selskapene er etablert. Saken følges nærmere opp i 2017.
- **Connected Toys:** Henvendelsen gjaldt primært at smarte dukker brukte barns stemmer for egne formål og hadde dårlig informasjonssikkerhet. Bak behandlingen av personopplysninger sto en Hongkong-basert og en amerikansk virksomhet. Det nederlandske datatilsynet hadde allerede anmodet søstermyndighetene våre i Hongkong, Kina (PCPD) og USA (FTC) om å etterforske saken. Dessuten hadde den amerikanske uavhengige forskningsstiftelsen EPIC (Electronic Privacy Information Centre) levert en grundig klage til FTC. Vi valgte derfor å gjøre som det nederlandske datatilsynet for å unngå dobbeltarbeid og fordi det er lite tvilsomt at forholdet faller innenfor PCPD og FTCs kompetanse og jurisdiksjon.

Under sin Appfail-kampanje fant Forbrukerrådet også ut at Vipps sendte data til Facebook. Vi valgte å undersøke dette nærmere overfor DnB. Det viste seg at DnB benyttet Facebooks såkalte Custom

Audience tjeneste, som innebar at visse opplysninger ble sendt fra Vipps til Facebook. DnB fjernet denne koblingen til Facebook etter at vi tok opp saken.

Internasjonalt arbeid

Vi lanserte «Det store datakappløpet» internasjonalt på den årlige personvernkonferansen CPDP i Brussel i januar 2016. Der avholdt vi en paneldebatt med engasjerte og gode innledere fra IAB Europe (interesseorganisasjon for annonseindustrien), Microsoft, BEUC (den europeiske forbrukerorganisasjonen), Universitetet i Amsterdam og det nederlandske datatilsynet. Vi holdt selv hovedinnlegget. Møtet ble godt besøkt og både møtet og rapporten fikk svært god mottagelse.

Vi har etablert tett kontakt med European Data Protection Supervisor (EDPS), som er EUs ombudsmann for personvern, og den europeiske forbrukerorganisasjonen BEUC. Det norske Datatilsynet er blitt anerkjent for å være blant tilsynsmyndighetene i Europa som har størst kompetanse på spørsmål knyttet til Big Data og den digitale data-økonomien. Datatilsynet var blant annet invitert med som paneldeltager i en større konferanse EDPS og BEUC arrangerte i Brussel om forbruker- og personvern i digitale tjenester. EDPS har tatt initiativ til å etablere et såkalt «digital clearing house» som skal være en møteplass for personvern- og forbrukermyndigheter i Europa der de kan diskutere felles problemstillinger og følge opp konkrete saker. Datatilsynet har takket ja til å delta i dette prøveprosjektet.

Vi har også presentert «Det store datakappløpet» for Artikkel 29-gruppen, Berlin-gruppen, GPEN (internasjonalt nettverk for personvernmyndigheter) og ICPEN (internasjonalt nettverk for forbrukerombud). Vi har dessuten delt vår kunnskap om personvernutfordringer i medie- og annonseindustrien med det tyske og franske konkurransetilsynet som har skrevet en felles rapport om dette markedet.

Stor foredrags- og informasjonsaktivitet

Interessen for «Det store datakappløpet» har vært stor. Vi har vært invitert til en lang rekke konferanser og møter med bransjeaktører for å gjøre innholdet i rapporten kjent.

Fremtidige utfordringer

Innsamling og bruk av personopplysninger til kommersielle formål vil øke i årene som kommer. Personalisering av tjenester får fotfeste i sektor etter sektor. Det blir en viktig utfordring fremover å styrke borgerens kontroll over egne data. Virksomhetene må bli flinkere til å informere tydelig om hvilke opplysninger de samler inn, hvor lenge de blir lagret og hvordan de behandles. Det skal være lett for folk å be om innsyn og å få sine data slettet hvis de ønsker det. Opplysninger som samles inn og brukes til profilering bør lagres så kort som mulig. Jo mer data som lagres, jo mer omfattende og detaljerte profiler er det mulig å lage. Den nye forordningen gir nye og viktige rettigheter til forbrukeren, blant annet rettigheten til dataportabilitet. Datatilsynet vil jobbe for at virksomheter utvikler løsninger som på en enkel måte lar brukeren ta med seg data fra en tjeneste og laste dem opp i en ny.

Neste år vil vi særlig se på hvordan personopplysninger samles inn og brukes til profilering i dagligvarehandelen og innen finans- og forsikringsbransjen.

I januar 2017 la EU-kommisjonen frem forslag til ny ePricacy-regulering. Dagens direktiv foreslås erstattet av en forordning for å få best mulig harmonisering med personvernforordningen. I forslaget til ny regulering er loven utvidet til også å omfatte såkalte «over-the-top»-tjenester som for eksempel Skype og Facebook messenger. EU-kommisjonen foreslår også at håndhevingen av

regelverket legges til den nasjonale datatilsynsmyndigheten. Hvis forslaget fra kommisjonen godkjennes vil Datatilsynet altså bli tillagt håndhevelse av dette regelverket fra 2018.

Barn, skole og utdanning

Dette er et felt vi ikke har prioritert høyest, men som det er stor interesse omkring. Vi ser en gradvis økning i interessen for barns personvern. Vi har i meldingsåret gjennomført flere aktiviteter som har oppstått som en direkte følge av vårt prosjektarbeid knyttet til personvern i barnehage og skole i tidsrommet 2013-15. Eksempler på dette er våre tilsyn om sterk autentisering. Noen interessante nye tema innenfor denne sektoren har også dukket opp, slik som for eksempel læringsanalyse.

Gjennomførte aktiviteter

Tilsyn

I 2015 behandlet vi flere saker som underbygde kravet vårt om sterk autentisering for ansattes innlogging på læringsplattformer. I en av sakene hadde en elev skaffet seg tilgang til sin lærers brukernavn og passord til læringsplattformen. Dette ga ham også tilgang til skoleadministrativt system hvor han endret på sine egne og andres karakterer.

I etterkant av disse sakene ble det startet et arbeid for å tilby sterk autentisering via FEIDE som er en løsning for sikker identifisering). En slik løsning var klar høsten 2016, og vi valgte derfor å spørre skoleeiere om de hadde tatt i bruk løsningen. Kontrollene medførte at samtlige ti skoleeiere på pålagt å etablere sterk autentisering.

Sentrale høringsuttalelser

Kunnskapsdepartementet har hatt flere store lovarbeider på høring i 2016 som Datatilsynet har hatt synspunkter til. Vi ønsker å trekke frem disse høringsuttalelsene:

Forslag til endring av barnehageloven og rammeplan

Kunnskapsdepartementet la i 2015 frem et forslag til endringer i barnehageloven. Endringene skulle blant annet gjøre barnehageeiers hjemmel for å behandle personopplysninger om barna tydeligere.

Vi leverte en kritisk høringsuttalelse hvor vi påpekte at endringen som foreslås er en utvidelse og omdefinering av hva barnehagens arbeid med dokumentasjon består av. Vi mente at endringen som ble foreslått ville legge til rette for å innføre en utstrakt måling og sammenligning av barnas ferdigheter. En slik måling har det ikke har vært tradisjon for i barnehager i Norge.

Vi var glade for å registrere at Stortinget var enige med oss, og regjeringen ble bedt om å komme tilbake til Stortinget med et forslag som ikke la til rette for en utvidet dokumentasjonspraksis.

På denne bakgrunn ble vi overrasket over at Kunnskapsdepartementet i sitt forslag til ny forskrift for rammeplan for barnehager har brukt lignende formuleringer som de som ble nedstemt i Stortinget. I vår høringsuttalelse minner vi om at det er forventet at Regjeringen følger opp Stortingets vedtak og kommer med en ny lovtekst før denne kan detaljeres i forskrifts form.

Skikkethetsvurdering i høyere utdanning

Noen ganger kan en student være uskikket for jobben han eller hun utdanner seg til. En skikkethetsvurdering er en kontroll av om en person har de faglige og personlige egenskapene som skal til for å kunne utføre et bestemt arbeid. «Begrunnet tvil» om en student er skikket, er et vilkår for å sette i gang vurderingen (Forskrift om skikkethetsvurdering i høyere utdanning §2). Da Kunnskapsdepartementet i 2016 foreslo noen endringer i forskrift om skikkethetsvurdering hadde Datatilsynet noen merknader.

Vi bemerket at den innrapporterte studentens rett til informasjon og innsyn så ut til å være godt ivaretatt fra det tidspunkt det besluttes å gjøre en skikkethetsvurdering, men det er ikke like tydelig hvilken informasjonen studenten får om det er kommet inn en tvilsmelding om vedkommende, og hvilken informasjon som blir gitt dersom beslutningen blir å ikke gå videre med en skikkethetsvurdering.

Vi påpekte at det er vanskelig å vite hvilke personopplysninger som vil bli behandlet i slike skikkethetsvurderinger. Universitetene og høyskolene må ta høyde for at de vil kunne motta sensitive opplysninger om mulige straffbare forhold knyttet til konkrete personer. I så fall må kanalene som rigges for dette være beregnet på å behandle sensitive personopplysninger.

En sak Datatilsynet fikk inn i meldingsåret aktualiserte nettopp disse problemstillingene. Saken omhandlet dårlig informasjonssikkerhet i behandlingen av en students skikkethetsvurdering. Det aktuelle universitetet fikk et overtredelsesgebyr på 75 000 kroner.

Øvrige aktiviteter

Deltakelse i arbeidsgruppe om læringsanalyse

Standard Norge og Senter for IKT i utdanningen har tatt initiativ til en arbeidsgruppe som jobber med problemstillinger knyttet til bruk av læringsanalyse i norsk skole. Her er personvern en sentral del av arbeidsgruppens drøftinger og Datatilsynet er representert. Gjennom meldingsåret har det vært innledende møter hvor ulike tema har vært drøftet (eierskap til data, dataportabilitet, åpenhet om algoritmer og lignende) men foreløpig har gruppen ikke produsert noe skriftlig.

Arbeidsgruppen vil fortsette sitt arbeid i 2017 og Datatilsynet skal fortsatt være representert. Det er et mål å produsere etiske retningslinjer for bruk av læringsanalyse.

Arbeid for å få på plass en norm for godt personvern i skoler og barnehager

Etter tilsynene i opplæringssektoren i 2013 og 2014, tok vi til orde for at det måtte tas grep når det gjelder hvordan virksomhetene innen sektoren veiledes i etterlevelse av personvernregelverket. Vi ser det fremdeles som nødvendig at det lages veiledningsmateriell som er vel forankret hos aktørene, og vi mener at en norm for sektoren er riktig vei å gå. Et viktig steg i positiv retning ble tatt i september 2015 da Kunnskapsdepartementet ga Utdanningsdirektoratet og Senter for IKT i utdanningen i oppdrag å koordinere eksisterende veiledningsmateriell. Dette har i meldingsåret resultert i www.personvernskolen.no.

Normtanken er imidlertid noe som aktørene i sektoren enda ikke har omfavnet. Det har vært holdt møter i meldingsåret med sentrale aktører, og Datatilsynet benytter blant annet slike anledninger til å promotere norm som en måte å arbeide på.

Samarbeidsprosjektet «Du Bestemmer»

Du Bestemmer er en læringsressurs som ble startet opp i 2007, og som vi driver i samarbeid med Senter for IKT i utdanningen. Målet med opplegget er å øke barn og unges kunnskap om personvern og digital dømmekraft, og heve deres bevissthet om valg de gjør ved bruk av digitale medier. De unge skal lære seg å ta kontroll over egne personopplysninger, men samtidig respektere andres opplysninger.

Det kommer jevnlig inn bestillinger på hefter fra hele landet, og nettstedet er svært godt besøkt. Opplegget benyttes ikke bare i skoler, men også av politi, helsepersonell, frivillige organisasjoner,

bibliotek, foreldrerepresentanter, til konformasjonsundervisning og lignende. Dette arbeidet genererer også mange henvendelser om å holde foredrag, samt pressehenvendelser om tematikken.

Fremtidige utfordringer

Vi er nok ikke helt der at alle skoleeiere har den nødvendige bevisstheten som skal til for å ivareta elevenes personvern på en tilstrekkelig måte. Vi er imidlertid på god vei når vi opplever både at de ansvarlige myndighetene for sektoren tar ansvar og at skoleeierne tar kontakt i forkant av et planlagt innkjøp av for eksempel informasjonssystemer med et ønske om å gjøre ting rett. Også utviklere av programvare tar kontakt og ønsker å tilby produkter som kan skilte med innebygd personvern.

Det at vi har foreslått at opplæringssektoren arbeider frem en norm for godt personvern, gjør at vi mener vi har satt i gang et arbeid som krever en viss oppfølging. Sektoren har nå tatt tak i deler av dette ved arbeidet med å koordinere eksisterende veiledningsmateriell, men det er enda et godt stykke igjen før aktørene selv sørger for at det lages veiledningsmateriell som er vel forankret i sektoren.

Målet med norm for godt personvern i skolen er at skoleeiere skal gå i takt og stille de samme kravene til leverandører av informasjonssystemer og applikasjoner.

Når det gjelder barn og unges personvern generelt, er det stor oppmerksomhet rundt dette – særlig i mediene. Det oppstår stadig nye områder der barns personopplysninger spres, og da gjerne uten deres samtykke, eller enda verre, kjennskap. Voksne i ulike roller som sprer bilder og annen informasjon på nett i ulike kanaler er en utfordring, og vi ser at veilednings- og opplysningsarbeid om barn og unges rettigheter vil være viktig også fremover. Barna skal tross alt ta ansvar for sitt eget personvern når de en dag får samtykkekompetanse, da er det en utfordring at de allerede vil kunne ha en svært detaljert digital profil på nett – definert av deres egne foreldre.

GPS-klokker er et eksempel der barns rett til personvern veies opp mot foreldrenes behov for kontroll, og der personvernet ofte taper. Slike måter å overvåke og kontrollere barn på, vil vi nok se stadig mer av fremover, og det blir stadig viktigere å fremheve Barnekonvensjonens artikler om rett til personvern og til å si sin mening og bli hørt.

Forordningen

Den store regelverksendringen som EU sin nye personvernforordningen fører med seg, har vært en betydelig oppgave for Datatilsynet i 2016 og vil også være det i årene som følger. Det nye regelverket ble vedtatt i april 2016 og skal implementeres i norsk rett 25. mai 2018. I perioden frem til ikrafttredelse må både Datatilsynet og virksomhetene som skal etterleve det nye regelverket forberede seg.

Arbeidet ble påbegynt i Datatilsynet i 2015 og intensivert i 2016. Vi har fulgt regelverksutviklingen hos EU meget tett, og vi har prioritert vår internasjonale tilstedeværelse. I tillegg har vi påtatt oss oppgaver i arbeidet med forordningen i EU-regi, for å være best mulig forberedt når forordningen trer i kraft.

Samarbeidet med de nordiske datatilsynsmyndighetene er også intensivert i forbindelse med dette arbeidet. Gjennom arbeidet som er gjort og møtene vi har hatt med våre søsterorganisasjoner i de nordiske landene, har vi sett at vi fra norsk side har kommet langt i arbeidet med forberedelsene til ny forordning. Vi har hatt mye kontakt med Island siden vi er i samme situasjon ved at ingen av landene er EU-medlemmer. Det har igjen betydd at kontakten med Danmark, Sverige og Finland har vært meget viktig, siden disse landene som medlemmer sitter nærmere det som skjer innenfor EU.

Datatilsynet deltar også, som eneste ikke departement, i en tverrdepartemental arbeidsgruppe som ledes av Justis- og beredskapsdepartementet, knyttet til implementeringen i norsk rett.

Vi har identifisert en rekke tiltak som må gjennomføres i perioden fram til forordningens ikrafttredelse 25. mai 2018. Noen av tiltakene er:

- Analysere konsekvenser av forordningen.
- Forberede behov for endringer i forvaltningspraksis.
- Bistå med regelverksutvikling, herunder høringsarbeid i forbindelse med endring av særlovgivning hjemlet i personopplysningsloven og andre lover vi fører tilsyn etter.
- Bistå departementet med spørsmål og oppgaver som faller på dem i forbindelse med implementeringen.
- Oppdatere vårt nettsted og informasjonen der.
- Utvikle organiseringen av personvernombudsordningen til å håndtere det nye regelverket.
- Kommunisere regelverksendringene til publikum og virksomheter.
- Tilpasse arkiv- og saksbehandlingssystem.
- Gjennomgå egen tilsynsmetodikk, og utarbeide nytt malverk.
- Økt samarbeid med andre lands personvernmyndigheter.
- Tilrettelegge for og gjennomføre egen kompetanseheving.

Digitalisere vår egen saksbehandling og vår kontakt med publikum, for å kunne håndtere forordningens nye krav og selvsagt for å bli en mest mulig digital etat i tråd med «Digital agenda».

Gjennomføringen av arbeidet med personvernforordningen er organisert i et prosjekt med fem delprosjekt. De fem delprosjektene er:

- **Nytt regelverk (juridisk).** Dette delprosjektet har ansvar for å vurdere hva det nye regelverk betyr for Datatilsynet. Det holder også i våre internasjonale forpliktelser og har kontakt med Justisdepartementet om dets arbeid med å innføre forordningen i norsk rett.

- **IKT og prosess-støtte.** Dette delprosjektet sørger for at vi har nødvendige og hensiktsmessige fagsystemer for å håndtere oppgavene våre etter nytt regelverk. Dette inkluderer gode løsninger for samhandling med eksterne parter og støtte i vår interne saksbehandling.
- **Kommunikasjonsprosjektet**. Delprosjektet skal håndtere de rene kommunikasjons-oppgavene knyttet til de nye reglene. Først og fremst skal prosjektet legge til rette for at både offentlige og private virksomheter får den informasjon de trenger for å kunne etterleve det nye regelverket og for at innbyggerne får informasjon om sine rettigheter.
- **Personvernombud**. I dette delprosjektet håndteres tilpasninger av personvernombuds-ordningen til det nye regelverket. Ordningen går fra å være frivillig til å være obligatorisk for alle offentlige virksomheter og den vil også pålegge langt flere private virksomheter å opprette personvernombud. Delprosjektet skal i tillegg til dette utrede og forstå hvordan den fremtidige opplæringen av personvernombud skal foregå.
- **WEB**. I dette delprosjektet håndteres nødvendige endringer av plattform, struktur og innhold på vårt nettsted.

Nærmere om arbeidet i delprosjektene

Juridisk

Arbeidet med å gå gjennom og fortolke forordningsteksten del for del er påbegynt og for noen områder også avsluttet. Dette er et omfattende og meget viktig arbeid som danner grunnlaget for våre anbefalinger til Justis- og beredskapsdepartementet, for vår internopplæring, for de endringer som er påkrevd i våre arbeidsprosesser, og for all ekstern kommunikasjon vi må gjennomføre i tilknytning til at et nytt regelverk innføres.

Innenfor det juridiske området er det også jobbet mye internasjonalt. Det er viktig for oss å delta så nært det som skjer innenfor EU/EØS som mulig, både for å vise at vi kan og ønsker å bidra og for å kunne lære og forstå det nye regelverket best mulig. Vi har også sett at det er naturlig og nødvendig å samarbeide tett med våre nordiske kolleger da vi stort sett har de samme utfordringene og problemstillingene. Gjennom et slikt samarbeid kan vi utnytte ressurser og kompetanse på tvers innenfor Norden på en god og effektiv måte.

IKT

Det viktigste vi har jobbet med og gjennomført i dette delprosjektet, er tilknytning til og å ta i bruk offentlige fellesløsninger slik som Altinn, ID-porten og Sikker Digital post. Vi har også gjort tilpasninger i vårt eget saksbehandlingsverktøy for å effektivisere vår måte å jobbe på. Innføringen av det nye regelverket vil kreve av vi lærer oss nye måter å jobbe og saksbehandle på, derfor er det veldig viktig for oss at vi tar i bruk nye, moderne og digitale verktøy for å bygge denne endringen med.

Personvernombudsordningen

Arbeidet med å fortolke og forstå hvilke krav forordningen stiller til opprettelse av personvernombud har stått sentralt her. Det er ingen tvil om at dagens frivillige ordning blir erstattet av en obligatorisk ordning som vil bety at antallet ombud vil stige betraktelig. Vi har derfor satt i gang et arbeid med å kartlegge mulighetene for å finne samarbeidspartnere innenfor universitets- og høgskolemiljøene for å kunne gi kvalifisert opplæring til både eksisterende og alle nye personvernombud. Det er også startet opp et samarbeid med Brønnøysundregistrene for å se på hvordan det er mulig å bygge opp et register med oversikt over virksomheter med personvernombud.

Kommunikasjon og opplæring

Det er utarbeidet planer for opplæring av Datatilsynets ansatte for samtlige deler av det nye regelverket. Det er også utarbeidet planer for eksternkommunikasjon både i forhold til innhold og til kanaler. Vi har innledet samarbeid med interesseorganisasjoner som IKT-Norge, KS, KINS og andre for å finne arenaer for å informere om forordningen og for å rekruttere «agenter» som kan hjelpe oss med å spre det budskapet som vi ønsker.

WEB

Vårt eget nettsted er og skal være hovedkilden til god, oppdatert og korrekt informasjon om det regelverket vi forvalter. Det er også viktig at vi klarer å gjøre dette nettstedet så godt at våre brukere også ser dette som hovedkilden når de skal søke informasjon om eller fra Datatilsynet. Når regelverket endres og vi blir ytterligere digitale i vår måte å jobbe på, fordrer det at vi har et moderne, effektivt og meget godt oppdatert nettsted. Vi har startet et arbeid med å oppdatere og modernisere nettstedet slik at vi skal møte disse utfordringene på en best mulig måte.

Fremtidige utfordringer

Arbeidet vi har startet og står midt oppe i, med å bidra til en god og effektiv innføring av og overgang til nytt regelverk, er selvsagt krevende både faglig og ressursmessig. Det er viktig at vi samtidig som vi gjennomfører prosjektaktiviteter, intern opplæring og endrer vår måte å jobbe på, også holder en daglig drift etter gjeldende lovverk på normalt nivå. Dette krever meget stram og god ledelse med svært god oversikt og tydelige prioriteringer.

Til syvende og sist er det virksomhetene, private og offentlige som skal etterleve det nye regelverket. Selv om vi i Datatilsynet gjør det som er mulig innenfor våre rammer, vil det være elementer som skal sikre etterlevelse som står utenfor vår kontroll. Dette vil være aktiviteter som sektorene, virksomheten og Regjeringen må sørge for at skjer.

På reguleringssiden må det tas stilling til om områder som i dag er regulert i personopplysningsloven med forskrift, men som ikke har noen regulering i den nye forordningen, fortsatt skal ha en særregulering. Sektorer og bransjer må ta sitt ansvar for å møte de nye regelverkskravene. Bransjenormen er sett på som et viktig instrument for etterlevelse, og det krever handling særlig fra bransjeorganisasjonene. Krav om innebygget personvern og vurderinger av personvernkonsekvens forutsetter kunnskap og handling hos ansvarlige, leverandører og organisasjoner.

Kort oppsummert forutsetter en vellykket innføring av personvernforordningen vesentlig større aktiviteter enn det som skjer i regi av Datatilsynet.

Annen vesentlig aktivitet

Arbeidsliv

Arbeids- og oppdragsgivere behandler store mengder personopplysninger om ansatte, innleide, kunder og tredjepersoner. Målt i antall henvendelser Datatilsynet mottar, er problemstillinger knyttet til arbeidslivet det desidert største fagfeltet. Sektoren har ikke hatt hovedprioritet i 2016, men det er likevel gjennomført flere aktiviteter og det har blitt behandlet et relativt høyt antall saker.

Saksbehandling og nemndsavgjørelser

I meldingsåret endte ni arbeidslivsrelaterte saker med overtredelsesgebyr i størrelsesorden 50 000 – 100 000 kroner. Tre av sakene har blitt påklaget til Personvernnemnda. Sakene gjaldt alt fra ulovlig innsyn i e-post, kameraovervåking på arbeidsplassen, samt sammenstilling av GPS-data og timelister.

I meldingsåret fattet Personvernnemnda vedtak i ti klagesaker innenfor fagfeltet arbeidsliv. I halvparten av sakene gjaldt klagen tilsynets vedtak om å ilegge overtredelsesgebyr, samt størrelsen på overtredelsesgebyret. Personvernnemnda fant ingen grunn til å fjerne eller endre på overtredelsesgebyrets størrelse i noen av sakene.

Øvrige aktiviteter

Arbeidstilsynet, Skatt øst, Politi (UP), Statens vegvesen og Datatilsynet sto samlet på felles stand på Transport 2016 på Norges Varemesse i Lillestrøm. Hovedtemaet under messen var miljø, sikkerhet og kompetanse. Messen hadde over 11 200 besøkende.

Datatilsynet har i samarbeid med Arbeidstilsynet, Petroleumstilsynet og partene i arbeidslivet arbeidet med en ny veileder om kontroll og overvåking i arbeidslivet. Prosjektet ble startet i 2015 og veilederen blir trolig publisert i begynnelsen av 2017.

Arkivhensyn versus personvernhensyn

Datatilsynet registrerer at det jevnlig dukker opp saker hvor arkivhensyn og personvernhensyn står steilt mot hverandre. Det er for så vidt ikke noe nytt, men vi ser at denne motstriden viser seg i nye former etter hvert som det offentlige tar i bruk nye digitale verktøy og det legges til rette for akkumulering av mer informasjon enn det som har vært mulig med tradisjonelle IKT-verktøy.

Arkivloven er teknologinøytral og fastslår at alt som kan betegnes som dokumenter, og som blir til som et ledd i den virksomheten organet driver, skal arkiveres. Dette er en ordlyd som legger opp til en innsamling av personopplysninger uten begrensninger begrunnet i personvernhensyn. Samtidig har vi eksempler på at det i fortolking av særlovgivning er slått fast at det å lagre dokumentasjon i form av film, bilder og lydbåndopptak av privatpersoner og/eller deres private hjem kan være å anse som inngrep i den private rettssfære som krever samtykke eller klar lovhjemmel. Et slikt eksempel har vi i barnevernlovgivningen.

Datatilsynet er oppmerksom på disse problemstillingene og adresserer dem i høringssvar, eksterne arbeidsgrupper vi deltar i og i møter med Riksarkivet.

Bank, forsikring og finans

Bank-, finans- og forsikringsbransjen behandler personopplysninger om de fleste. I sum er det tale om store mengder opplysninger, til dels av sensitiv og privat karakter. Bransjen leverer tjenester som

er viktige for den enkelte og samfunnet som helhet. Som følge av digitalisering er bransjen i endring, noe som kan føre til nye måter å drive virksomhet på og nye aktører.

Sektoren har ikke vært prioritert område for 2016, men vi har mottatt og fulgt opp mange saker.

I løpet av 2016 registrerte Datatilsynet over 200 saker/henvendelser fra sektoren. Sakene omfattet blant annet konsesjonssøknader, avviksmeldinger og klager. Disse har fortløpende blitt fulgt opp i henhold til vanlige rutiner. Vi har videre hatt veiledningssaker og vi har gitt innspill i forbindelse med høringer.

Vi må særlig nevne at vi har behandlet to konsesjonssøknader fra forsikringsselskaper om registering av kjøreatferden til kunder som ledd i bilforsikring. Kjøreatferden blir registrert ved hjelp av utstyr som monteres i bilen eller ved hjelp av mobiltelefonen. Vi fant at selskapene opptrer innenfor regelverket og ga tillatelse. Vi har i tillegg mottatt ytterligere en søknad, som vil bli ferdigbehandlet i 2017.

Det som kjennetegner sakene er at digitaliseringen gir muligheter for å samle inn mer informasjon om kunden, noe som gir grunnlag for andre risikoberegninger, mer prisdifferansiering og nye forretningsmuligheter. Prisen kunden må betale for en avtale som kan være rimeligere rent økonomisk, er et større inngrep i privatlivet. Selv om det er et individuelt valg for den enkelte, kan det spørres om vi som samfunn er tjent med en slik utvikling.

Biometri og ID

I løpet av meldingsåret har vi sett at det fremdeles er en stor interesse for bruk av biometri. Biometri blir ofte sett på som en løsning for å bli kvitt passord som er vanskelige å huske, samt å sikre at det er rett person som gis for eksempel en tilgang. I 2016 har det vært en ytterligere økning av bruken av biometri i forbindelse med enkel tilgang til mobiler og PC-er. Utstyret har fingeravtrykk som preferert teknologi, men bruk av iris er tatt i bruk på PC-er og mobiler.

Datatilsynet er etterspurt som deltaker og diskusjonspartner av mange av de som jobber med og har ansvar for dette området. Dette betyr at vi er på de arenaene der slik spørsmål diskuteres, det være seg hos de forskjellige i politiet, i Justis- og beredskapsdepartementet eller hos NorSIS, som alle jobber med dette. I 2016 ble det fastslått at biometri ikke skal inn i Folkeregisteret, men at Folkeregisteret kan vise til at det er andre registre som har biometri på vedkommende.

Den internasjonale personverndagen

For fjerde året på rad markerte Datatilsynet den internasjonale personverndagen med et personvernseminar og utgivelse av en egen rapport i samarbeid med Teknologirådet. Årets tema var «overvåkingsøkonomien» og fant sted på Litteraturhuset i Oslo den 28. januar. Arrangementet ble raskt fullbooket med 200 deltakere.

Det ble gjort en befolkningsundersøkelse om folks holdninger til kommersiell sporing på nett i forbindelse med arrangementet. Rapporten beskriver også de teknologiske trendene og forretningsmodellene bak overvåkingsøkonomien, og beskriver personvernutfordringene knyttet til denne. Arrangementet ble avsluttet med en paneldebatt med statssekretær Paul Chaffey fra KMD, Ingvild Næss fra Schibsted og Erik Kristiansen fra MediaCom.

Droner

Droner har de siste årene aktualisert seg som en personvernproblemstilling, og dronemarkedet har hatt en stor vekst. I første fase er utfordringene knyttet til bruk av kamera på droner av blant andre privatpersoner og eiendomsmeglere. Andre og større personvernutfordringer kommer imidlertid når droner tas i bruk til andre formål, særlig overvåking og bruk av ulike sensorer. Problemstillinger er økt overvåking, manglende informasjon og innsamling av overskuddsinformasjon. Datatilsynet har prioritert å være i dialog med bransjeorganisasjoner og myndigheter for å kommunisere personvernutfordringer. I meldingsåret har vi oppdatert vår veiledning, kommunisert vurderinger fra Artikkel 29-gruppen og Berlin-gruppen om droner, og bidratt til at andre aktører videreformidler vårt veiledningsmateriale.

Forskning og utvikling

Formålet med Datatilsynets satsing på forsknings- og utviklingsarbeid, er å gjøre oss selv bedre til å sette personvernhensyn inn i en samfunnsmessig kontekst, og til å fange opp trender og utviklingstrekk på et tidlig stadium. I tillegg ønsker vi å stimulere og støtte personvernrelevant forskning som kan gi positive samfunnsmessige ringvirkninger.

Partner i NTNU CCIS

Datatilsynet er siden 2015 partner i NTNU CCIS (Center for Cyber and Information Security). NTNU CCIS innehar Norges største akademiske fagmiljø innen informasjonssikkerhet. Vi vil gjennom partnerskapet med CCIS bidra til at hensynet til personvern blir vektlagt i forskningsprosjekter om cyber- og informasjonssikkerhet, og ved utvikling av nye sikkerhetsløsninger. Samarbeidet innebærer også en betydelig satsing på prosjekter med personvern som fagfelt. Datatilsynet sitter i styret til CCIS Education Advisory Board (EAB), som gir tilsynet mulighet til å påvirke innholdet i studieplaner og undervisningsopplegg. Den viktigste begivenheten i 2016 var ansettelsen av professor Staal Vinterbo i et professorat dedikert til personvernspørsmål. Vi ser frem til et tett og nært samarbeid med professor Vinterbo og hans studenter i tiden fremover.

Forskningsprogrammet Secure Societies

Datatilsynet deltar i referansegruppen for forskningsprogrammet «Secure societies – Protecting freedom and security of Europe and it's citizens», som går i regi av Forskningsrådet.

Forskningsprogrammet er en del av et omfattende forsknings- og innovasjonsprogram i EU, kalt «Horizon 2020». Også norske aktører kan søke om midler til forskning og innovasjon. Underdelen «Secure societies – Protecting freedom and security of Europe and its citizens» handler om forsknings- og innovasjonsaktiviteter for å beskytte borgere, samfunn og økonomi, samt infrastrukturer og tjenester, velstand og politisk stabilitet. Det ble avholdt ett møte i referansegruppen i 2016 der Datatilsynet dessverre var forhindret fra å delta.

Forskningsprosjekt om crowdsourcing

Vi er representert i referansegruppen til forskningsprosjektet «Social Responsible Crowdsourcing for Environmental Research and Decision» (iResponse). Prosjektet ble etablert i 2015. Flere forskningsinstitutter samarbeider om å utvikle såkalte crowdsourcing-verktøy knyttet til byplanlegging, forurensing og miljø. Prosjektet finansieres av Forskningsrådets program SAMANSVAR, som legger særlig vekt på ansvarlig innovasjon og Corporate Social Responsibility (CSR). Ivaretakelse av personvernhensyn er selvsagt viktig ved utvikling av slike verktøy. I 2016 deltok vi i en workshop og bidro til en artikkel om ivaretakelse av personvern ved bruk av crowdsourings-verktøy i forskningssammenheng.

Bistand til mastergradsstudenter

Vi har stilt vår kompetanse til rådighet for flere mastergradsstudenter som ønsket å skrive om personvern og vi har kommet med forslag til mastergradsoppgaver. Vi har blant annet arrangert et møte med studenter fra Senter for rettsinformatikk (SERI) for å informere hverandre om interessante problemstillinger og tema vi er engasjert i.

Internettsveipet

Datatilsynet sjekket personverninformasjonen i seks hjemmetestprodukter koblet opp mot smarttelefon. Produktene målte blodtrykk, blodsukker (typisk brukt av diabetikere) og såkalte oksymeter/pulsoksymeter som måler oksygenmetning i blodet og puls (aktuelt for kolspasienter). Vi har sett på produkter som er lett tilgjengelig for norske forbrukere. Kartleggingen, eller «sveipet» som vi kaller det, er del av et internasjonalt samarbeidsprosjekt med 25 deltakende tilsynsmyndigheter.

Vi har funnet varierende og i hovedsak for dårlig personverninformasjon på de seks produktene vi testet:

- Fem av seks produkter får stryk fordi de ikke forklarer hvordan personopplysningene blir samlet inn, brukt og delt på en tilfredsstillende måte.
- Fire av de seks produktene hadde ingen personvernerklæring.
- Det var varierende kvalitet på informasjon fra produkt til produkt. Resultatene spenner fra ingen informasjon til en del relevant og god informasjon.
- Ingen av produktene forklarte på en god måte hvordan personopplysningene til brukeren blir lagret.
- Ingen av produktene forklarte hvordan brukerne kan slette egne personopplysninger.

Det er enkelt å komme i gang, installere apper, ta tester og å lese av resultater. Det er imidlertid vanskelig for brukeren å finne informasjon om hva som skjer med personopplysningene. Selvråderett er et viktig prinsipp i et godt personvern, og informasjon er en forutsetning for bevisste valg.

Hovedinntrykket fra både det norske og det internasjonale sveipet gir grunn til ettertanke – Du kan ikke nødvendigvis regne med å få forståelig og dekkende informasjon om bruk av personopplysninger når du kjøper «smarte» produkter som kommuniserer via internett.

Kameraovervåking og kamerateknologi

I meldingsåret var kameraovervåking det temaet som var oftest besøkt på våre nettsider. Mange av henvendelsene kommer fra personer som føler seg urettmessig overvåket, men også fra virksomheter som ønsker råd og veiledning i tilknytning til planlagt kameraovervåking.

Vi gjennomførte fire stedlige kameratilsyn i løpet av 2016 innenfor velværebransjen, butikkbransjen og callsenter-bransjen. Disse bransjene ble valgt på bakgrunn av mottatte tips. Tre av tipsene kom fra ansatte i virksomheter som benyttet seg av overvåkingskameraer. På to av disse var det også grunn til å gjøre et parallelt tilsyn med Arbeidstilsynet.

Datatilsynet fortsatte i 2016 arbeidet med kameraovervåking i det offentlig rom. Dette innebærer oppfølging av de store tilsynene som ble gjennomført i 2015, samt å utarbeide veiledningsmateriell spesielt rettet mot kommuner og politi.

Datatilsynet har i 2016 sett en stadig økende bruk av ny kamerateknologi i ulike bransjer, mye grunnet nye internettbaserte løsninger. Spesielt har spørsmål rundt bruk av flyvende droner med kamera reist flere problemstillinger som vi har tatt opp i ulike fora. Vi ser derfor et behov for å følge droneutviklingen konkret i 2017. Som et ledd i prosjektet «sporing i det offentlige rom» har vi dessuten gjennomført ett tilsyn som gjelder intelligent videoanalyse. Dette arbeidet videreføres til 2017.

Etter en gjennomført forskriftsendring i 2016 falt meldeplikten til Datatilsynet for kameraovervåking bort med virkning fra 01.01.2017.

Kredittvurdering

De fleste nordmenn vil oppleve å bli kredittvurdert én eller flere ganger i løpet av livet. En kredittvurdering inneholder mange opplysninger om vår økonomiske situasjon, og mange vil oppleve at disse opplysningene har en stor grad av beskyttelsesverdighet. Videre utfører kredittopplysnings-virksomhetene automatiserte analyser av sannsynligheten for at vi vil misligholde våre økonomiske plikter.

I 2016 har Datatilsynet behandlet flere saker som gjaldt innhenting av kredittvurdering i strid med loven. I disse sakene var det viktig for oss at personvernkrenkelsen dette utgjorde, ble behandlet på linje med andre, tilsvarende krenkelser. Derfor ila vi flere overtredelsesgebyr. Vi har også hatt dialog med kredittopplysningsbransjen om praktiske utfordringer, analysemodellene og den kommende personvernforordningen.

Kryptering av datasentertrafikk

I 2016 fortsatte vi vårt arbeid med å kontrollere virksomheter som leverer datasentertjenester. Vi behandlet de sakene som var påbegynt i 2015, og vi gjennomførte fem nye kontroller i 2016 som fortsatt er under behandling. Formålet med samtlige kontroller var å undersøke om det var etablert kryptering av kommunikasjonen mellom leverandørers datasentre, og mellom kunde og datasenter. Der det har vært mangelfullt, har vi gitt pålegg til leverandører om å implementere kryptering av kommunikasjon mellom sine datasentre. Vi har også gitt pålegg om at leverandører skal gjennomføre planlagte og systematiske tiltak for å forsikre seg om at kommunikasjon mellom behandlingsansvarlig og datasenter er kryptert. Det siste er en internkontrollplikt for å sørge for at hvis en databehandler vet at det kommuniseres beskyttelsesverdig informasjon, skal kommunikasjonen være kryptert.

Personvernombudsordningen

Ved utgangen av 2016 har Datatilsynet registrert 554 virksomheter med personvernombud. Det er en økning på 18 prosent siden starten av året da vi hadde registrert 470 virksomheter. 331 personvernombud representerer disse virksomhetene.

Vi opplever en økning i interessen for ombudsordningen i forbindelse med at det blir obligatorisk for mange virksomheter å ha ombud under den nye forordningen fra EU. Dette merker vi både i antall henvendelser vi får om ombudsordningen og antall påmeldte på kursene våre. Vi forventer en økning i antall nye ombud i tiden framover.

I 2016 har Datatilsynet arrangert grunnkurs for nye ombud, juridisk fordypningskurs og kurs om informasjonssikkerhet og internkontroll både høst og vår. I tillegg har vi hatt en egen fagdag for personvernombud innen helse og forskning, samt en konferanse for ombud med 130 deltakere. Vi har aldri hatt så mange deltakere på våre kurs og konferanser som i 2016. Snittet på antall deltakere på kursene våre har vært rundt 60. Vi har gjort brukerevalueringer av samtlige arrangementer og tilbakemeldingene er gode både faglig og knyttet til selve gjennomføringen.

Med den nye forordningen videreføres mye av det eksisterende opplegget rundt personvernombud i Norge, men det er også en del endringer. Datatilsynet har i 2016 startet forberedelsene til ny forordning for ombudene. Det har hovedsakelig bestått av tre hovedaktiviteter:

- Gi informasjon til eksisterende ombud om endringer med nytt regelverk gjennom kurs og konferanser, nyhetsbrev, foredrag og våre nettsider
- Lage nytt system for registrering av ombud
- Undersøke muligheter for eksterne kursopplegg for ombud og bidra til å utvikle disse

Publisering av personopplysninger på nett

Retten til å bli glemt

I 2016 har vi arbeidet aktivt for å oppnå en enhetlig etterlevelse av retten til å bli glemt, i tråd med andre EU-lands praksis. Vi har saksbehandlet samtlige reelle klager om avindeksering som vi har mottatt. Vi har utarbeidet interne retningslinjer for effektiv og enhetlig saksbehandling og kommunikasjon med søkemotorene, og vi har deltatt på fellesmøte med andre europeiske datatilsyn for å utveksle erfaringer og oppdatere retningslinjene fra Artikkel 29-gruppen. Retningslinjene er ikke endelig oppdatert av Artikkel 29-gruppen ved utgangen av 2016, men vi forventer at dette vil skje i løpet av 2017.

I 2016 mottok vi 31 saker om retten til å bli glemt. Dette er omtrent det samme antallet saker som vi mottok i 2014 og 2015 til sammen. Av de 31 sakene fra 2016 har tre fått avslag på klagen sin. I ni saker har klager fått medhold av oss og den aktuelle søkemotoren har fjernet søketreff. 19 saker er fortsatt under behandling.

Ratingsider

Vi har i meldingsåret arbeidet videre med saker som gjelder «ratingsider» på nett. Dette er sider der brukere rangerer personer innenfor et yrke eller innenfor annet kommersielt område. I 2015 kom Datatilsynet til at norskdrevne nettsider som behandler opplysninger og vurderinger om navngitte enkeltpersoner i utgangspunktet har behandlingsansvar for innholdet på siden, og må dermed følge personopplysningsloven. På bakgrunn av dette har vi i 2016 mottatt henvendelser knyttet nettsider som ratemyteacher.no, legelisten.no, minleietaker.no og hybelrating.no.

Sak – Hacking av politiske partier med lav sikkerhet

De to politiske partiene Sosialistisk Venstreparti (SV) og Miljøpartiet De Grønne (MDG) ble høsten 2016 varslet om overtredelsesgebyr for dårlig informasjonssikkerhet, en mangel som medførte at uvedkommende fikk tilgang til medlemsopplysninger. Begge de to partiene benyttet samme medlemssystem, og i løpet av juni 2016 ble de utsatt for en rekke angrepsforsøk. Inntrengeren klarte i begge tilfellene og ta over brukere for så å skaffe seg tilganger og rettigheter. Slik kom medlemsopplysninger på avveier.

Politisk oppfatning er definert som en sensitiv personopplysning i personopplysningsloven. Dette betyr at medlemsregisteret inneholder sensitiv informasjon som må sikres så opplysningene ikke kommer på avveier. Mangelfull sikring vil øke sannsynligheten for sikkerhetsbrudd. Det er viktig å sikre slike opplysninger godt og en sterk autentisering, ville trolig kunne forhindret hendelsene. Begge partiene får derfor gebyr for mangelfulle sikkerhetstiltak.

Samferdsel

Innen samferdselssektoren har vi særlig arbeidet med Intelligente transportsystemer (ITS), ikke minst på grunn av ITS-loven som legger til rette for flere tjenester på sektoren. Retten til å ferdes anonymt er en viktig rettighet, men den utfordres siden teknologiske løsninger hele tiden legger opp til å vite mer om den enkelte og hvor den enkelte er. Smarte byer og intelligente transportsystemer gir utfordringer for personvernet, og vi har i 2016 fortsatt arbeidet med ITS via samarbeid med andre etater, foredragsvirksomhet og veiledning. Arbeidet med regulering av selvkjørende biler har startet opp. Vi har også gitt råd i forbindelse med diskusjon om veiprising og etableringen av lavutslippssoner.

Sporing i det offentlige rom

Virksomheter tar i stadig økende grad i bruk teknologi som gjør det mulig å spore enkeltmennesker i det offentlige rom. I dette prosjektet har Datatilsynet skrevet en rapport om slike teknologier, med fokus på WiFi- og Bluetooth-sporing, nettvarder og intelligent videoanalyse. I rapporten har vi gjort rede for hvordan teknologiene fungerer, hvordan og i hvilken grad de brukes i Norge i dag og hva personvernkonsekvensene av teknologiene er. Dessuten har vi laget klare retningslinjer for hvordan virksomheter kan benytte sporingsteknologi i tråd med personopplysningsloven.

I tillegg til utadrettet kommunikasjon om emnet har Datatilsynet iverksatt kontroller mot virksomheter som benytter sporingsteknologier i det offentlige rom. Per desember 2016 hadde vi gjennomført tilsyn med henholdsvis WiFi-sporing, nettvarder og intelligent videoanalyse. Disse kontrollsakene avsluttes 2017. I 2017 vil vi også utføre nye tilsyn, fortsette kommunikasjonsvirksomheten om emnet og se nærmere på andre teknologier.

Telekommunikasjon

Arbeidet med å få oversikt over lagringen av personopplysninger innen telekom- og internettsektoren, fortsatte i 2016, og det har vært et godt samarbeid med Nasjonal kommunikasjonsmyndighet (Nkom).

Med bruk av smarttelefoner der mobilen mer eller mindre kontinuerlig sjekker e-post eller av andre grunner kobles opp mot internett, vil trafikkdata og signaleringsdata være informasjon som forteller noe om vår minste bevegelse hvert minutt i løpet av dagen. Våre bevegelser logges så å si kontinuerlig hele dagen og lagres i opptil 30 dager for de omfattende signaleringsdataene, og opp til tre måneder for trafikkdata. I tillegg til lokasjonsinformasjon logges også hvilken internettadresse du har benyttet til enhver tid. Dette sammen med informasjon om hvordan du benytter mobilen, er omfattende kunnskap om den enkelte av oss – dette er data vi mener det er unødvendig å logge bare for å fakturere oss eller for å få nettet til å virke.

I 2016 har vi sett at lagringstiden når det gjelder lokasjon har vært for lang, og en av teleoperatørene reduserte også denne betydelig. Det er grunnlag for å arbeide videre med dette temaet. Videre har det vært et fokus på etablering av lagring for å ivareta problematikken rundt Signaleringssystem 7. Dette arbeidet videreføres i 2017.

Vi ser også et omfattende skifte i teknologi på telekomsiden fra vanlig telekom til IP-baserte tjenester. Dette arbeidet gjør norske teleoperatører i det internasjonale samarbeidet i GSMA hvor blant andre Google er en sentral aktør.

Internasjonalt arbeid

Internasjonalt arbeid er viktig for Datatilsynet. Siden Norge ikke er medlem i EU, kan det være utfordrende å skaffe seg påvirkningsmuligheter inn mot EUs beslutningsprosesser. Målet for 2016 var å søke større synlighet på den internasjonale arenaen, og finne fora hvor vi kan være med og komme til orde. Vi har benyttet alle de fora vi er representert i til å søke oppmerksomhet.

Ettersom internasjonalt samarbeid blir stadig viktigere fremover med et harmonisert regelverk på personvernområdet, er det viktig for oss å ha et godt internasjonalt nettverk.

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

Artikkel 29-gruppen er opprettet i henhold til personverndirektivet, og er den øverste rådgivende forsamlingen for EU-kommisjonen i spørsmål om personvern og informasjonssikkerhet. Her møter alle lederne for EU-landenes datatilsynsmyndigheter. Norge har observatørstatus som EØS-land. Dette innebærer at vi kan delta og bidra med vår faglige kompetanse og gi innspill i møter og undergrupper, med uten stemmerett.

I 2016 har Datatilsynet deltatt med to representanter (en i ledelsen) på plenumsmøtene i denne gruppen. Det er holdt fem plenumsmøter i 2016, og Datatilsynet har vært representert på alle. I tillegg har vi hatt representanter i ulike undergrupper til Artikkel 29-gruppen. Datatilsynet har faste representanter i «Cooperation Subgroup» og «Technology Subgroup», men deltar også i undergruppen «Future of privacy» (avhengig av tema for diskusjon).

Technology Subgroup er en arbeidsgruppe som gjør saksforberedelser for Artikkel 29-gruppen. Disse forberedelsene danner grunnlag for mange av Artikkel 29-gruppens uttalelser. Vår deltakelse i arbeidsgruppen gir god mulighet til å fremme norske synspunkter innenfor spørsmål om bruk av teknologi og koblingen til juss og regelverk. Undergruppen diskuterer også konsekvensen av nye teknologier som påvirker personvernet, noe som er svært nyttig som informasjonskilde for oss. Vi benytter også anledningen til å fremme våre forslag inn i gruppen og deltar som co-rapportør i aktuelle grupper.

Future of Privacy Subgroup (FOP) er en annen undergruppe. Her foregår mange av diskusjonene om den nye forordningen. Vi er representert med en jurist, og har vært med på alle møtene som har vært holdt i 2016. Vi har også bidratt til utformingen av to sett med retningslinjer, om henholdsvis administrative sanksjoner og nasjonalt handlingsrom.

Året har vært preget av arbeidet med det nye felles europeiske personvernregelverket. Datatilsynet har vært medforfatter av to viktige uttalelser om felles europeisk tilsyn og administrative sanksjoner (overtredelsesgebyr) etter forordningen. I tillegg har vi utarbeidet saksflyttdiagrammer for samtlige former for samarbeid mellom tilsynsmyndigheter etter forordningen. Disse ble vedtatt i plenum og skal danne grunnlag for utvikling av det fremtidige IKT samarbeidsplattformen til EDPB og organisering av rutiner for samarbeid i medlemslandene.

Når det gjelder uttalelsen om overtredelsesgebyr, fortsetter samarbeidet med det britiske datatilsynet og EDPS (European Data Protection Supervisor, EUs ombudsmann for personvern), begge strategiske partnere for Datatilsynet i årene som kommer.

International Working Group on Data Protection in Telecommunications er også en undergruppe av Artikkel 29-gruppen. Denne gruppen tok i 2015 initiativ til å lage retningslinjer for personvern i læringsplattformer og andre digitale plattformer i skolen. Arbeidet har foreløpig resultert i et utkast til «Working Paper on the use of E-Learning Platforms in Primary and Secondary Education». Datatilsynet har bidratt til dette arbeidet i 2016 og følger opp videre i 2017.

Berlingruppen - International Working Group on Data Protection in Telecommunications (IWGDPT)

Berlingruppen er et internasjonalt fellesskap som arbeider med personvern innen elektronisk kommunikasjon i utvidet forstand. I det vesentlige er det personvernmyndigheter som deltar. Gruppen avgir uttalelser (Working Papers) om aktuelle personvernspørsmål.

Datatilsynet har over flere år vært en aktiv deltaker i Berlingruppen. Våren 2016 var vi vertskap for Berlingruppens møte i Oslo. I forbindelse med gruppens høstmøte i Berlin fremkom det forslag om å sette ned antall møter til ett i året. Gruppens fremtidige form er under diskusjon, vår strategi er å beholde to møter i året.

Den internasjonale personvernkonferansen (ICDPPC)

På den internasjonale personvernkonferansen (ICDPPC) i 2016 ble det vedtatt en resolusjon om internasjonalt rammeverk for personvern i utdanning. Datatilsynet har bidratt til resolusjonen med erfaringer fra arbeidet med Du bestemmer.

Eurodac og Visumsamarbeidet i Europa

Vi er fullverdig medlem av begge disse koordineringsgruppene. Møtene finner som regel sted samtidig, ettersom de to temaene er beslektet. Vi deltok på ett av møtene som ble avholdt i 2016.

Global Privacy Enforcement Network – GPEN

I tillegg til å delta i GPEN Privacy Sweep Day i mai (les under *Årets viktigste aktiviteter, Annen vesentlig aktivitet*), har Datatilsynet bidratt økonomisk til å etablere tjenesten GPEN Alert. GPEN Alert er et multilateralt varslings- og kommunikasjonssystem som gjør det mulig for datatilsynsmyndigheter å dele informasjon på tvers av grenser. Vi har også vært med å teste dette systemet, som er utviklet og drives av Federal Trade Commission (FTC) i USA.

Vi deltar jevnlig på «GPEN conference calls» der tilsyn fra hele verden deler erfaringer fra arbeidet sitt.

Samarbeid med de nordiske datatilsynsmyndighetene

Det nordiske datatilsynsmøtet ble i år avholdt på Island. Hovedtemaet var den nye forordningen. De nordiske datatilsynsmyndighetene har dessuten jevnlig kontakt, både i form av uformelle samtaler og på andre internasjonale arenaer. Den nye personvernforordningen er naturlig nok et tema som har gått igjen i 2016.

Schengen Coordination Group (SCG)

Vi er fullverdig medlem av Schengen-koordinasjonsgruppen som møtes i EU-parlamentet i Brüssel. Vi har deltatt på ett møte i 2016. I tillegg deltok en ekspert fra Datatilsynet i tilsynsteamet som inspiserte Schengen informasjonssystem i Italia i 2016. Vi planlegger også fremover å være med på kontroller av andre Schengen-land.

Nasjonale samarbeidsrelasjoner

Datatilsynet har utstrakt kontakt med andre aktører. Nedenfor følger en oversikt over vår mest sentrale deltakelse i nasjonale fora.

I tillegg til disse kommer det et stort antall kontaktmøter med sentrale aktører og samarbeid av mer kortvarig art. Datatilsynet har også avtaler om faglig samarbeid med Nasjonal Sikkerhetsmyndighet (NSM), Nasjonal kommunikasjonsmyndighet og Arbeidstilsynet.

Aktørforum e-signatur

Nasjonal kommunikasjonsmyndighet (Nkom) samler aktørene innen e-signaturområdet til aktørforum, hovedtema er Kommisjonens forslag til forordning om blant annet e-ID og e-signatur. Aktørforumet skal systematisere kontakten mellom aktørene. Datatilsynet har fulgt opp arbeidet i forumet.

Bransjenorm for sikkerhetsbransjen

NHO Service har tatt initiativ til å utarbeide en bransjenorm for sikkerhetsbransjen. Arbeidet med normen startet i 2015, og har fortsatte gjennom 2016. Datatilsynet er representert i arbeidsgruppen og i styringsgruppen.

ID-nettverket for en helhetlig ID-forvaltning

Datatilsynet deltar sammen med flere andre sentrale organisasjoner i dette nettverket. Hovedmålet til nettverket er å arbeide for en helhetlig ID-forvaltning i Norge, og for å forebygge kriminalitet for dermed redusere trusselen mot velferdsstaten. Datatilsynets deltakelse er viktig både for å ivareta personvernet i ID-forvaltningen, og for å bidra til at sikre løsninger etableres.

ITS-rådet (ITS – Intelligente Transport Systemer)

Én 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.

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 to representanter i referansegruppen, samt at vi har deltatt i enkelte møter i prosjektet. Vi har i 2016 jobbet særlig med ID-forvaltning og adresser i folkeregisteret. Problemstillinger knyttet til hvilke opplysninger som skal inn i folkeregisteret er noe vi jevnlig må forholde oss til. Datatilsynet er tilfreds med at det er slått fast i ny folkeregisterlov at biometri ikke skal inn i folkeregisteret.

Forumet «Stopp nettsvindelen»

Forumet drives av Norsk senter for informasjonssikring, NORSIS. Datatilsynet deltar sammen med flere andre sentrale offentlige og private organisasjoner i dette forumet. Det legges vekt på presentasjon av trender, metoder og fremgangsmåter som svindlere benytter, herunder identitetstyveri og svindel. Det fokuseres på erfaringsutveksling, tiltak og virkemidler.

Kommunal informasjonssikkerhet (KINS)

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

Medietilsynet Trygg bruk

Medietilsynet Trygg bruk er Norges Safer Internet Centre. De ønsker å hjelpe barn og unge til å få en tryggere og bedre digital hverdag. De samarbeider og utvikler ressurser med andre aktører både i Norge og internasjonalt. Datatilsynet deltar jevnlig på møter og arrangementer i regi av Medietilsynet Trygg Bruk.

Nasjonalt råd for Facilitation – NAFAL

Datatilsynet er oppnevnt med én 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.

Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren

I september 2006 ble en bransjenorm om informasjonssikkerhet for helsesektoren lansert. Datatilsynet deltar som observatør i styringsgruppen. Ved behov deltar vi også i grupper knyttet til utarbeidelse av faktaark og veiledninger etter normen. I 2016 startet vi diskusjonen om og hvordan Normen skal bli en bransjenorm etter personvernforordningen.

Norsk Biometri Forum

Datatilsynet deltar i Norsk Biometri Forum som er et uformelt forum for presentasjon og diskusjon innenfor biometri. Det er lagt stor vekt på å få inn nye ideer, samtidig som møtene 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 møtes omtrent to ganger i året, og har deltakere fra departementer, direktorater og en del private bedrifter, samt NTNU i Gjøvik. Dette forumet arrangeres i tett samarbeid med Forum for Research and Innovation in Security and Communications (FRISC) og European Association for Biometrics (EAB).

Norsk senter for Informasjonssikring (NorSIS)

Datatilsynet er representert i styret til NorSIS ved direktøren. Vi har mange overlappende ansvarsområder med NorSIS, og samarbeider derfor med dem om ulike tema, blant annet nasjonal sikkerhetsmåned.

Referansegruppe - Fulltekstpublisering av dokumenter i OEP

Datatilsynet er representert i referansegruppen for Fulltekstpublisering av dokumenter i OEP. Det er viktig for oss å delta i dette arbeidet for å fremme de personvernmessige prinsippene som gjør seg gjeldende ved innføring av fulltekstpublisering av dokumenter i OEP. Vi har erfart at det både er mangelfulle rutiner og risikovurderinger knyttet til de avvik tilsynet har mottatt på dette området, og at det er viktig at man ved innføring av fulltekstpublisering gjør en vurdering av risikoen ved at personopplysninger gjøres tilgjengelig på nett.

Samarbeidsprosjektet Du Bestemmer

Du Bestemmer er et prosjekt som drives i samarbeid mellom Senter for IKT i utdanningen og Datatilsynet, og som ble lansert i januar 2007. Målet med prosjektet er å øke ungdoms kunnskap om personvern generelt, samt heve deres bevissthet om valg de gjør ved bruk av digitale medier slik som

internett og mobiltelefon. Prosjektet driver blant annet en nettressurs som skal bidra til at barn og unge skal lære seg å ta kontroll over egne personopplysninger, men samtidig respektere andres opplysninger. Hele eller deler av dette opplegget er til nå tatt i bruk i over 20 andre land.

Standardisering – komitédeltagelse

Vi 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 deltakelsen 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.

Datatilsynet deltar 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.
- SN/K 186 Læringsteknologi

VURDERING AV FRAMTIDSUTSIKTER

De siste kalde vinterdagene i januar arrangeres hvert år Europas største personvernkonferanse. Uten at vi akkurat satt med ordtelleren, var det fire begreper som gikk igjen i nær sagt alle innlegg: Algoritmer, kunstig intelligens, automatiserte avgjørelser og ny personvernforordning. Det har vært snakk om alt dette i mange år. Ja, ordet algoritmer stammer faktisk fra den persiske matematikeren og astronomen Muhammad ibn Musa al-Khwarizmi (ca. 780 – 850) som laget en algoritme om hvordan en bestemt annengradsligning skulle løses.

Det som er nytt, er at algoritmer vil treffe beslutninger om svært viktige spørsmål i livene våre, kunstig intelligens vil finne sammenhenger vi ikke engang har fantasi til å tenke på og stadig flere avgjørelser vil treffes uten at en mann eller kvinne har sett på et eneste saksdokument. Og midt i alt dette: EUs nye personvernforordning som trer i kraft i Norge 25. mai 2018.

Vi står ved et veiskille nå. Digitalisering, økt tilgang på gode datasett, lavere pris på lagring og økt prosessorkraft trekkes ofte fram som noen viktige faktorer. Nesten daglig kan vi lese om bransjer som snus på hodet av nye aktører (som taxibransjen), og om leger som finner en unik behandling for svært sjeldne kreftformer ved hjelp IBMs Watson. Vi ser det også i nye, ganske så dagligdagse, tjenester. Algoritmer brukes til å gi mer presis beregning av forsikringspremier, slik at vi kan få rabatter dersom vi jogger, spiser sunt eller passer på å lade mobilen hver natt. Politiet i andre land tar i bruk algoritmer og kunstig intelligens for å finne ut hvor det vil begås forbrytelser, og enda verre, hvem som vil gjøre det. Algoritmer kan gi beslutningsstøtte til, kanskje på sikt avgjøre, hvem som vil begå straffbare handlinger og hvem som skal prøveløslates.

Algoritmer vil også fatte beslutning om liv og død. Det er ingen tvil om at selvkjørende biler vil rulle rundt på norske veier om ikke veldig mange år. Køene vil reduseres, utslippene av klimagasser vil gå ned og færre vil dø i trafikken. Men *noen* vil fortsatt dø, og det er algoritmen som bestemmer hvem. Er det en 53 år gammel statsansatt kvinne med høy inntekt (som sikrer gode skatteinntekter) og god helse, eller en 57 år gammel ufør, kjederøykende mann som bruker dagene på å spille bingo? Men det kan også fremskaffe kunnskap som kan redde mange menneskeliv innen medisinsk forskning.

Å treffe avgjørelser automatisk har også mange fordeler. Det er for eksempel billigere, og saksbehandlingstiden kan bli svært kort, ja, den kan nesten skje i sanntid. Maskiner har også evne til å lære, og til å øve seg på å bli flinkere. Kvaliteten kan derfor bli bedre, mer presise. Her ligger noe av grunnen til at mange avgjørelser allerede treffes helt automatisk, for eksempel i Statens Lånekasse for utdanning og Husbanken.

Men det er ingen tvil om at den utviklingen vi beskriver, tross positive sider, skaper noen store utfordringer for folks personvern. Noen av grunnprinsippene i personvernet utfordres. Dataminimalisering handler om at man ikke skal samle inn mer data enn det som er nødvendig, og all behandling skal ha et klart formål. Data som brukes skal være relevante for dette formålet. Selve ideen med stordataanalyse er imidlertid å samle inn mest mulig data og bruke dem til nye formål, og alle data er i prinsippet relevante. Som det iblant hevdes blant forskere er det data som i utgangspunktet ikke virker relevante i det hele tatt, som faktisk fører til et gjennombrudd i forskningen.

Den nye personvernforordningen vil få stor betydning for hvordan data kan behandles. Den slår fast at de viktige prinsippene over fortsatt vil gjelde. Dette vil skape utfordringer (litt enkelt sagt) for de som mener det skal være fri bruk av alle data til alle mulige formål, og det er nettopp det som har vært lovgivers intensjon. Virksomhetene skal ansvarliggjøres, de skal ha kontroll på egne behandlinger, og de skal gode rutiner for lagring, sletting og videre bruk.

I relasjon til de vi skriver om her, er én de nye rettighetene i forordningen særlig viktig, nemlig *retten til en forklaring*. Men hvordan forklare det som i virkeligheten er uforklarlig, som kan innebære behandling og analyse av titusener av ulike datapunkter, regnet ut av en algoritme i et millisekund?

Et eksempel fra forsikringsbransjen er illustrerende: En premieberegning på en bilforsikring er selv i dag krevende å forklare. Her inngår en rekke faktorer, som for eksempel alder, antall år man har kjørt bil, og man bor i byen eller på landet, om man parkerer i garasje eller i gata osv. Dersom forbrukeren i tillegg har inngått avtale om en å ha en svart boks i bilen, kommer fart, oppbremsing, bruk av blinklys og så videre inn i beregning. Fortsatt er det mulig å forklare, men det blir nærmest umulig dersom også andre, utenforliggende forhold trekkes inn. Det kan være hva man «liker» i sosiale medier, venner man har, hva man spise, hvor man drar på ferie, hva man ser på TV eller om man stadig lar mobilen gå ut på batteri. Vi er svært spent på hvordan virksomhetene vil løse denne oppgaven.

Forbrukerne får også, på visse betingelser, rett til å kreve manuell behandling av automatiserte avgjørelser. En tilsvarende regel gjelder i dag, men har i realiteten aldri vært brukt. Framtiden vil vise om den vil få noen betydning i det framtidige regelverket, eller om det vil forbli en sovende bestemmelse.

Også som tilsynsmyndighet står vi overfor noen store, men spennende utfordringer. Det en prioritert oppgave å utvikle en metodikk for tilsyn med algoritmer. Men hvordan gjøre det? Det ligger i algoritmens natur at den er dynamisk, og at den skal lære av det den finner ved søk i ustrukturerte data. Vi tror likevel vi har mye å hente fra dagens tilsynsmetodikk, supplert med undersøkelser om de nye kravene/rettighetene i forordningen, ved å stiller helt åpne spørsmål som:

- Hva er formålet med innsamlingen?
- Hvilke data anser dere som relevante for formålet?
- I hvilken grad er algoritmen bygd på prinsippene for innebygd personvern og dataminimalitet?
- Hvor lenge vil dere oppbevare dataene?
- Hvordan legger dere til rette for at forbrukerne kan bruke sin rett til dataportabilitet?

Men vi har også tro på andre virkemidler enn tilsyn. I Norge har vi på flere sektorer med stort hell utarbeidet bransjenormer, for eksempel ved kollektivtransport-bransjen. Dette har ført til at svært mange velger anonyme reiseløsninger, og ikke minst skapt grobunn for et konstruktiv og godt samarbeid mellom bransjen og tilsynet. Ikke minst i en verden der teknologiutviklingen går svært fort er dette viktig. Som et eksempel kan nevnes at vi på få år har gått fra gamle plastikk-reisekort, til en svært vellykket app, uten at det har gått ut over personvernet. Når bransjen nå begynner utrullingen av nye, sanntidsløsninger basert på Big Data og algoritmer, har vi et godt grunnlag for å finne gode løsninger.

VEDLEGG

Gjennomførte kontroller

	Saksnr.	Tilsynsobjekt	Kategori
1.	15/01042 16/00074	Kontroll hos Svelvik kommune - Internkontroll og informasjonssikkerhet	Offentlig – Internkontroll /infosikkerhet
2.	15/01356	Kontroll hos Franke Sjøberg AS - Kameraovervåking på arbeidsplassen	Kamera
3.	15/01357	Kontroll hos Kreftregisteret - Rutiner for innsamling av biologisk materiale og opplysninger i Janus Serumbank	Helse
4.	16/00313	Kreftregisteret - Brevkontroll - Behandling av sensitive personopplysninger i lovhjemlede helseregistre	Helse
5.	16/00361	Kontroll hos Losby Gods - Kameraovervåking	Kamera
6.	16/00374	Helsedirektoratet - IPLOS - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
7.	16/00375	Folkehelseinstituttet - Reseptregisteret - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
8.	16/00376	Folkehelseinstituttet - Dødsårsaksregisteret - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
9.	16/00378	Folkehelseinstituttet - MSIS - Meldingssystem for smittsomme sykdommer - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
10.	16/00379	Folkehelseinstituttet - SYSVAK - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
11.	16/00380	Forsvarsdepartementet - Forsvarets helseregister - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
12.	16/00381	Helsedirektoratet - NPR - Norsk Pasientregister - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
13.	16/00382	Folkehelseinstituttet - Nasjonalt register over hjerte- og karlidelser - Brevkontroll med behandling av sensitive personopplysninger i sentrale helseregistre	Helse
14.	16/00400	Kontroll hos The Well AS - Kameraovervåking	Kamera
15.	16/00426	Kontroll av Politiets utlendingsregister - Politiets utlendingsenhet	Justis
16.	16/00506	Kontroll hos Rana kommune - Internkontroll og informasjonssikkerhet	Offentlig – Internkontroll /infosikkerhet

	Saksnr.	Tilsynsobjekt	Kategori
17.	16/00585	Brevkontroll hos Trumf AS - Behandling av personopplysninger ved registering av kontonummer på Trumf.no	Kommersiali-sering
18.	16/00629	Kontroll av Kautokeino kommune - Internkontroll og informasjonssikkerhet	OFF IK/IS
19.	16/00656	Kontroll hos Skedsmovollen Bilistsenter Vest - NS Stasjonsdrift AS - Kameraovervåking	Kamera
20.	16/00664	Kontroll hos Michael Kors (Norway) AS - Kameraovervåking i butikk	Kamera
21.	16/01087	Kontroll hos InsightOne - Kommersialiseringsprosjektet	Kommersiali-sering
22.	16/01437	Varsel om kontroll hos Elkjøp Lørenskog Megastore - kameraovervåking	Kamera
23.	16/01456	Varsel om kontroll hos Rakkestad kommune - Internkontroll og informasjonssikkerhet	Offentlig – Internkontroll /infosikkerhet
24.	16/01457	Varsel om kontroll hos Aremark kommune - Internkontroll og informasjonssikkerhet	Offentlig – Internkontroll /infosikkerhet
25.	16/01481	Brevkontroll hos Nord-Trøndelag fylkeskommune - Sterk autentisering	Utdanning
26.	16/01482	Brevkontroll hos Sør Trøndelag fylkeskommune - Sterk autentisering	Utdanning
27.	16/01483	Brevkontroll hos Hordaland fylkeskommune - Sterk autentisering	Utdanning
28.	16/01484	Brevkontroll hos Rogaland fylkeskommune - Sterk autentisering	Utdanning
29.	16/01485	Brevkontroll hos Vest-Agder fylkeskommune - Sterk autentisering	Utdanning
30.	16/01486	Brevkontroll hos Aust-Agder fylkeskommune - Sterk autentisering	Utdanning
31.	16/01487	Brevkontroll hos Telemark fylkeskommune - Sterk autentisering	Utdanning
32.	16/01488	Brevkontroll hos Hedmark fylkeskommune - Sterk autentisering	Utdanning
33.	16/01489	Brevkontroll hos Finnmark fylkeskommune - Sterk autentisering	Utdanning
34.	16/01490	Brevkontroll hos Akershus fylkeskommune - Sterk autentisering	Utdanning
35.	16/01522	Varsel om kontroll hos Trondheim båtforening - Grilstad småbåthavn - Automatisk skiltgjenkjenning	Kamera
36.	16/01537	Brevkontroll med Hitra kommune - Oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet

	Saksnr.	Tilsynsobjekt	Kategori
37.	16/01549	Brevkontroll hos Sauda kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
38.	16/01550	Brevkontroll hos Osen kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
39.	16/01551	Brevkontroll hos Fjaler kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
40.	16/01552	Brevkontroll hos Nesset kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
41.	16/01553	Brevkontroll hos Hasvik kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
42.	16/01554	Brevkontroll hos Vinje kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
43.	16/01555	Brevkontroll hos Jevnaker kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
44.	16/01556	Brevkontroll hos Gjøvik kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
45.	16/01557	Brevkontroll hos Mandal kommune - oversikt over behandling av personopplysninger og risikovurdering	Offentlig – Internkontroll /infosikkerhet
46.	16/01587	Varsel om kontroll - Schengen Informasjonssystem - SIS	Justis
47.	16/01590	Varsel om kontroll hos Ullevaal Stadion - Nettvarder (beacons) og WiFi-sporing	Sporing
48.	16/01656	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Stavanger HF	Helse
49.	16/01657	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Fonna HF	Helse
50.	16/01658	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Bergen HF	Helse
51.	16/01659	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Førde HF	Helse
52.	16/01660	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Møre og Romsdal HF	Helse

	Saksnr.	Tilsynsobjekt	Kategori
53.	16/01661	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - St Olavs Hospital HF	Helse
54.	16/01662	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helse Nord-Trøndelag HF	Helse
55.	16/01663	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Helgelandssykehuset HF	Helse
56.	16/01664	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Finnmarkssykehuset HF	Helse
57.	16/01665	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Nordlandssykehuset HF	Helse
58.	16/01666	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Universitetssykehuset Nord-Norge HF	Helse
59.	16/01667	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Akershus universitetssykehus HF	Helse
60.	16/01668	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Oslo universitetssykehus HF	Helse
61.	16/01669	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 -Sunnaas sykehus HF	Helse
62.	16/01670	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Sykehuset i Vestfold HF	Helse
63.	16/01671	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Sykehuset Innlandet HF	Helse
64.	16/01672	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Sykehuset Telemark HF	Helse
65.	16/01673	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Sykehuset Østfold HF	Helse
66.	16/01674	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Sørlandet sykehus HF	Helse
67.	16/01675	Brevkontroll med helseforetakenes behandling av helseopplysninger til intern kvalitetssikring etter helsepersonelloven § 26 - Vestre Viken HF	Helse

	Saksnr.	Tilsynsobjekt	Kategori
68.	16/01676	Brevkontroll hos Røstad legesenter - samarbeid om behandlingsrettede helseregistre	Helse
69.	16/01677	Brevkontroll hos Legesenteret Molde - samarbeid om behandlingsrettede helseregistre	Helse
70.	16/01678	Brevkontroll hos Volda legesenter - samarbeid om behandlingsrettede helseregistre	Helse
71.	16/01679	Brevkontroll hos Nardosletta legesenter - samarbeid om behandlingsrettede helseregistre	Helse
72.	16/01680	Brevkontroll hos Nesbru legesenter - samarbeid om behandlingsrettede helseregistre	Helse
73.	16/01681	Brevkontroll hos Kurbadet legesenter - samarbeid om behandlingsrettede helseregistre	Helse
74.	16/01682	Brevkontroll hos Vennesla legesenter - samarbeid om behandlingsrettede helseregistre	Helse
75.	16/01683	Brevkontroll hos Furubo legesenter - samarbeid om behandlingsrettede helseregistre	Helse
76.	16/01684	Brevkontroll hos Fenring legesenter - samarbeid om behandlingsrettede helseregistre	Helse
77.	16/01685	Brevkontroll hos Utsikten legesenter - samarbeid om behandlingsrettede helseregistre	Helse
78.	16/01715	Brevkontroll hos USIT - Kontroll med kryptering hos databehandlere	Sikkerhet
79.	16/01719	Brevkontroll hos Jottacloud - Kontroll med kryptering hos databehandlere	Sikkerhet
80.	16/01721	Brevkontroll hos Datametrix - Kontroll med kryptering hos databehandlere	Sikkerhet
81.	16/01722	Brevkontroll hos Broadnet - Kontroll med kryptering hos databehandlere	Sikkerhet
82.	16/01723	Brevkontroll hos CGI Norge - Kontroll med kryptering hos databehandlere	Sikkerhet
83.	16/01774	Trumf AS - analyse og markedsføringsformål	Kommersi-alisering
84.	16/01789	Brevkontroll med Olav Thon Gruppens sentre - Bruk av sporingsteknologi	Sporing
85.	16/01794	Brevkontroll med CC Stadion Hamar - Bruk av sporingsteknologi	Sporing

Høringssvar

Tabellen viser en oversikt over høringer Datatilsynet har hatt merknader til i 2016:

	Dok. nr.	Tittel	Til/fra
1.	16/01580-2	Høringsuttalelse - Forslag til forskrift om kontroll med informasjon innhentet ved bruk av luftbårne sensorsystemer	Forsvarsdepartementet
2.	16/01743-2	Høringsuttalelse - Forskrift om narkotikaprogram med domstolskontroll mv	Justis- og beredskapsdepartementet
3.	16/01763-3	Høringsuttalelse - Endringer i politiregisterloven og forskriften - implementering av direktiv EU 2016/680	Justis- og beredskapsdepartementet
4.	16/01704-3	Høringsuttalelse - Forslag til lov om registrering av enkeltpersoners gjeld - gjeldsregisterloven	Barne- og likestillingsdepartementet
5.	16/01335-3	Høringsuttalelse - Forslag til tre nye forskrifter til lov om verneplikt og tjeneste i Forsvaret med mer - Forsvarsloven	Forsvarsdepartementet
6.	16/01700-2	Høringsuttalelse - forslag til endring i postloven	Samferdsels-departementet
7.	16/01165-2	Høringsuttalelse - Nasjonale retningslinjer for åpen tilgang til forskningsresultater	Kunnskapsdepartementet
8.	16/01371-2	Høringsuttalelse - Politiets tilgang til utlendingsmyndighetenes registre	Justis- og beredskapsdepartementet
9.	16/01375-2	Høringsuttalelse - Forslag til ny lov om omsorgssentre for enslige mindreårige asylsøkere - Omsorgssenterloven - Barne- og likestillingsdepartementet	Barne- og likestillingsdepartementet
10.	16/01348-2	Høringsuttalelse - Forslag til nye bestemmelser om rapportering av individdata til database for statistikk om høyere utdanning og fagskoleutdanning	Kunnskapsdepartementet
11.	16/01040-2	Høringsuttalelse - Forslag til endringer i arbeidsmiljølovens regler om varsling	Arbeids- og sosialdepartementet
12.	16/01414-2	Høringsuttalelse - Forslag til norsk standard for metadata for læringsressurser	Utdanningsdirektoratet
13.	16/01243-2	Høringsuttalelse - Europakommisjonens forslag til forordning om geo-blokkering og diskriminering på bakgrunn av basert på bosted etableringssted eller nasjonalitet	Nærings- og fiskeridepartementet
14.	16/01152-2	Høringsuttalelse - Forslag til endring av vegtrafikkloven - §§ 13 - 19 - 19a - 32 og 36a	Statens vegvesen
15.	16/01151-2	Høringsuttalelse - Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer	Justis- og beredskapsdepartementet

	Dok. nr.	Tittel	Til/fra
16.	16/00604-2	Høringsuttalelse - Kommunelovutvalgets utredning 2016: 4 - Ny kommunelov	Kommunal- og moderniserings-departementet
17.	16/01211-2	Høringsuttalelse - Ny delversjon av Referansekatalogen for anbefalte og obligatoriske IT-standarder sommer 2016	Difi - Direktoratet for forvaltning og IKT
18.	16/01108-2	Høringsuttalelse - Forslag om sentral forskrift om lavutslippssone for biler	Samferdsels-departementet
19.	16/01281-2	Høringsuttalelse - forslag til endringer i forskrift om elektronisk kommunikasjon med domstolene og forskrift om postforkynning	Justis- og beredskapsdepartementet
20.	16/01019-2	Høringsuttalelse - Forslag til selvdeklareringsordning for mobile helseapplikasjoner	Direktoratet for e-helse
21.	16/01122-2	Høringsuttalelse - Forslag til lov om informasjonstilgang - taushetsplikt mv for Statens helsetilsyn ved gjennomgang av et utvalg saker om akuttplassering og omsorgsovertakelse etter barnevernloven	Barne- og likestillingsdepartementet
22.	16/01148-2	Høringsuttalelse med merknader - forslag til endringer i tobakksforskriftene og ny forskrift om elektroniske sigaretter	Helse- og omsorgsdepartementet
23.	16/01042-2	Høringsuttalelse - Ny forskrift om avleveringsplikt for allment tilgjengelige dokument og endringer i forskrift til åndsverkloven	Kulturdepartementet
24.	16/00886-2	Høringsuttalelse - Endringer i kjernejournal- og reseptformidlerforskriftene	Helse- og omsorgsdepartementet
25.	16/00503-3	Høringsuttalelse - Forslag til ny åndsverklov	Kulturdepartementet
26.	16/01055-2	Høringsuttalelse - utvidet lagringstid for opplysninger fra Tolletatens skiltgjenkjenningssystem (ANPR)	Finansdepartementet
27.	16/00768-2	Høringsuttalelse - Styrking av Tolletatens kontroll med vareførsel over grensen - Finansdepartementet	Finansdepartementet
28.	16/00674-2	Høringsuttalelse - Endringer i opplæringsloven og friskoleloven - Nytt kapittel om skolemiljø	Kunnskapsdepartementet
29.	16/00744-2	Høringsuttalelse - Vegtrafikkloven ny § 43 b - Rett til å behandle personopplysninger - politiets tilgang til personopplysninger i Statens vegvesens registre	Samferdsels-departementet
30.	16/00826-2	Høringsuttalelse - Utkast til veileder for håndtering av dokumentasjon i barnevernet	KS - Kommunesektorens organisasjon
31.	16/00807-2	Høringsuttalelse - Forslag til ny lov om statens ansatte	Kommunal- og moderniseringsdepartementet

	Dok. nr.	Tittel	Til/fra
32.	16/00531-2	Høringsuttalelse - Opphentingsprogram for HPV-vaksinen - Forslag til endringer i forskrift om nasjonalt vaksinasjonsprogram og SYSVAK-registerforskriften - Helse- og omsorgsdepartementet	Helse- og omsorgsdepartementet
33.	16/00495-3	Høringsuttalelse - Nasjonal strategi for persontilpasset medisin i helsetjenesten	Helsedirektoratet
34.	16/00124-4	Høringsuttalelse - Forskrift om farmakogenetiske undersøkelser	Helse- og omsorgsdepartementet
35.	16/00232-2	Høringsuttalelse - Endringer i straffeprosessloven og politiloven - Utlevering av informasjon fra PST til E-tjenesten	Justis- og beredskapsdepartementet
36.	16/00372-2	Høringsuttalelse - Evalueringen av offentleglova	Justis- og beredskapsdepartementet
37.	16/00236-2	Høringsuttalelse - Forslag til endring i ekomlov og ekomforskrift	Samferdsels-departementet
38.	15/01672-2	Høringsuttalelse - Økt åpenhet om informasjon om eiere i aksjeselskaper - Nærings- og fiskeridepartementet	Nærings- og fiskeridepartementet
39.	15/01605-2	Høringsuttalelse - Digital sårbarhet - NOU 2015:13	Justis- og beredskapsdepartementet
40.	16/00104-2	Høringsuttalelse - Utkast til forskrift om gjennomføring av delegert Kommisjonsforordning (EU) nr. 962/2015 forordning iht. ITS-direktivet 2010/40/EU	Statens vegvesen
41.	16/00047-1	Høringsuttalelse - Gjennomføring av EUs forordning om elektronisk identifisering (eID) og tillitstjenester for elektroniske transaksjoner i det indre marked	Nærings- og fiskeridepartementet
42.	16/00190-1	Høringsuttalelse - varsling om vitnemålsforfalsking mm	Kunnskapsdepartementet
43.	15/01402-1	Høringsuttalelse - Forskrift om styringssystem i helse- og omsorgstjenesten	Helse- og omsorgsdepartementet
44.	16/00111-2	Høringsuttalelse - Forslag til midlertidig lov som gir utvalg tilgang til opplysninger underlagt lovbestemt taushetsplikt	Barne-, likestillings- og inkluderings-departementet
45.	15/01583-2	Høring - Veileder om spesifisert faktura	Nasjonal kommunikasjons-myndighet
46.	15/01472-1	Høringsuttalelse - Helseberedskap ved miljø- og kjemikaliehendelser	Helse- og omsorgsdepartementet
47.	15/01315-1	Høringsuttalelse - Advokatutvalgets utredning NOU 2015:3 - Advokaten i samfunnet	Justis- og beredskapsdepartementet

Saker sendt til Personvernnemnda

Tabellen viser alle sakene Datatilsynet har sendt til Personvernnemnda for klagebehandling og som er registrert hos nemnda i 2016:

Sak	Klager	Tittel	Dato DT	Sak PVN	Vedtak i PVN
15/01327	Hovedrednings-sentralen for Nord-Norge	Klage på vedtak om pålegg og ileggelse av overtredelsesgebyr etter kontroll	05.01.2016	PVN-2016-02	Klagen tas delvis til følge
15/01350	Advokatfirma Stiegler ANS på vegne av privatperson	Klage på avvisningsvedtak - Privat kameraovervåking av nabo	18.03.2016	PVN-2016-03	Klager gis medhold og saken sendes tilbake
15/01355	Arntzen de Besche Advokatfirma AS på vegne av privatperson	Klage på avslag - krav om sletting av brukervurderinger på Legelisten.no	15.04.2016	PVN-2016-04	Saken sendes tilbake
16/00028	Privatperson	Klage på avslag på sletting av saksdokumenter og personopplysninger fra Datatilsynets arkiv	18.04.2016	PVN-2016-05	Klagen tas ikke til følge
15/01338	Vaktmester Andersen AS	Klage på ileggelse av overtredelsesgebyr - Bruk av elektronisk kjørebok	19.05.2016	PVN-2016-06	Klagen tas ikke til følge
15/01643	Synkron Media AS	Klage på ileggelse av overtredelsesgebyr-manglende sletting av epostkasse	19.05.2016	PVN-2016-07	Klagen tas ikke til følge
15/01424	Advokatfirma Raugland AS på vegne av privatperson	Klage på beslutning om å ikke fatte vedtak om sletting av tilrettevisning - Trondheim kommune	31.05.2016	PVN-2016-08	Klagen tas ikke til følge
15/01324	Codex Advokat Oslo AS	Klage på vedtak om overtredelsesgebyr - Innsyn i e-post	21.06.2016	PVN-2016-09	Klagen tas ikke til følge
15/01359	Advokatfirmaet Føyen Torkildsen AS på vegne av Google	Klage over pålegg om å slette søketreff i søkemotoren Google	24.06.2016	PVN-2016-10	
15/01555	Musikernes fellesorganisasjon i Troms på vegne av privatperson	Klage på vedtak om avslag på krav om sletting av personopplysninger i personalmappe	04.08.2016	PVN-2016-11	Saken er trukket
16/00571	Advokatfirmaet Johnsrud & Co på vegne av privatperson	Klage på avslag om sletting av personopplysninger i personalmappe hos Stange kommune	05.08.2016	PVN-2016-12	Klages tas ikke til følge
16/00982	Privatperson	Klage på avvisningsvedtak - Krav om sletting av journalopplysninger	22.08.2016	PVN-2016-13	Klages tas ikke til følge

Sak	Klager	Tittel	Dato DT	Sak PVN	Vedtak i PVN
16/00366	Årdal kommune	Klage på vedtak om overtredelsesgebyr - Publisering av sensitive personopplysninger på offentlig journal	05.09.2016	PVN-2016-14	Klagen tas delvis til følge
16/00403	Dialog Advokater AS på vegne av privatperson og Tromsø kommune	Klage på vedtak om innsyn i dokumenter hos arbeidsgiver Tromsø kommune	07.09.2016	PVN-2016-15	Klagen tas til følge
15/01475	Sykehuset Telemark HF	Klage på vilkår i konsesjon til å behandle personopplysninger i Gastronet	07.11.2016	PVN-2016-16	
16/01514	Privatperson	Klage på vedtak om ikke å pålegge retting av opplysninger i AA-registeret	18.11.2016	PVN-2016-17	
16/01690	Privatperson	Klage på vedtak om ikke å pålegge NAV å rette opplysninger om klagers yrkeskompetanse	22.11.2016	PVN-2016-18	

Vedtak om overtredelsesgebyr

Mottaker	Vedtaksbrev	Størrelse	Kommentar	Stikkord
XO Mat & Vinhus AS	13.01.2016	25.000	Avsluttet	Kontroll - Kameraovervåking på internett
Universitetet i Bergen	02.02.2016	350.000	Avsluttet	Utlevering av forskningsdata
Codex Advokat Oslo AS	10.02.2016	75.000	Klagesak i PVN	Innsyn i e-post
NextGentel AS	04.05.2016	500.00	Avsluttet	Utlevering av personopplysninger
Kverneland Bil Trondheim AS	19.05.2016	75.000	Avsluttet	Innsyn i e-post
Årdal kommune	16.06.2016	50.000	Klagesak i PVN	Publisering av personopplysninger på internett
Askvoll kommune	16.06.2016	75.000	Avsluttet	Publisering av personopplysninger på internett
Os kommune	17.06.2016	100.000	Avsluttet	Publisering av personopplysninger på internett
Harstad kommune	17.06.2016	100.000	Avsluttet	Publisering av personopplysninger på internett
Rustfrie Bergh AS	22.06.2016	50.000	Avsluttet	Innsyn i e-ost
Jotunheimen Eiendom AS	27.06.2016	100.000	Avsluttet	Innsyn i e-post
Hordaland fylkeskommune	27.07.2016	150.000	Avsluttet	Publisering av personopplysninger på internett
NTNU	05.08.2016	75.000	Avsluttet	Uautorisert innsyn i personopplysninger
Hereid Hus AS	21.09.2016	75.000	Klagebehandling	Innsyn i e-post/manglende sletting
Securitas AS	29.09.2016	150.000		Kameraovervåking på arbeidsplassen
R. Gjestad AS/Rema1000 Prinsensgate	29.09.2016	50.000		Kameraovervåking på arbeidsplassen
NTNU/ Olympiatoppen Midt-Norge	24.10.2116	100.000		Misbruk av kamerasystem
Bertram Bil AS	25.10.2016	75.000	Klagebehandling	Kredittvurdering uten saklig behov
Isurvey Group AS	07.11.2016	75.000		Manglende sletting av e-postkasse
Axactor Norway AS	16.11.2016	250.000	Klagebehandling	Kredittvurdering uten saklig behov
Feiring Bruk AS	09.12.2016	100.000	Klagebehandling	
YX Frøya	01.12.2016	50.000	Krav midlertidig stoppet hos SI	Utlevering av kameraopptak

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep.,
0034 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no