



ÅRSMELDING FOR 2015

Hva rører seg på personvernfeltet?

INNHold

LEDERS BERETNING	3	Annen vesentlig aktivitet	45
2015 - året da personvern ble internasjonal politikk	3	Arbeidsliv	45
INTRODUKSJON OG HOVEDTALL.....	6	Finanssektoren.....	46
Virkemidler	6	Teknologi, internett og telekom	46
Organisasjon og budsjett.....	9	Samferdsel	48
Tilsynsvirksomheten.....	10	Forskning og utvikling (FoU)	48
Saksbehandlingen.....	13	Kommersiell utnyttelse av personopplysninger	50
Veiledningstjenesten.....	19	Den internasjonale personverndagen ..	50
Kommunikasjonsvirksomheten	24	Internet Sweep Day - personvern i apper for barn	51
ÅRETS VIKTIGSTE AKTIVITETER.....	28	Personvernombudsordningen	51
Justissektoren.....	28	Internasjonalt arbeid	52
Gjennomførte aktiviteter	28	Nasjonale samarbeidsrelasjoner	55
Fremtidige utfordringer.....	30	VURDERING AV FRAMTIDSUTSIKTER.....	58
Barn, skole og utdanning.....	31	Internasjonalt.....	58
Gjennomførte aktiviteter	31	Nasjonalt.....	58
Fremtidige utfordringer.....	34	VEDLEGG	60
Offentlig sektor.....	35	Gjennomførte kontroller	60
Gjennomførte aktiviteter	35	Saker sendt til Personvernemnda.....	63
Fremtidige utfordringer.....	37	Høringer	65
Helse og velferd.....	39	Ilagte sanksjoner	68
Gjennomførte aktiviteter	40		
Fremtidige utfordringer.....	43		

LEDERS BERETNING

2015 - året da personvern ble internasjonal politikk

Det mest spennende med å være leder i Datatilsynet er at det alltid dukker opp store saker som gjør at vi må snu opp ned på prioriteringene våre. Noen opplever kanskje dette som frustrerende, men som jeg pleier å si til de flinke folka i tilsynet: Vi skal være veldig glade for at vi har en arbeidsplass der vi hele tiden må gjøre prioriteringer og endre på planene våre.

Året begynte med fire prioriterte sektorer og to prioriterte prosjekter. Justissektoren, der borgernes rett til å leve sitt liv uten overvåking står mot fellesskapets behov for trygghet, var som alltid viktig. Det samme var helsesektorens innsamling av våre mest sensitive og private opplysninger, samt offentlig sektor for øvrig der det er store mengder opplysninger om oss alle og der man nok ikke alltid har full oversikt over hvilke opplysninger som faktisk behandles. Så var det utdanningssektoren der opplysninger som tidligere var i meldingsbøker, på karakterutskrifter og i ranselpost, blir digitalisert og gjort til gjenstand for analyse og vurdering.

De to prosjektene har et klart internasjonalt tilsnitt. Vi skal forberede oss på EUs nye personvernregelverk i form av en forordning som også vil bli gjeldende lov i Norge. Vi ville også kartlegge hvordan personopplysninger blir brukt kommersielt, særlig når det gjelder å skreddersy reklame basert på den enkeltes interesser, bosted, familieforhold og inntekt.

Mer overraskende var at de to siste prosjektene plutselig befant seg i kjernen av en langt større konflikt, nemlig hvorvidt USA er et trygt land å lagre data i, og om det skal være lov for europeiske selskaper å overføre data til USA.

Sporene etter Snowden

Men la oss spole noen år tilbake. I begynnelsen av juni 2013 sto en beskjeden mann med navn Edvard Snowden fram med banebrytende avsløringer. Ikke bare hadde National Security Agency (NSA) samlet inn enorme datamengder om helt vanlige borgeres liv, de hadde også avlyttet telefonen til storheter som Angela Merkel og 35 andre statsledere. Det er ulike meninger om Edvard Snowden, men det er hevet over enhver tvil at hans avsløringer har hatt svært stor betydning for personverndebatten og forholdet mellom Europa og USA.

Det startet allerede da EU-parlamentet skulle debattere personvernforordningen. Kommisjonens opprinnelige forslag bygde på det vi kan kalle den tradisjonelle lære – en virksomhet må være etablert i et europeisk land for at europeisk rett skal gjelde. Spørsmålet om jurisdiksjon er viktig, for på personvernområder, som på mange andre, er det stor forskjell på europeisk og amerikansk rett. Blant annet er terskelen for hva som er en personopplysning høyere i USA, og muligheten for å dele data større. Men EU-parlamentet vedtok en regel om at europeisk rett skal gjelde for alle virksomheter som retter sine tjenester mot europeiske borgere, og det gjelder de aller fleste. Jeg har tidligere kalt dette lex Snowden, fordi parlamentet i begrunnelsen hadde en veldig enkel begrunnelse, de gjorde dette på grunn av Snowdens avsløringer som viste at vi europeere måtte sørge for at europeiske regler gjaldt i Europa.

Når forordningen ble vedtatt var lex Snowden en del av pakka. Men før det, hadde nok en avgjørelse rystet store deler av næringslivet og relasjonene mellom USA og Europa. Da avgjorde nemlig EU-domstolen at den såkalte Safe Harbor-avtalen er ugyldig. De færreste hadde hørt om denne avtalen, men plutselig var den på alles lepper. Personvernregelverket er på dette punktet veldig enkelt: Det er

forbudt å overføre data til tredjeland, det vil si utenfor EØS-området. Dette med mindre EU-kommisjonen har definert tredjelandet som et trygt sted å lagre data. Derfor er det inngått en rekke avtaler mellom EU og land som Chile, Israel og Uruguay, og fastslått at overføring til disse landene er trygt. Så også til USA, men der har avtalen fått et eget navn, Safe Harbor. Den inneholder ganske enkelt et sett regler som amerikanske selskaper kan forplikte seg til å følge. Ved å skrive under en egenerklæring er de et sertifisert datasenter som europeiske selskaper kan overføre data til. Når vi vet at overføring av persondata er en sentral del av nær sagt enhver forretning mellom EU og USA, trengs det ingen tilleggsforklaring på at avgjørelsen som kjente avtalen ugyldig var svært dramatisk. At det er over 4 000 sertifiserte Safe Harbor-sentre sier nok.

Så var det Edvard Snowden igjen. Generaladvokaten i EU-domstolen, som skriver innstillinger til dom, la i sin innstilling vekt på nettopp Edvard Snowdens avsløringer når han kom med sin konklusjon om at USA ikke var et trygt land når det gjaldt å behandle data om europeiske borgere. Og EU-domstolen kom kun uker senere til samme konklusjon.

Avgjørelsen var banebrytende, og burde strengt tatt vært omtalt på førstesiden av alle landets aviser. I realiteten, hvis det ikke blir inngått en ny Safe Harbor-avtale, betyr avgjørelsen at mange tusen europeiske virksomheter ikke lenger kan overføre data til USA i medhold av Safe Harbor, men må finne andre, mer tungvinte metoder. Mest nærliggende er å bruke noe som kalles standard modellavtaler, men nå hadde personvernere fått blod på tann. De hevdet at standardavtalene hadde akkurat samme svakheten som Safe Harbor-avtalen, nemlig at amerikanske sikkerhetsmyndigheter kan få tilgang til dataene. Det er vel ingen hemmelig at de fleste jurister mener det er godt hold i et slikt argument.

Dermed måtte vi i Datatilsynet kaste oss rundt. Vi la ut veiledning på hjemmesiden vår, sendte brev til over hundre virksomheter vi visste brukte Safe Harbor og besvarte en lang rekke telefoner. I skrivende stund er det forhandlet fram en ny Safe Harbor-avtale, kalt Privacy Shield, men det kan stilles store spørsmålsteget ved om denne er god nok.

USA versus Microsoft

Men det er ikke bare europeiske domstoler som har vist muskler. Også en domstol i New York fattet en avgjørelse som kan få dramatisk konsekvenser. Microsoft har datasentre over hele verden, men er som alle vet et amerikansk selskap. CIA ville imidlertid ha utlevert blant annet e-poster som lå lagret på en server i Microsofts datasenter i Dublin, Irland. Microsoft nektet og hevdet en amerikansk domstol ikke kan fatte beslutninger som får konsekvenser for europeiske borgere lagret i et europeisk datasenter. Men dommeren mente det motsatte, og påla Microsoft å utlevere e-postene under henvisning til at det var et amerikansk selskap. Dommen skal opp til avgjørelse i en høyere domstol, og ender trolig i Høyesterett, men den illustrerer et interessant forhold. Når slutter amerikansk rett å gjelde? Ved USAs grense? Eller kan et amerikansk selskap tvinges til å utlevere data fra borgere i hele verden, uansett i hvilket land selskapet har sin virksomhet?

Microsoft har protestert heftig og skrevet til alle datatilsynsmyndighetene i Europa og bedt om støtte for sin sak. Konsekvensen for europeiske borgere kan bli dramatisk dersom avgjørelsen blir stadfestet av høyere domsinstanser. Det betyr i klartekst at et amerikansk selskap etablert i Norge, kan tvinges til å utlevere norske borgeres data til USA, et land EU-domstolen har fastslått ikke er trygt i så henseende. Et paradoks? Javisst, men det er også dette: Dersom Høyesterett i USA kommer til at dataene må utleveres til USA, bryter de virksomhetene som utleverer dataene europeisk lov. Dersom de nekter å etterkomme en amerikansk dom, bryter de amerikansk lov.

Siste ord er ikke sagt i denne saken, men vi kan trygt slå fast at det blir meget spennende å følge dette videre, ikke minst om Microsoft og andre teknologigiganter lager selskapskonstruksjoner som

gjør at de juridisk sett ikke lenger er amerikanske selskaper når det lagres data i Europa. Følgene av dette kan bli store.

Annonseindustriens datakappløp

Datatilsynet lanserte i september rapporten «Det store datakappløpet – om kommersiell utnyttelse av personopplysninger». Som det først datatilsyn i verden, kartla vi hvordan annonseindustrien samler inn enorme mengder svært detaljerte opplysninger om oss. Dette er opplysninger som i sin tur brukes til å sende skreddersydd reklame basert på akkurat vår profil. Det vil for eksempel bety at ti mennesker som går inn på morgenavisen.no vil få ti ulike annonser. Dette utfordrer personvernet på en rekke områder. Kan dataene avsløre følsomme opplysninger om oss? Kan det føre til diskriminering av kunder? En undersøkelse i USA viste at menn får annonser for bedre betalte jobber enn kvinner, og at folk med lav inntekt og betalingsproblemer i større grad enn andre får annonser for kreditter med høy rente. Det er også bekymringsfullt at det digitale annonsemarkedet er svært komplisert og at de aller færreste, om noen, har oversikt over hva som skjer.

Det kom mange reaksjoner fra norske aktører på rapporten, de fleste positive. Samtidig kom det fram en bekymring: Norske virksomheter må ikke ha dårlige rammebetingelser enn våre konkurrenter. Og konkurrentene er jo «the usual suspects» som Facebook, Google og Microsoft. Dermed er vi tilbake der denne innledningen til årsmeldingen startet, ved våre to prioriterte prosjekter, som ikke bare ble nasjonale anliggender, men en del av en personvernkonflikt mellom USA og Europa.



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 i offentlig ordskifte 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. Eller dersom de setter begrensninger på seg selv fordi de er redde for at myndighetene registrerer og lagrer opplysninger om deres kommunikasjon med andre, om ferdselsmønstre, interesser eller uttrykk for holdninger. Datatilsynet må derfor jobbe aktivt for å oppnå en god ivaretagelse av personvernet i avveiningen mot andre samfunnsinteresser.

Hovedaktiviteter

For å realisere hovedmålet om en best mulig beskyttelse av folks personvern har Datatilsynet gjennomført følgende hovedaktiviteter i 2015:

- Arbeide for å øke kjennskapen til lovfestede plikter og rettigheter både i befolkningen og i virksomheter.
- Fremme bruk av innebygd personvern og stimulere til at personvern hensyn blir ivaretatt tidlig ved utvikling av nye løsninger eller nytt regelverk.
- Gjennomføre tilsyn i prioriterte sektorer basert på risikoanalyse, systematisert og kommunisere funn fra tilsynene til aktuelle målgrupper, samt følge opp etterlevelse av pålegg. Dette gjelder både i de enkelte kontrollsakene og gjennom etterkontroller.
- Delta aktivt i internasjonalt personvernarbeid.

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 en rapport om hvordan et fremvoksende marked for automatisert annonsehandel intensiverer innsamlingen og utnyttelsen av personopplysninger for kommersielle formål. Dessuten startet vi forberedelsene til det nye felles europeiske personvernregelverket som trolig vil bli vedtatt i EU våren 2016.

Virkemidler

For å nå hovedmålet vårt har vi i hovedsak fem ulike virkemidler til disposisjon. Ved å ha kontinuerlig oppmerksomhet på hvordan vi kombinerer virkemidlene våre, kan vi oppnå en betydelig bedre effekt enn om vi benytter hvert virkemiddel alene.

Saksbehandling som virkemiddel

Gjennom saksbehandling tilegner vi oss erfaring og kunnskap om hvordan personvern hensyn i praksis ivaretas. Spesielt skal vi 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. Tilsynsvirkemiddelet 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 kontrollhjelm 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

For at øvrige virkemidler skal gi best mulig effekt, er kommunikasjonsvirksomheten et sentralt virkemiddel. Datatilsynet integrerer i større grad enn tidligere kommunikasjonsvirksomheten med de øvrige virkemidlene vi har til disposisjon. En del av kommunikasjonen og dialogen vår skjer derfor gjennom veiledningstjenesten, veiledningsmøter og annen dialog med rammesettere og beslutningstakere.

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. Kommunikasjon har naturlig nok også vært det dominerende virkemiddelet ved utøvelse av vår ombudsrolle. Dette blir blant annet gjort ved utspill og kommentarer overfor mediene, foredragsvirksomhet og blogginnlegg.

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 personvern fremmende 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 i bruk i flere saker i 2015.

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 personvern hensyn 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 personvern hensyn også blir ivaretatt i annen forskning.

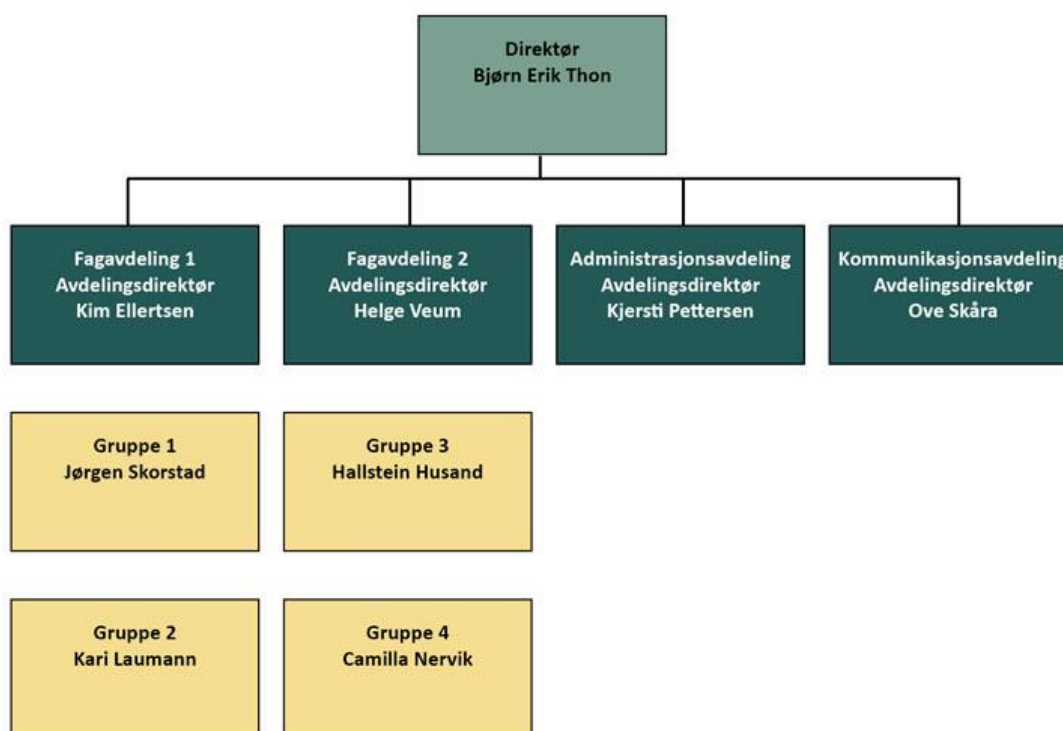
Vårt eget utredningsarbeid og kartlegginger utgjør også en viktig kilde til kunnskap. De gir dybde til ulike temaer vi jobber med og er med på å skape oppmerksomhet om personvern spørsmål. Resultater fra vårt forsknings-, utviklings- og utredningsarbeid legges naturlig nok også til grunn ved bruk av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

Organisasjon og budsjett

Datatilsynet ledes av direktør Bjørn Erik Thon. Ledergruppen består av fire menn og én kvinne.

I 2015 har Datatilsynet hatt 43 faste stillinger. Av disse var 56 prosent kvinner og 44 prosent menn. I løpet av året har fem medarbeidere sluttet (mot to året før). Av disse har én benyttet seg av AFP-ordningen og én har gått av med pensjon etter fylte 70 år.

Organisasjonskart per 31. desember 2015, med ledergruppe og gruppeledere:



Budsjett

Når overføringene fra 2014 var gjort og tilleggsbevilgninger var lagt til, hadde vi totalt 40 959 000 kroner til disposisjon i 2015. Av dette fikk vi i revidert nasjonalbudsjett (RNB) 2 830 000 kroner til IKT og MVA-refusjon. Fordelt på lønn og drift, utgjorde lønnsutgiftene 30 300 000 kroner (74 prosent). Driftsutgiftene utgjorde 10 659 000 kroner (26 prosent).

Oversikt over bevilgninger de siste årene:

År	Bevilgning
2012	35 015 000,-
2013	37 753 000,-
2014	38 264 000,-
2015	37 262 000,-
RNB 2015	2 830 000,-
Totalt 2015	40 092 000,-

Tilsynsvirksomheten

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

I 2015 gjennomførte vi totalt 54 tilsyn (se fullstendig oversikt under *Vedlegg*). I tillegg kommer bruk av kontrollhjemplene våre i 161 andre saker enn tilsynsvirksomheten. Til sammen utgjør dette dermed 215 saker.

I løpet av året gjennomførte vi flere tilsyn med internkontroll og informasjonssikkerhet i offentlig sektor for å påvirke til bedre etterlevelse av regelverket. Vi gjennomførte også kontroller med virksomheter som driver med samfunnsforskning. Kontrollene skal danne grunnlag for videre oppfølging av disse virksomhetene. Videre ble det første tilsynet etter politiregisterloven gjennomført ved at vi kontrollerte DNA-registeret hos Kripos. Det ble dessuten gjennomført tilsyn med reiseselskap. Vi valgte oss ut reiseselskapene som en bransje med middels risiko hos de individuelle objektene, men hvor vi mener det er muligheter for å påvirke mange aktører gjennom oppfølging etter tilsynene. For øvrig har vi gjennomført tilsyn med et sentralt register i finanssektoren, felles pasientdatabaser i helsesektoren, bruk av nettsky og kryptering av kommunikasjonen hos store datasentre.

De mest sentrale tilsynene er nærmere beskrevet under *Årets viktigste aktiviteter*.

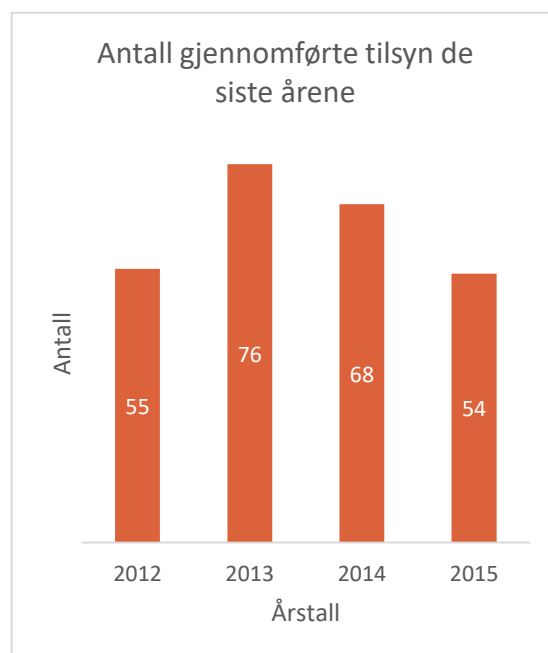
Generelle kommentarer

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.

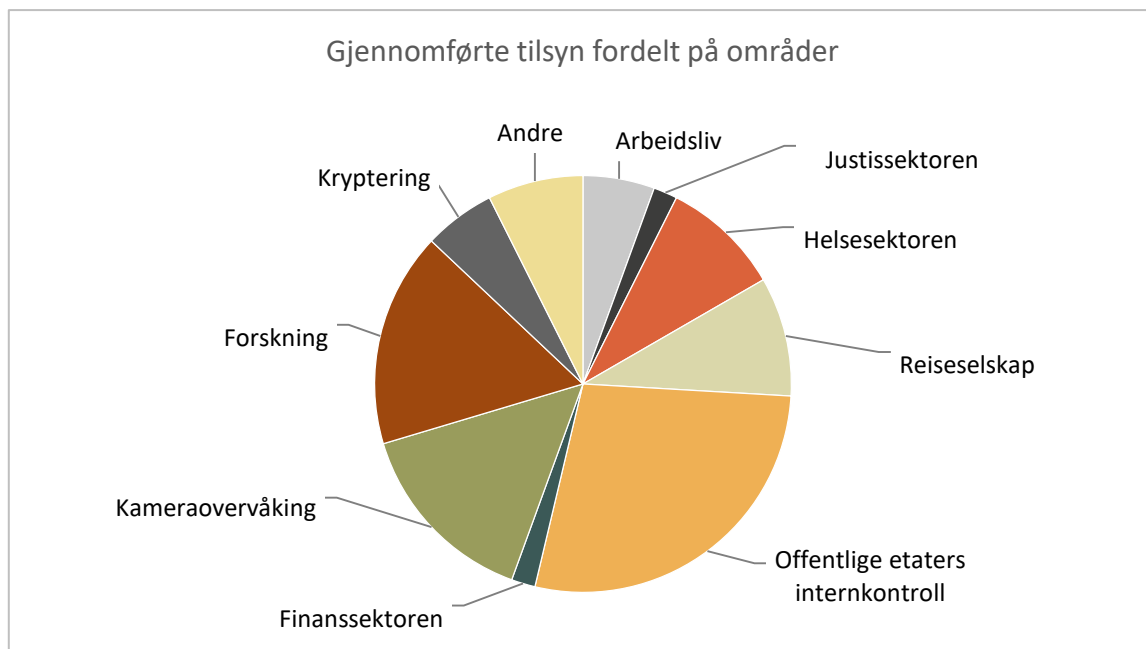
I noen tilfeller gjennomføres planlagte kontroller som en skriftlig prosess, uten at vi er på fysisk besøk hos virksomheten. Dette er i tilfeller der det vi ønsker å undersøke er egnet å få avklart uten et stedlig oppmøte. I 2015 ble 39 av tilsynene gjennomført hos virksomhetene (stedlig tilsyn), mens 15 ble gjennomført via brev (brevlig tilsyn).

De brevlige tilsynene skiller seg fra bruk av de samme kontrollhjemplene i øvrig saksbehandling ved at de er en planlagt undersøkelse av konkrete forhold i virksomhetene. I 2015 ble brevlige tilsyn særlig vurdert som hensiktsmessig for den oppfølgingen vi hadde av samfunnsforskning og kryptering i datasentre.

Det har blitt gjennomført færre tilsyn i 2015 enn i de foregående årene, og færre enn vi hadde planlagt. Dette gjelder særlig tilsyn på helseområdet og justisområdet. Årsakene er utsettelse, omprioriteringer og noe sykefravær. Vi fristilte blant annet en medarbeider store deler av året for å bidra i sekretariatet til det digitale sårbarhetsutvalget, vi har prioritert opp arbeidet med



personvernforordningen og kontrollen med DNA-registeret hos Kripos krevde en del ressurser. Som omtalt over, gjennomfører vi også kontroll med om regelverket følges i enkeltsaksbehandlingen utover det som fremgår som enkelttilsyn her. Reduksjonen i kontrollaktiviteten vår er derfor ikke så betydelig som tallet på antall gjennomførte tilsyn skulle tilsi.



Oversikt over kontrollene vi gjennomførte i 2015, fordelt på stedlige og brevlige tilsyn:

Bransje/sector/område	Stedlig	Brevlig	Totalt
Arbeidsliv	3	0	3
Finanssektoren	1	0	1
Helsektoren	1	4	5
Reiseselskap	5	0	5
Justissektoren	1	0	1
Kameraovervåking	8	0	8
Offentlige etaters internkontroll	15	0	15
Forskning	3	6	9
Kryptering	0	3	3
Andre	2	2	4
Sum	39	15	54

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 omtalt under *Årets viktigste aktiviteter*. Vi vil likevel på generelt grunnlag fremheve at vi fremdeles ser systematiske avvik i offentlig sektor knyttet til internkontroll, informasjonssikkerhet og etablering av databehandlertaler.

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 2015:

- I tilsynsprosjektet med reiseselskaper, gjennomførte vi først noen få tilsyn, før vi hadde dialog med bransjeforeninger (NHO og Virke) for å påvirke disse til å utarbeide veiledningsmaterieell for bransjen. Det arbeides nå med veiledning, og vi vil ha dialog med foreningene i forbindelse med ferdigstilling av materialet. Bred etterlevelse av regelverket får vi først når sektorer selv arbeider for etterlevelse. Formålet med prosjektet er derfor å initiere slike prosesser med kun en begrenset ressursbruk fra vår side.
- Kontroller med kommuner over flere år, og særlig bruk av overtredelsesgebyr etter tilsyn gjennomført i 2014, har ført til en konstruktiv dialog med Kommunenes arbeidsgiver-, interesse- og medlemsorganisasjon (KS) om hvordan det kan legges bedre til rette for kommuners regelverksetterlevelse.
- Etter tilsyn med kameraovervåking i regi av lokalt politi er det tatt kontakt med Politidirektoratet for å koordinere rammene og omfanget av slik overvåking
- I forbindelse med kontroll av kryptering av datasentertrafikk, 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, vil bli kommunisert tilbake til sektoren. For øvrig er disse tilsynene ikke analysert i tilstrekkelig grad til at andre tiltak er bestemt.

Etterkontroller

I 2015 gjennomførte vi etterkontroll med to kommuner der tema var internkontroll og informasjonssikkerhet. Videre gjennomførte vi etterkontroll med Husbanken og med en kommunes bruk av skytjenester. I tillegg legger vi fremdeles negative svar om etterlevelse av internkontrollplikten fra kommuneundersøkelsen vår i 2010 og 2011 til grunn ved utvelgelsen av tilsynsobjekter i kommunesektoren.

Saksbehandlingen

Saksbehandling utgjør en stor del av oppgaveløsningen i Datatilsynet, og det er mange brukere som har en forventning om at vi kan behandle alle sakene vi får inn. Vi har også i 2015 jobbet for å ha en så effektiv avviking av saker som mulig gjennom å prioritere hvilke saker vi skal ta opp til behandling og ved å vurdere hvordan vi jobber med de enkelte sakstypene. I den anledning har vi revidert prioriteringskriteriene vi skal bruke fremover. I forlengelsen av dette arbeidet skal vi i 2016 gå gjennom de interne arbeidsprosessene våre. Vi skal kontinuerlig se etter forbedringer og effektivisering som en del av hvordan vi arbeider.

Forslag til endring i regler for konsesjon og meldeplikt

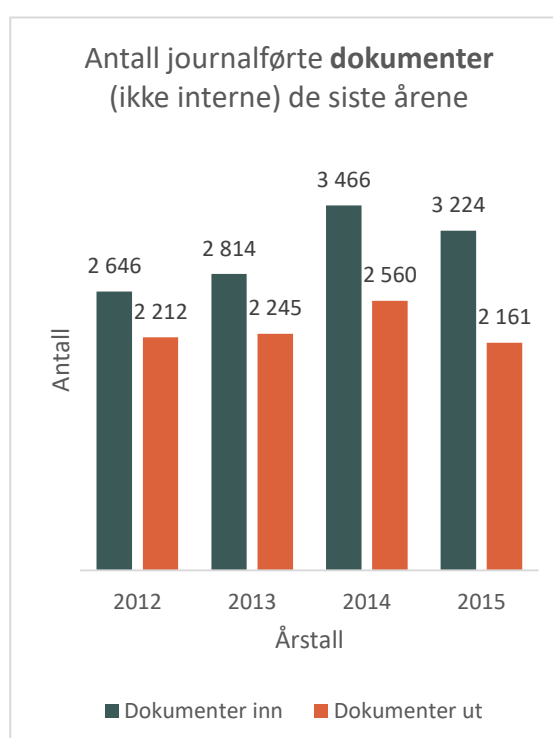
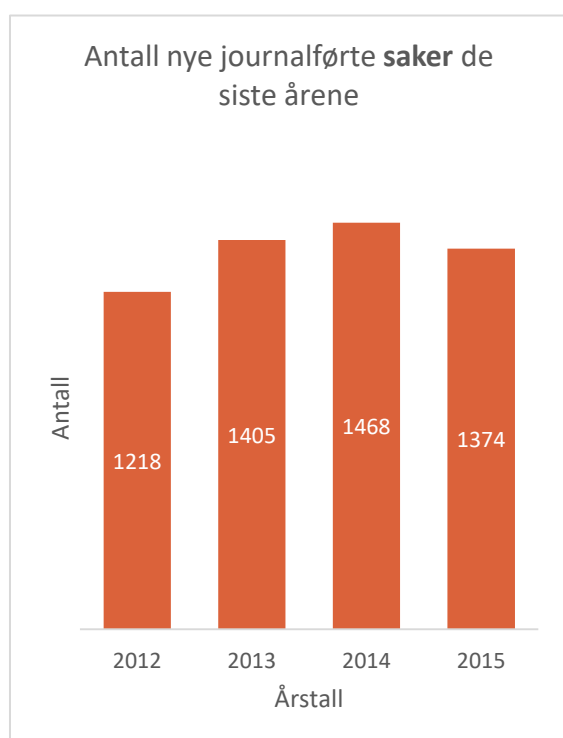
Som en del av Kommunal- og moderniseringsdepartementets (KMD) arbeid med redusere tidstyver, har vi kommet med forslag om å oppheve konsesjons- og/eller meldeplikten for flere nærmere angitte behandlinger av personopplysninger. De behandlingene vi foreslår å oppheve fra plikten, oppleves som tidstyver for de behandlingsansvarlige. Samtidig har de liten informasjonsverdi for publikum som søker etter informasjon om behandling av egne personopplysninger.

Kameraovervåking er en av behandlingene som er foreslått unntatt fra meldeplikten. Det samme gjelder varsling av kritikkverdige forhold i arbeidslivet, samt behandling av personopplysninger ved bruk av kjørebok/flåtestyring.

Vi har dessuten foreslått overfor Helse- og omsorgsdepartementet at det blir utarbeidet en forskrift for behandling av helseopplysninger i befolkningsundersøkelser i stedet for at vi gir konsesjon til denne typen undersøkelser.

Antall saker og saksdokumenter

I løpet av meldingsåret ble det registrert 1 374 nye saker hos Datatilsynet, noe som er en liten nedgang sammenliknet med året før. Volummessig synes 2015 som et ganske normalt år i denne sammenheng. Nedgangen i antall saker og antall innregistrerte dokumenter er omtrent like stor (om



lag 6,5 prosent), noe som viser at sakene inneholder like mange dokumenter som i 2014. Det er en indikasjon på at kompleksiteten økte frem til 2014 og har deretter vært stabil.

Saksomkostninger

Generelt merker vi også en viss profesjonalisering av henvendelsene til oss. Flere benytter seg av advokatbistand enn tidligere. Vi har for eksempel hatt flere saker om dekning av advokatkostnader i meldingsåret enn tidligere. Vi har også hatt klagesaker med dette som tema i Personvernemnda, samt én som er påklaget til KMD.

Konsesjoner

Det er en av Datatilsynets lovpålagte oppgaver å ta stilling til konsesjonssøknader. I 2015 mottok vi totalt 249 søknader om konsesjon, og innvilget til sammen 192. Dette er en liten oppgang i forhold til søknader og gitte konsesjoner i 2014.

De fleste konsesjonssøknadene gjelder forskning eller opprettelse av registre innen helsesektoren. Arbeidet med konsesjoner er, ved siden av kontrollsakene, de mest arbeidskrevende oppgavene vi har. Det er viktig å huske at behandling av konsesjonssøknader i realiteten er en forhåndskontroll av om de som søker har tilstrekkelig rettslig grunnlag for det de ønsker å gjøre.

Forhåndskontrollen kan også omfatte andre deler av personopplysningslovens krav, for eksempel om virksomhetene har på plass tilstrekkelige rutiner for internkontroll. Vi kan gjennom konsesjonsarbeidet også kompensere for personvernulemper som behandlingen eventuelt fører med seg ved å stille vilkår for den aktuelle behandlingen.

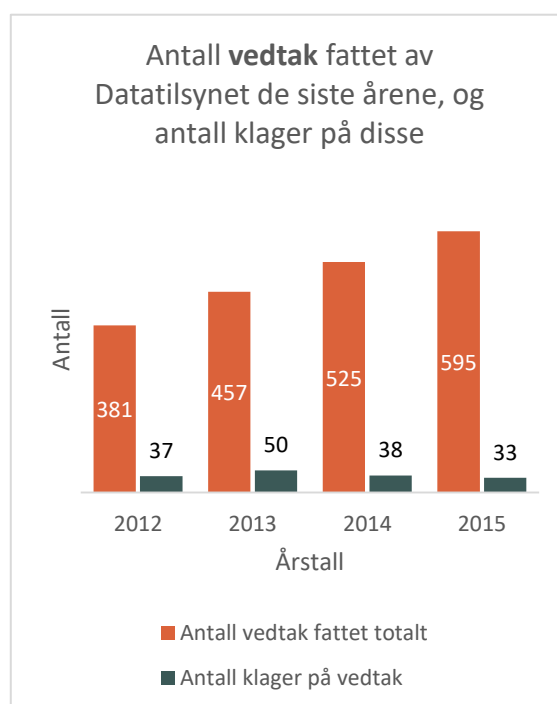
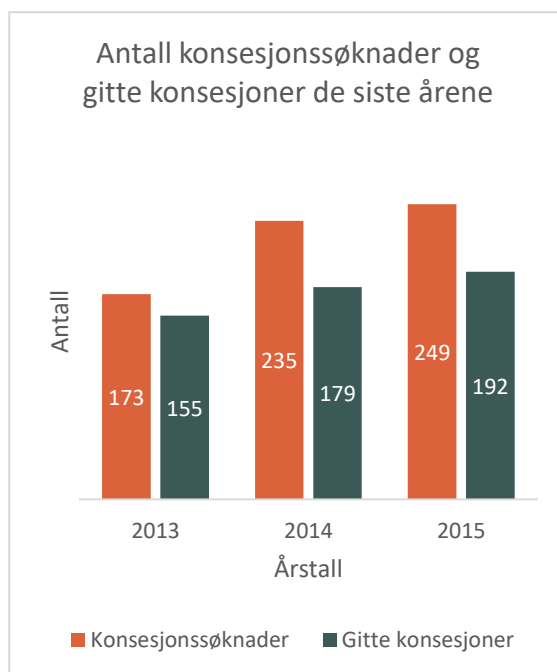
Vedtak og klageomfang

Vi har fattet 595 vedtak i 2015. Det er en økning sammenliknet med tidligere år.

De fleste av beslutningene knytter seg til behandling av konsesjonssaker som utgjør om lag 35 prosent.

Tallene i år fremkommer av en kategorisering av dokumenter i vårt saksbehandlingssystem hvor saksbehandler angir med stikkord hva dokumentet inneholder. Dette er nytt for 2015. Tidligere har vi kommet frem til tallene etter manuelle tellinger. Det vil si at det er en viss usikkerhet i tallene, men vi mener trenden likevel er tydelig – vi fatter stadig flere vedtak.

Klageomfanget er fortsatt svært lavt sammenliknet med antallet avgjørelser vi fatter i form av vedtak. Vi opplever stort sett at vedtakene våre blir



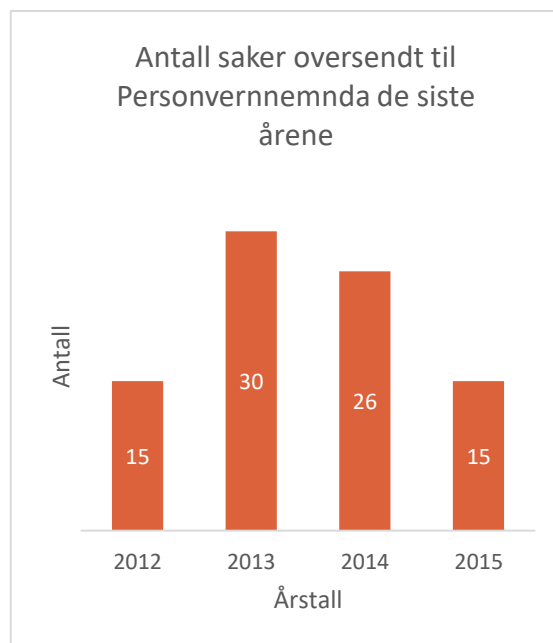
akseptert. Vi har fortsatt utfordringer knyttet til beslutninger om **ikke** å ta opp saker til behandling. Personvernemnda tok i 2014 konkret stilling til en del saker om våre prioriteringer. Nemnda har imidlertid ikke avgjort spørsmålet om denne typen beslutninger faktisk kan påklages. Datatilsynet vil prøve å få en endelig avklaring på dette spørsmålet via Justisdepartementet i 2016. Det er ønskelig med en slik avklaring da klagebehandling er ressurskrevende, og vi ønsker forutsigbarhet på hvilke beslutninger vi kan gjøre med endelig virkning.

Saker oversendt Personvernemnda

I 2015 sendte vi 15 saker til Personvernemnda. Det er færre enn året før, men sammenlignet med tidligere år er det ikke et unormalt lavt antall. Av de sakene som er sendt over i 2015, er det så få som er avgjort av nemnda at det ikke er utarbeidet noen statistikk over i hvilken grad klagene er gitt medhold eller ikke. Kun to av sakene fra 2015 er behandlet av nemnda ved årets slutt.

Fullstendig oversikt over antall saker som ble oversendt til nemnda kan sees under *Vedlegg*. Der er det også tatt med tre saker vi sendte over i 2014, men som ble registrert hos Personvernemnda i 2015. Som oversikten viser er en av disse sakene heller ikke ferdig behandlet.

Erfaringen generelt er som tidligere at vi opplever at vi i tilstrekkelig grad får medhold i sakene vi sender til Personvernemnda. Saker som blir gjort om, er typisk saker som er komplekse eller som inneholder problemstillinger knyttet til samfunnsutvikling og ny teknologi.



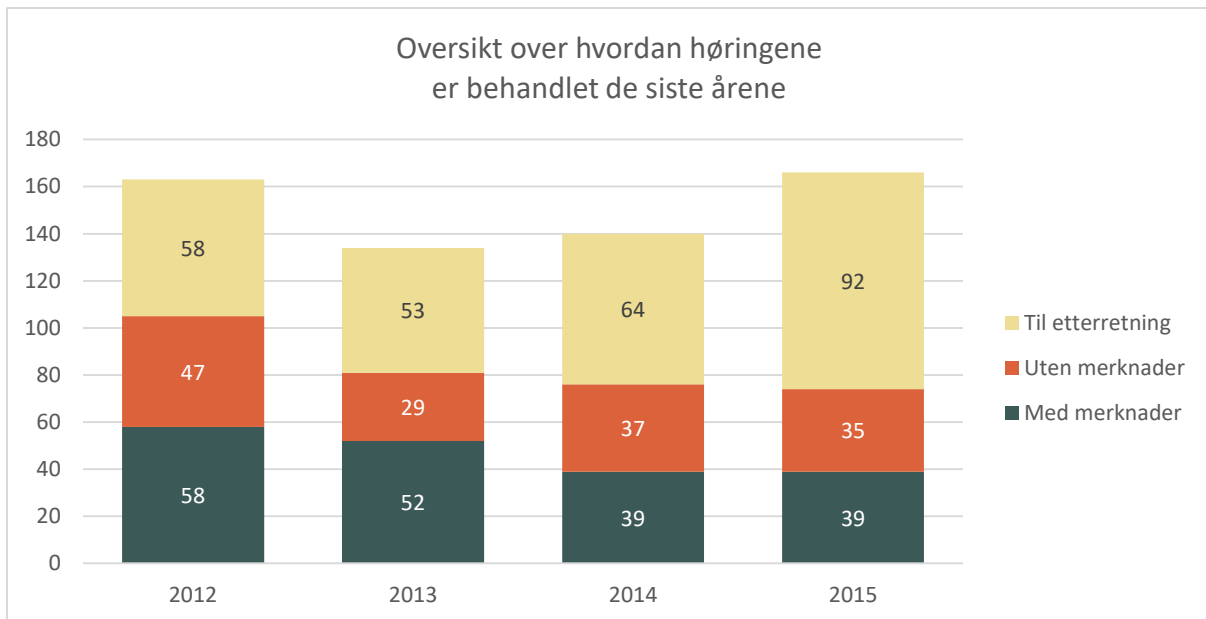
Datatilsynet som høringsinstans

I 2015 har vi gitt merknader til 39 høringer vi har mottatt, noe som er et normalt omfang, selv om det er mottatt flere invitasjoner enn tidligere (se fullstendig liste over høringer under *Vedlegg*). På samme måte som i 2014, er det Justisdepartementet vi avgir flest høringsuttalelser med merknader til.

Vi mener at vi i 2015 har lykket godt med velge ut de hørings sakene som har konsekvenser for personvernet, og at vi har hatt rimelig godgjennomslagskraft med våre uttalelser. Les mer om enkelthøringer innenfor de respektive fagområdene under *Årets viktigste aktiviteter*.

Oversikt over antall høringer vi har fått til vurdering de siste årene:

	2012	2013	2014	2015
Totalt antall høringer	163	134	140	166



Avviksmeldinger

Hendelser som har medført uautorisert utlevering av personopplysninger der konfidensialitet er nødvendig, skal rapporteres til Datatilsynet (personopplysningsforskriften § 2-6).

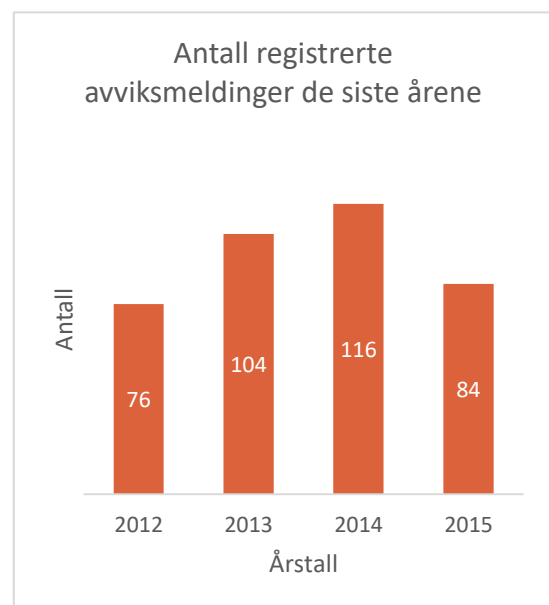
Rapporterte avvik er en indikator på hvor godt virksomhetene fanger opp avvik og kjenner til rapporteringsplikten for disse.

Frem til 2014 så vi en økning i antall avvik som ble meldt inn til oss, mens i 2015 var det derimot en nedgang i meldte avvik.

I meldingsåret analyserte vi sakene fra 2014 for å se om de faktisk var meldepliktige etter personopplysningsforskriften. Konklusjonen var at de fleste sakene falt innunder plikten som følger av § 2-6, og at en svært liten andel av sakene falt klart utenfor.

Analysen avdekket også at den vanligste grunnen til å melde avvik til Datatilsynet er feilforsendelser. Hele 48 prosent av avviksmeldingene som ble registrert i 2014 var rapporter om feilsendinger – analoge og digitale.

Erfaringen er imidlertid at kjennskapen til personvernreglene (og dermed også plikten etter § 2-6) er liten, og at en nedgang i antallet saker meldt inn til oss indikerer at tilstanden ikke har bedret seg når det gjelder uønskede hendelser. Det blir



interessant å følge med utviklingen videre. Forslaget til ny personvernforordning inneholder nye regler for avvikhåndtering, og det ligger an til at plikten til å melde avvik blir videre enn den er i dag.

Bruk av administrative sanksjoner

Vi benytter oss av administrative sanksjoner kun i et fåtall saker. Som en etterfølgende sanksjon kan vi utstede overtredelsesgebyr, mens for å sikre gjennomføring av vedtak, kan vi pålegge tvangsmulkt (for eksempel et beløp per dag) frem til våre pålegg er etterkommet. Sanksjoner av denne typen er, og skal være, forbeholdt de mer alvorlige overtredelsene som i høy grad utfordrer rettighetene loven gir den registrerte. Vi har ikke benyttet tvangsmulkt i løpet av året.

I sakene hvor vi benytter overtredelsesgebyr, er det særlig konsekvensene av bruddet vi vurderer. Vi ser også på maktforholdet mellom behandlingsansvarlig og individ. Det siste er typisk i arbeidslivssaker om ulovlig innsyn i e-post og bruk av opplysninger fra kjørebøker til andre formål enn det som er avtalt.

Vi har hatt flere saker hvor personopplysninger innhentet ved bruk av overvåkingskameraer har blitt publisert på internett eller det har skjedd annen ulovlig utlevering. Dette er en bruk av opplysninger den registrerte (den avbildede) ikke kan vegre seg mot på noen effektiv måte. Noen av sakene minner om selvtækt, da den behandlingsansvarlige ønsker informasjon om personer de mener begår lovbrudd. Dette er primært politiets oppgave og utlevering til andre enn politiet er ikke tillatt, og anses som et grovt brudd på dette forbudet. Derfor er overtredelsesgebyr benyttet i slike tilfeller.

Erfaringen viser at når noe først er publisert på nett, mister avsenderen kontrollen over opplysningene og potensialet for at det blir en varig krenkelse av personvernet er stor. Dette hensynet er med på å begrunne hvorfor Datatilsynet reagerer med overtredelsesgebyr i slike saker.

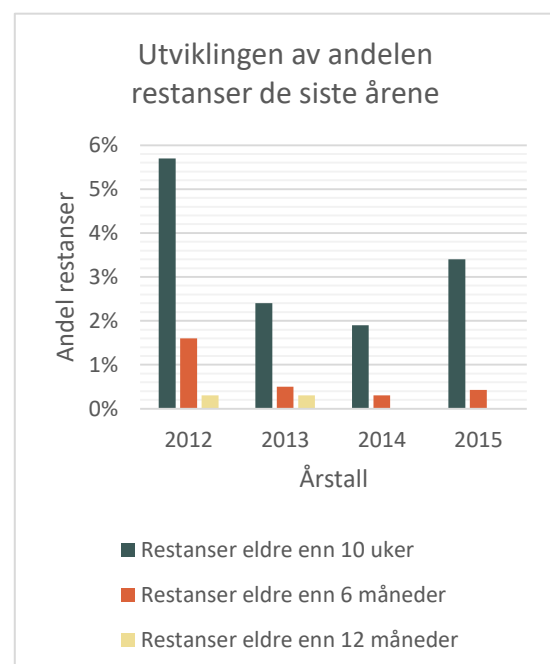
Mange av de offentlige virksomhetene vi har kontrollert har dessuten så store mangler i sin internkontroll at vi har sett oss nødt til å ilegge overtredelsesgebyr. Et mangelfullt, eller fravær av, internkontrollsystem øker potensialet for brudd på personopplysningsloven. Større virksomheter er mer sårbare for feil uten en systematisk oppfølging av at rutiner følges – rutiner som er ment å sikre etterlevelse av plikter. Denne økte risikoen for at personopplysningsloven ikke følges, er grunnen til at vi ser alvorlig på mangler ved internkontrollen.

Flere av de konkrete sakene der det er gitt overtredelsesgebyr, er nærmere omtalt innenfor de respektive fagområdene i *Årets viktigste aktiviteter*. Se for øvrig fullstendig liste over hvilke virksomheter vi har gitt overtredelsesgebyr under *Vedlegg*.

Restanser

Datatilsynet har som mål at saker og henvendelser skal være besvart eller håndtert på annen måte innen ti uker. De aller fleste sakene og henvendelsene blir besvart med en gang eller i løpet av fire uker.

Ved årsskiftet hadde 3,4 prosent av sakene tatt mer enn ti uker å behandle. Det er noe dårligere enn tidligere år. Det er likevel ikke alarmerende og kommer av økt fravær av medarbeidere i noen av faggruppene deler av året. Det positive er at vi som i



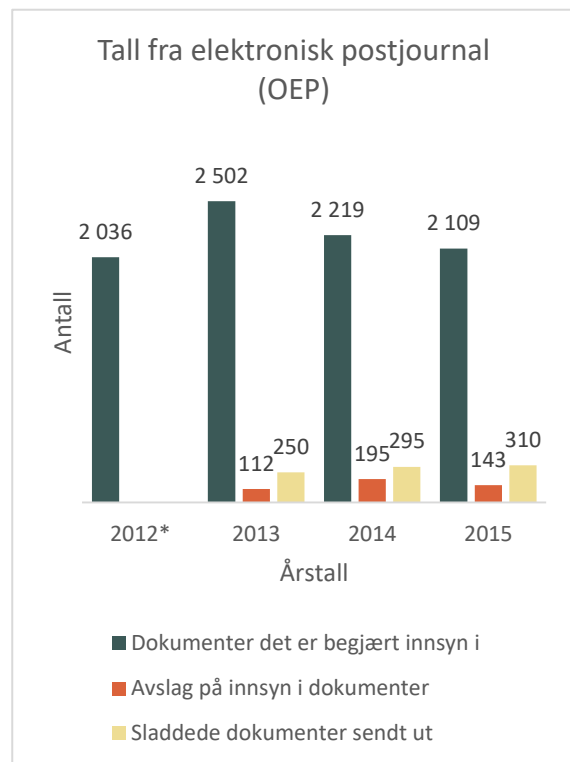
fjor ikke har saker eldre enn 12 måneder. Vi mener vi har god kontroll på saksmengden ved å etablere rutiner for oppfølging av eldre saker.

Offentlighetsloven og innsynskrav

I 2015 håndterte Datatilsynet innsynskrav om til sammen 2 109 dokumenter via elektronisk postjournal (OEP), noe som er omtrent som året før. Vi har laget interne rutiner som fungerer godt med en god 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 forsøker hele tiden å etterleve reglene om meroffentlighet. Vi ser en forsiktig økning i antallet sladdede dokumenter som vi har sendt ut. Det mener vi er en naturlig utvikling ettersom kompleksiteten i sakene øker og mengden beskyttelsesverdig informasjon som vi mottar synes å øke. Vi har i forbindelse med en del kontroller bedt om sikkerhetsdokumentasjon som vi i stor grad ikke leverer ut, eller bare leverer ut delvis.

Vi benytter betydelige ressurser på denne oppgaven, men planlegger i 2016 å benytte digitale kommunikasjonsløsninger direkte fra saksbehandlingssystemet i større grad enn vi har gjort i 2015.



* Vi har ikke tall fra OEP på antall avslag på innsyn eller sladdede dokumenter som ble sendt ut fra tidligere enn 2013.

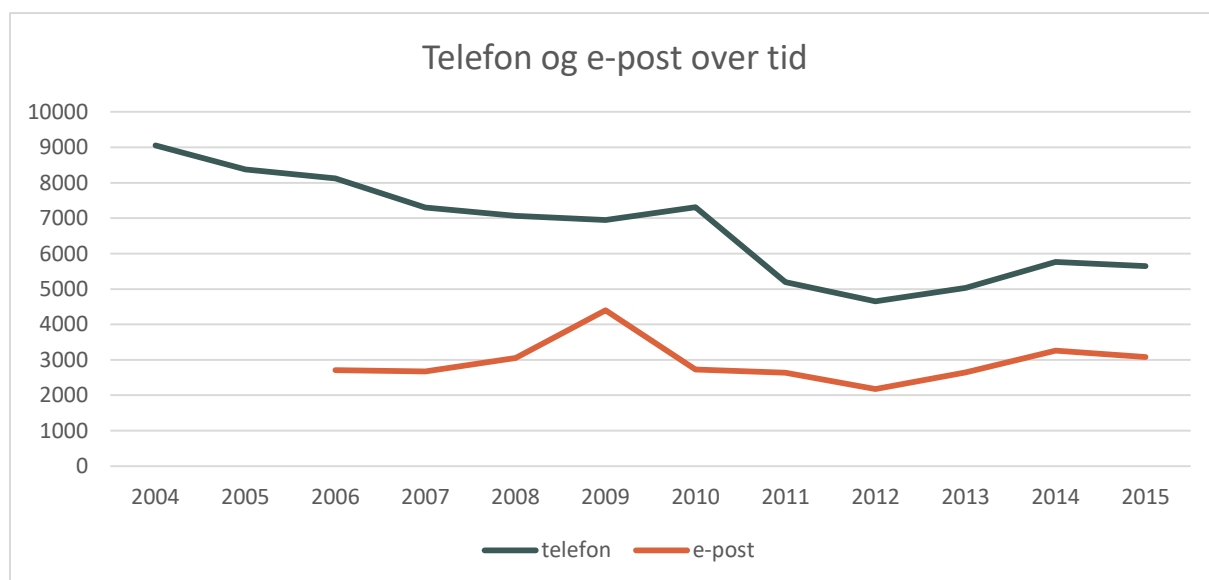
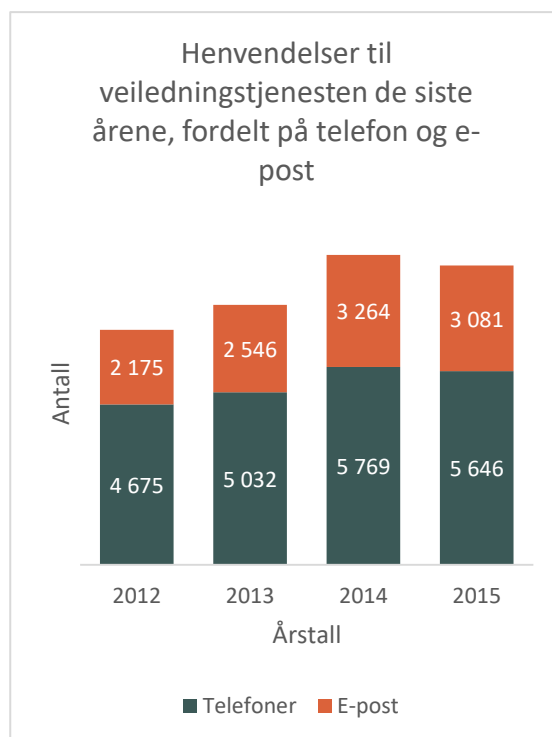
Veiledningstjenesten

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 virksomheter til å følge pliktene i personvernlovgivningen.

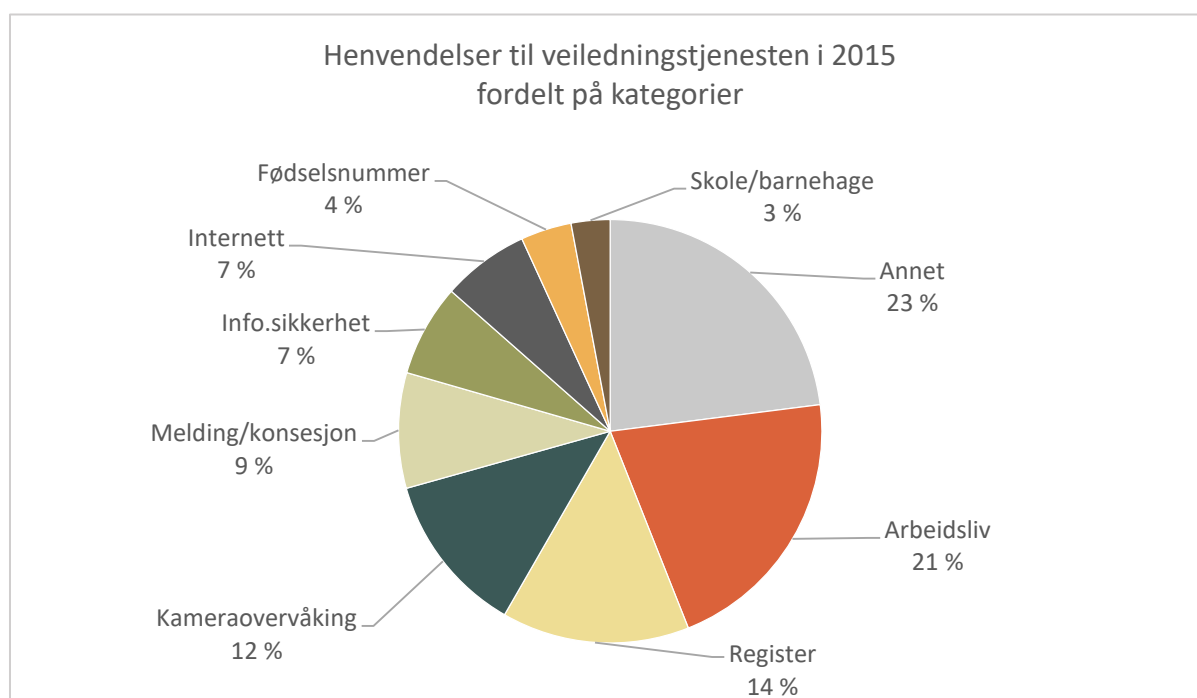
Det er stort spenn i spørsmålene, og de er av både juridisk, teknisk og sikkerhetsmessig art. Svarene vi gir er av veiledende karakter og er ikke bestemmende for rettigheter eller plikter, i motsetning til vedtak som fattes i den mer tradisjonelle saksbehandling.

I løpet av 2015 har veiledningstjenesten besvart 8 727 henvendelser. Dette består av 3 081 henvendelser på e-post og 5 646 per telefon. Antallet er ganske likt året før, men vi ser en liten nedgang med 306 færre henvendelser totalt. Nedgangen er primært en reduksjon i antallet e-posthenvendelser.

Det har de siste ti årene vært en nedgang i antall telefonhenvendelser. Hva forklaringen på det er, er vanskelig å si, men kanskje er stadig mer oversiktlige og utfyllende nettsider noe av forklaringen.



Hva handler henvendelsene om?



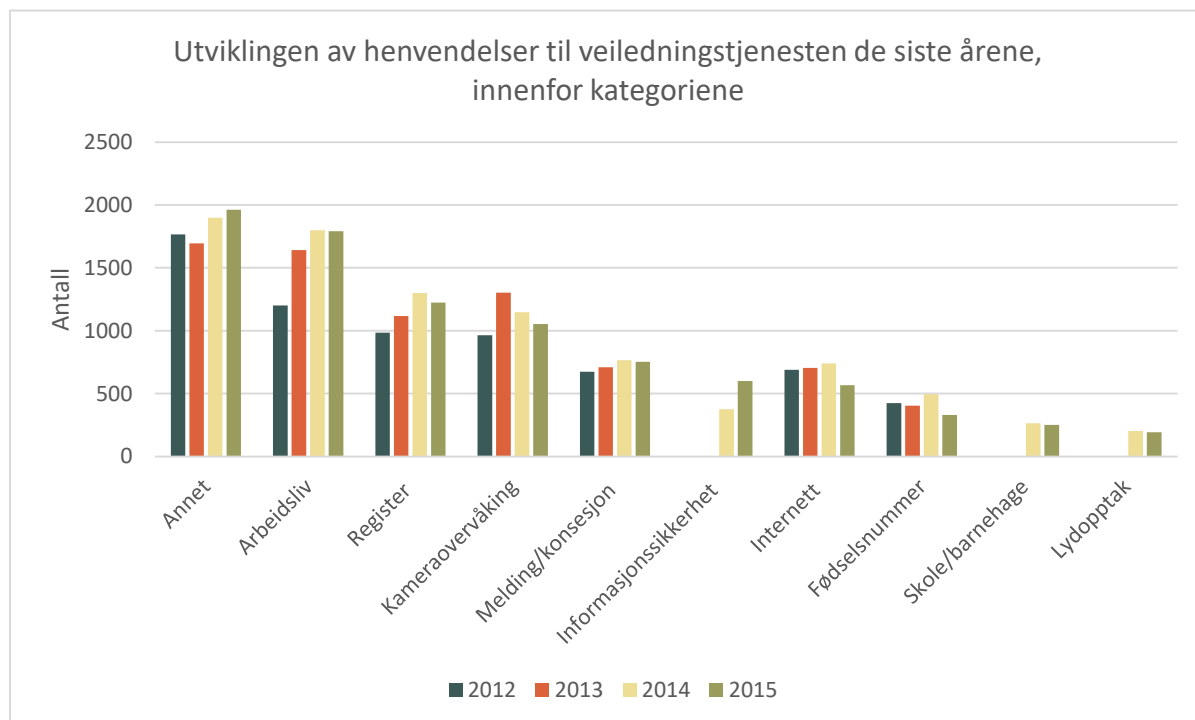
Oversikt over antall henvendelser til veiledningstjenesten de siste årene fordelt på ulike kategorier:

Kategori	2012	2013	2014	2015
Arbeidsliv	1 201	1 642	1 798	1 791
Register (helse-, kreditt-, kunde-, medlems- og offentlige)	985	1 118	1 301	1 223
Kameraovervåking	965	1 302	1 148	1 053
Internett	689	705	741	568
Melding/konsesjon	675	711	766	752
Fødselsnummer	424	405	495	331
Informasjonssikkerhet	-	-	376	600
Skole/barnehage	-	-	265	253
Lydopptak	-	-	204	194
Annet	1 911	1 695	1 939	1 962
Totalt	6 850	7 578	9 033	8 727

Tabellen viser at antallet henvendelser innen hver kategori i hovedtrekk har vært ganske stabilt de siste fire årene. Antall henvendelser innen kategorien «Informasjonssikkerhet», har imidlertid gått opp fra 276 til 600 henvendelser siden året før, noe som er en oppgang på 60 prosent. Ellers ser vi en nedgang på 23 prosent i internettrelaterte spørsmål, samt 33 prosent nedgang i spørsmål om fødselsnummer.

Når det gjelder informasjonssikkerhet, kan oppgangen i antall henvendelser delvis skyldes endring i praksis for hvordan sikkerhetshenvendelser blir behandlet og registrert. I 2015 var Safe Harbor og ny EU-forordning to store enkelttemaer for Datatilsynet. Vi har ikke tall på hvor mange telefon-

henvendelser vi har fått om dette, men på e-post fikk vi 25 henvendelser som nevner Safe Harbor, og rundt halvparten av dette angående den nye forordningen.



En beskrivelse av innholdet i henvendelsene

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

Arbeidsliv

Hele 21 prosent av henvendelsene til veiledningstjenesten dreide seg om arbeidslivsrelaterte spørsmål. Mange av spørsmålene handler om kontroll og overvåking av ansatte. Mange har 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.

Register

14 prosent av henvendelsene var ulike spørsmål knyttet til en eller annen form for register. Det vil si spørsmål 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 offentlige registre, samt helseregistre og registrering i forbindelse med kredittopplysningsvirksomhet.

Kameraovervåking

Kameraovervåking er en annen stor kategori som utgjorde 12 prosent av henvendelsene. Kameraovervåking i arbeidslivet kategoriseres under «Arbeidsliv», derfor er den totale andelen henvendelser innen dette temaet i realiteten noe høyere.

Kameraovervåking i borettslag og i nabosituasjoner er henvendelser som går igjen. Andre henvendelser gjelder bruk av webkamera, samt spørsmål om lovligheten av kameraer i for eksempel naturen eller i båthavner. Tjenesten får også en del spørsmål fra virksomheter som har, eller ønsker å sette igang, kameraovervåking.

Melding og konsesjon

Åtte prosent av henvendelsene gjaldt spørsmål om hvorvidt en behandling er melde- eller konsesjonspliktig, og hvordan melding og konsesjon skal leveres. En del av spørsmålene handlet også om endring og oppfølging av melding og konsesjon.

Informasjonssikkerhet

Sju prosent av henvendelsene gjaldt informasjonssikkerhet. Spørsmålene handler gjerne om sikker forsendelse, samt overføring og lagring av personopplysninger, både fysisk og elektronisk. Bruk av skytjenester og kryptering er temaer som går igjen. Det kommer også inn en del spørsmål om bruk av SMS og e-post til forsendelse av informasjon.

Henvendelser som gjelder dokumenter eller personopplysninger som har kommet på avveier og generelle henvendelser om hvilke plikter som gjelder med tanke på informasjonssikkerhet, faller også inn under denne kategorien.

Merk at spørsmål om informasjonssikkerhet også kan falle inn under de andre kategoriene. Totalt antall henvendelser om dette temaet til veiledningstjenesten, er derfor en del høyere enn det som fremgår her.

Internett

Ulike henvendelser om internett sto for sju prosent av henvendelsene. Mange av spørsmålene handler om sletting av uønsket informasjon. En god del av disse gjelder retten til å bli glemt, som følge av den såkalte Google-dommen. Denne dommen gir den registrerte mulighet til å få avindeksert søketreff med informasjon som er feil, irrelevant eller ikke lengre aktuell.

Tjenesten mottar også en god del spørsmål om regler for bruk av sosiale medier, og publisering av bilder på nett utgjør en stor del av disse. 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.

Fødselsnummer

Denne kategorien har eksistert i mange år, og antallet henvendelser om dette har hatt en svak nedgang de siste årene. Selv om det er et snevert tema, utgjør det fire prosent av henvendelsene. Spørsmålene knytter seg først og fremst til bekymrede privatpersoner som har opplevd at fødselsnummeret kommer på avveier, eller som føler ubehag ved å måtte oppgi fødselsnummeret sitt i ulike sammenhenger. Det er også noen spørsmål fra virksomheter om hvorvidt de har lov til å benytte seg av fødselsnummer.

Skole og barnehage

Dette er en relativt liten kategori og omfattet tre prosent av henvendelsene til tjenesten. Skole og barnehage var et satsningsområde for Datatilsynet i både 2014 og 2015. Flere av henvendelsene er knyttet til informasjonssikkerhet, som for eksempel ved bruk av læringsplattformer og lagring i skytjenester. Andre spørsmål gjaldt hvilke opplysninger som kan lagres om barnet, hvor lenge opplysningene kan oppbevares og hvilke opplysninger som kan overføres mellom skole og barnehage. Det er også en del henvendelser om fotografering og filming av barn.

Lydopptak

Denne kategorien utgjorde bare én prosent av henvendelsene. De fleste spørsmålene handlet om kunder som lurer på om virksomheten de har snakket med på telefon har lov til å gjøre lydopptak av samtalene.

Annet

Kategorien «Annet» inneholder 22 prosent av alle henvendelsene. Den største andelen i denne kategorien er henvendelser som vi ikke finner plass til ellers i kategoriseringen. Dette er ofte spørsmål som faller utenfor personvernlovgivningen. Et eksempel kan være spørsmål om bruk av personopplysninger til journalistiske formål. Ellers er det spørsmål om generell veiledning i personopplysningsloven, om overføring av personopplysninger til utlandet og om databehandleravtaler. Det er også her vi registrerer personvernspørsmål som er regulert av andre lover, slik som spørsmål knyttet til offentlighetsloven eller om brudd på taushetsplikt etter forvaltningsloven.

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 personvern hensyn. 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 selve navet i all vår kommunikasjonsvirksomhet og må derfor forvaltes deretter. 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

Størrelsen på nettstedet er et viktig styringsparameter. Nettstedet skal ikke vokse ukontrollert, og nettsider skal redigeres og slettes når de blir gamle og overflødige. Antallet sider på datatilsynet.no har ikke steget med mer enn 60 i løpet av 2015, ifølge Google Site Search. Det kan leses som en indikasjon på at nettstedet røktes på en god måte.

Antallet besøk på nettstedet går imidlertid ned. Dette er i tråd med en mer generell utvikling. Samtidig ser vi at hver besøkende på datatilsynet.no oppsøker noen flere sider, altså at de blir lenger når de først har kommet inn.

Oversikt over nøkkeltall fra nettstatistikken på datatilsynet.no:

	2014	2015
Antall sider på nettstedet (Google site search)	2 300	2 360
Antall besøk til nettstedet	185 000	148 000
Antall sidevisninger	460 000	413 000
Antall sidevisninger pr besøk	2,4	2,7
Gjennomsnittlig besøksvarighet	3 min og 29 sek	3 min og 47 sek
Antall søk i søkemotoren på datatilsynet.no	30 000	36 300
Andel besøk fra mobile enheter	16 prosent	16 prosent
Antall publiserte nyhetssaker	63	58

Personvernblogg, sosiale medier og debattinnlegg

Personvernbloggen.no er nå godt etablert etter nær tre års drift. Den fungerer etter intensjonen og er et rom hvor vi kan reise andre problemstillinger, og ta opp andre temaer, enn vi kan på den ordinære nettsiden. Sjangermessig og i temavalgene har bloggen funnet sin form, og i løpet av 2015 har vi fått nye skribenter blant de ansatte.

Vi følger systematisk med på omtale av Datatilsynet og temaet personvern på Twitter, og besvarer raskt de fleste spørsmål og kommentarer som kommer via denne kanalen. Vi har i 2015 hatt ni kronikker og debattinnlegg i ulike papirbaserte medier. Vi har også produsert flere fagartikler som er blitt tatt inn i fagblader knyttet til skole, barn og unge.

Oversikt over noen sentrale tall:

	2012	2013	2014	2015
Innlegg på Personvernbloggen	-	41	50	40
Besøk på Personvernbloggen	-	8 000	20 000	-*
Twittermeldinger	391	220	193	177
Twitterfølgere	7 500	10 065	12 392	14 100
Kronikker og debattinnlegg i andre medier	10	8	9	9

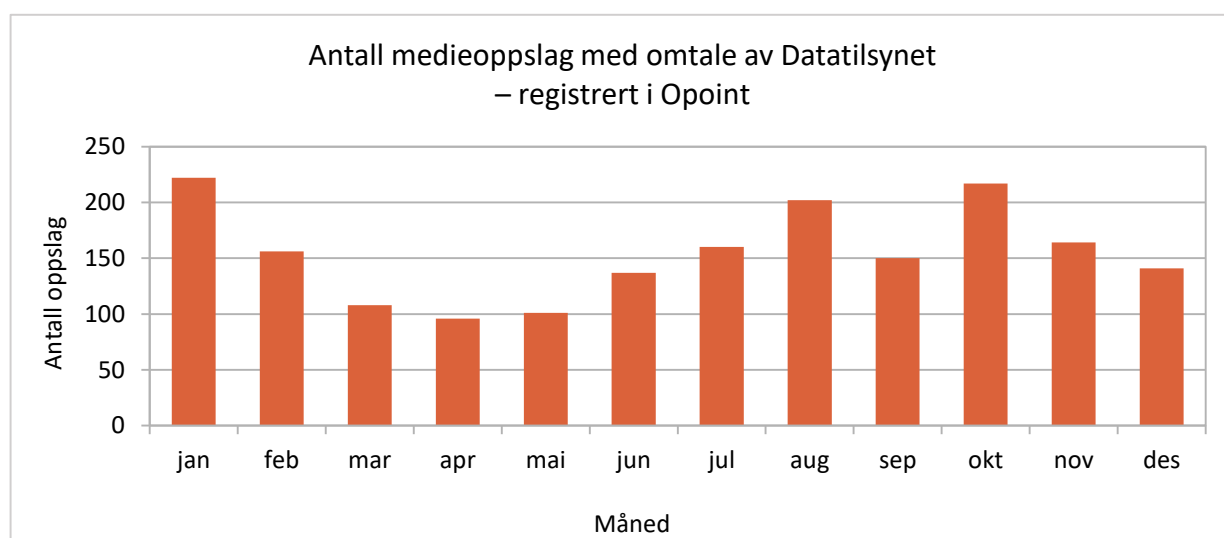
*Vi har ikke besøkstall for Personvernbloggen for 2015 på grunn av en feil i statistikkverktøyet.

Mediekontakt

I løpet av året har Datatilsynet registrert 650 besvarte mediehenvelseler. Det er noe lavere enn året før.

	2012	2013	2014	2015
Mediehenvelseler	876	850	800	650

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 mediehenvelseler som går direkte til direktøren, øvrig ledelse eller fagdirektører. Det reelle antallet er derfor noe høyere enn de registrerte henvelselerne. Medieovervåkingstjenesten Opoint har registrert til sammen 1 843 oppslag i norske nettbaserte medier hvor Datatilsynet er nevnt.



Som det går fram av figuren over, var det flest omtaler av Datatilsynet i media i januar, august og oktober. Dette skyldes enkelte saker som fikk særlig stor oppmerksomhet. Noen av temaene som fikk omtale gjennom året var:

- Den internasjonale personverndagen 28. januar, og konferansen Teknologirådet og Datatilsynet arrangerte i fellesskap i den anledning
- Justisdepartementets forslag om mobilregulerte soner
- Kunnskapsdepartementet vil kartlegge barn uten foresattes samtykke
- Barn og unges personvern. Overvåking fra foreldrenes side, og publisering av bilder av barn.
- Retten til å bli glemt. Søkemotorer og av-indeksering. (EU-domstolen og Google)
- Kameraovervåking – i drosje, båthavn, restaurant, i politiets regi og lignende
- Overtredelsesgebyr til kommuner og statlige etater for manglende internkontroll
- Overtredelsesgebyr til Justisdepartementet for publisering av sensitive personopplysninger i egenprodusert film
- Forskning på fremmedkrigere – påstand om at Datatilsynet hadde stoppet forskningen
- Universitetet i Oslo publiserte fødselsnummer på Internett – igjen
- Bruk av «black box» i bil for billigere forsikring
- Avtale om overføring av personopplysninger til USA (Safe Harbor) kjent ugyldig av EU-domstolen
- Facebook – nye tjenester og brukervilkår
- Tingenes internett, bruk av smartteknologi
- Kommersialisering av personopplysninger – kartlegging og rapport fra Datatilsynet
- Enighet i EU om nye felles personvernregler (personvernforordning)

Det er NRK.no som har flest omtaler av Datatilsynet, fulgt av Aftenposten og Adresseavisen.

Personvern knyttet til mediernes publisering av skattelister har tidligere år fått svært stor oppmerksomhet. I 2015 mottok vi imidlertid kun to mediehenndelser om temaet og det ble bare et par mindre oppslag om muligheten til å gjøre anonyme søk. Skattelisteopplysningene behandles nå på en måte som i liten grad vekker kritiske reaksjoner.

Vi har også i meldingsåret lagt en del innsats i å ta initiativ til redaksjonelle artikler og nyhetsinnslag. Vi har særlig fått mange medieoppslag basert på egne initiativ når det gjelder barn og unges personvern. Det gjelder nærmere bestemt foreldres publisering av bilder av egne barn, GPS-overvåking og nettvett. Læringsressursen Dubestemmer.no, om personvern og nettvett, har også fått god markedsføring via redaksjonell omtale. Du Bestemmer-prosjektet er nærmere omtalt under *Årets viktigste Aktiviteter, Barn skole og utdanning*.

Det er viktig for oss å benytte alle de mulighetene vi får til å skape oppmerksomhet og debatt om personvernsspørsmål. Vi legger derfor stor vekt på å prioritere deltakelse i debatter i radio og på TV om temaer som berører personvernet. I meldingsåret har vi for eksempel deltatt jevnlig i NRKs Dagsnytt 18, NRK Ekko og NRK Kulturnytt. Vi har videre stilt opp ved flere anledninger i TV2 Nyhetskanalen.

Foredragsvirksomheten

I tillegg til synlighet i mediene legger vi også vekt på å være tilstede på arenaer der vi møter representanter fra virksomheter, interesseorganisasjoner og andre aktører. Å stille med foredragsholdere, innledere, holde innlegg eller delta i paneldebatter på ulike arrangementer, er en viktig del av dette arbeidet.

I 2015 har vi holdt 159 foredrag på eksterne arrangementer, mot 170 året før:

	2012	2013	2014	2015
Antall	118	149	170	159

Vi får en rekke forespørsler om å holde foredrag gjennom hele året. Disse forespørslene vurderer vi ut fra satsingsområdene i virksomhetsplanen vår, antall deltakere, tema og kapasitet på aktuelt tidspunkt. Vi har et mål om å holde mellom 120 og 150 eksterne foredrag i løpet av året.

Foruten generelle foredrag om personvern, overvåking og Datatilsynets oppgaver, har vi holdt flest foredrag om:

- informasjonssikkerhet og internkontroll
- skytjenester
- helse, særlig om velferdsteknologi og tilgangsstyring
- Big Data og kommersiell utnyttelse av personopplysninger

Vi så også en økning i forespørsler om å holde foredrag om EUs nye personvernforordning og Safe Harbor. Dette er tema som nok vil bli enda mer aktuelle i 2016.

ÅRETS VIKTIGSTE AKTIVITETER

Justissektoren

Individets rett til å bestemme over egne personopplysninger gjelder ikke uinnskrenket. I justissektoren finnes det flere tungtveiende hensyn som taler for at staten kan gripe inn i den enkeltes rettssfære. I mange tilfeller behandler offentlige myndigheter personopplysninger uten at den enkelte kan kontrollere eller påvirke det. Retten til informasjon er dessuten begrenset. Som et resultat av dette, har hver enkelt færre muligheter til å ivareta sine interesser enn ellers. Det er derfor særlig viktig at tilsynsmyndighetene ser etter at individets rettigheter ivaretas på disse områdene.

Datatilsynet spiller, ved siden av politiet selv, en sentral rolle når det gjelder etterlevelse av politiregisterloven som trådte i kraft i 2014. Vi skal føre tilsyn med at loven med forskrifter blir fulgt, at feil eller mangler blir rettet, kontrollere at opplysningene om de registrerte blir behandlet i samsvar med loven og se til at reglene blir fulgt dersom den registrerte ber om innsyn. Datatilsynet har både en påleggs- og en anmerkningskompetanse.

Gjennomførte aktiviteter

Tilsyn

Høsten 2015 ble det første stedlige tilsynet i medhold av politiregisterloven gjennomført. Tilsynsobjektet var Kripas, og tema for kontrollen var politiets behandling av personopplysninger i DNA-registeret som Kripas er behandlingsansvarlig for. Kontrollrapporten ventes å være ferdig i februar 2016.

Sentrale høringsuttalelser

Utredning om advokaters behandling av personopplysninger

I Advokatlovutvalgets utredning NOU 2015:3 «Advokaten i samfunnet» tas det til orde for at det bør utarbeides særlige regler for behandling av personopplysninger i advokatvirksomhet. Vi ga i vår høringsuttalelse støtte til et slikt initiativ, men understreket hensiktsmessigheten med å avvente nærmere regulering til etter at den generelle databeskyttelsesforordningen er på plass. Vi kommenterte også forholdet til personopplysningslovens konsesjons- og meldeordning, samt forhold angående arkivhold og informasjonssikkerhet. Videre kommenterte vi advokatlovutvalgets forslag til nye lovbestemmelser om unntak fra advokaters taushetsplikt, og påpekte at Datatilsynet bør ha tilgang til den informasjonen som er nødvendig for å kunne føre kontroll med advokaters behandling av personopplysninger.

Lovforslag om politiets bruk av falske basestasjoner

Et lovforslag som kom fra Justisdepartementet i desember 2014, gikk ut på å gi politiet utvidede muligheter til å bruke falske basestasjoner, og det uten domstolskontroll. De foreslåtte lovbestemmelsene vil gripe inn i enkeltindividers frihet og personlige integritet. Slike tiltak må etter vår oppfatning alltid være forankret i lovregler som er presise, klare og forsvarlig begrunnet. Lovbestemmelsene må dessuten utformes på en slik måte at befolkningen gis klare indikasjoner på i hvilke sammenhenger, og under hvilke vilkår, myndighetene gjennomfører tiltak som potensielt kan ramme deres privatliv og integritet. Konsekvensene av lovvedtak i samsvar med forslagene må også utredes, og det er den som foreslår tiltaket som må analysere konsekvensene av tiltakene, også

utover den politimessige nytten de kan tenkes å ha. Vi skrev at vi var kritiske til endringer i politiloven og ekomloven som kan ramme kommunikasjonen og gripe inn i personvernet til et stort antall personer som ikke er mistenkt for å ha gjort noe straffbart. Vi påpekte videre at lovforslagene ikke sikrer rettsikkerheten til de berørte, og frarådet derfor at lovendringene gjennomføres.

Forslag til endring i psykisk helsevernlov

Utredningen NOU 2014:10 «Skyldevne, sakkyndighet og samfunnsvern» ble sendt på høring sent i 2014, og vi ga vår høringsuttalelse i 2015. Lovforslaget skal sikre at påtalemyndigheten får nødvendige opplysninger for å vurdere om det skal dømmes tvungent psykisk helsevern, men forslaget inneholdt etter vår mening uheldige formuleringer. Forslaget til endring i lov om psykisk helsevern § 5-6 første ledd har som formål å gi rom for at også fagfolk som tidligere har hatt ansvar for siktede personer, kan gi informasjon til påtalemyndighetene. Vi mente at forslaget var for uklart, og at hovedproblemet med den foreslåtte ordlyden var at loven også vil gjelde der det er spørsmål om forvaring skal forlenges – i disse tilfellene er det ikke klart hvem som skal gi den nødvendige informasjonen når den aktuelle personen allerede er domfelt og i fengsel.

Forslag til endringer i sikkerhetsloven

I mai sendte Forsvarsdepartementet forslag til enkelte endringer i sikkerhetsloven på høring. Endringene gikk blant annet ut på å innføre en lovhjemlet plikt for alle virksomheter til å kontinuerlig overvåke godkjente informasjonssystemer for sikkerhetstruende hendelser. Vi mente at departementet burde ha tatt seg tid til en tydeligere analyse av hva som ligger i forslaget. For eksempel var det vanskelig å få inntrykk av hvor mange mennesker som ville berøres av tiltakene som ble foreslått. Dessuten påpekte vi at de foreslåtte metodene og tiltakene teknisk sett er meget komplekse og vanskelige å forstå for høringsinstansene, og at det derfor burde ha vært gitt en grundigere og mer konkret analyse i høringsnotatet. I etterkant av vår uttalelse var vi i møte med Forsvarsdepartementet og redegjorde for hva vi mente de burde vurdere nærmere på veien frem mot en endelig revisjon.

Øvrige aktiviteter

I et brev til Justisministeren høsten 2015 tok vi til orde for opprettelsen av en personvernkommisjon for justissektoren. Initiativet kom som et resultat av politiets datakriminalitetsstrategi, som blant annet angir mulige tiltak for bekjempelse av ulike former for datakriminalitet. Vi mener strategien burde ha inneholdt klarere analyser av personvernkonsekvensene av de samme tiltakene, og har i et posisjonsnotat som er sendt til ministeren, pekt på en rekke svakheter ved strategien.

Internasjonalt

I EU har det i lengre tid pågått forhandlinger om et direktiv om beskyttelse av personopplysninger som behandles for rettshåndhevelsesformål. Dette har pågått parallelt med en dialog (forhandlinger mellom de tre politiske organene i EU – Parlamentet, EU kommisjonen og EUs ministerråd) om den generelle personvernforordningen for å komme frem til et omforent forslag.

Forslaget omfatter både grenseoverskridende og nasjonal databehandling for slike formål. Det omfatter forebygging, etterforskning, oppdagelse og rettsforfølging av straffelovovertridelser, og dessuten beskyttelse mot og forebyggelse av trusler mot den offentlige sikkerhet. Direktivet trer sannsynligvis i kraft våren 2016. Det er imidlertid noe uklart om direktivet får direkte konsekvenser for norsk lovgivning på området, både fordi den eksisterende politiregisterloven bygger på rådets rammebeslutning 2008/977/JIS av 27. november 2008 om vern av personopplysninger i forbindelse med politi- og justissamarbeid i kriminalsaker, og fordi det er uklart om hele direktivet vil være å anse som Schengen-relevant.

Fremtidige utfordringer

I justissektoren er det særlig kampen mot kriminalitet generelt og terror spesielt, som utgjør den største trusselen mot personvernet. I løpet av 2015 har vi sett konturene av flere tiltak som kan bli en realitet i fremtiden, og som vil innebære store inngrep i den enkeltes rettigheter og frihet. Denne debatten vil trolig fortsette, og vil bli prioritert av Datatilsynet også i fremtiden.

Vi ser også behov for klarere regulering av behandling av personopplysninger i forbindelse med bekjempelse av hvitvasking, skatteunndragelser og terrorfinansiering, det vil si områder hvor banker og finansvirksomheter har et lovpålagt ansvar for å kontrollere og treffe tiltak overfor den enkelte.

Barn, skole og utdanning

Datatilsynet har over en treårsperiode sett nærmere på opplæringssektoren. Gjennom møter med aktører i sektoren og kontroller ved en rekke barnehager, grunnskoler og videregående skoler, har vi skaffet oss en viss oversikt over hvilke opplysninger som registreres om barna i barnehager og skoler.

Samlet utgjør registreringene om et barn gjennom et helt utdannelsesløp, et sett med opplysninger som gir et omfattende og detaljert bilde av dette barnets utvikling, samt faglige og sosiale atferd. Det at flere opplysninger om barn lagres digitalt betyr også at spredningspotensialet blir større. Uten tekniske sperrer og gode rutiner er det lettere at opplysningene brukes til andre formål enn det de var ment til, og opplysningene kan med få tastetrykk spres til mange.

Vi har i løpet av denne perioden avdekket at rutinene for å sikre barns personvern i skoler og barnehager er mangelfulle. Samtidig vet vi at bruken av elektroniske og nettbaserte tjenester i skoler og barnehager bare vil øke ytterligere i årene som kommer.

Vårt prosjektarbeid knyttet til personvern i barnehage og skole i tidsrommet 2013-15 hadde som mål at bevisstheten om personvern blant skoleeiere, lærere, foresatte og elever innen 2016 skulle være så høy at Datatilsynet ikke trenger å være på banen med annet enn veiledning. Arbeidet er nå igangsatt.

Gjennomførte aktiviteter

Tilsyn

Høsten 2015 fikk vi informasjon om at en kommune hadde gjennomført full digitalisering av elevmapper i grunnskolene innen kommunen. Vi fikk samtidig indikasjoner på at tilgangsstyringen ikke var tilfredsstillende i den løsningen kommunen hadde valgt. Vi valgte dermed å dra på en kontroll for å undersøke hvilken tilgangsstyring og eventuelle andre sikkerhetstiltak kommunen hadde iverksatt i forbindelse med denne digitaliseringen.

Saken er prinsipielt viktig da den aktuelle kommunen er tidlig ute med digitalisering av elevmapper. De konklusjonene som kommer med hensyn til tilgangsstyring og andre sikkerhetstiltak, vil være førende for andre kommuner som skal starte med digitalisering. Saken er ikke ferdigbehandlet. Endelig kontrollrapport vil bli utarbeidet i første halvdel av 2016.

Sentrale høringsuttalelser

Kunnskapsdepartementet har hatt flere store lovarbeider på høring i 2015 som Datatilsynet har hatt synspunkter til. Vi ønsker å trekke frem disse høringsuttalelsene:

Forslag til endring av barnehageloven

Kunnskapsdepartementet har lagt frem et forslag til endringer i barnehageloven. Endringene skal 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 mener endringen som foreslås vil legge til rette for å innføre en utstrakt måling og sammenligning av barnas ferdigheter. En slik måling har det ikke vært tradisjon for i barnehager i Norge.

På vår tilsynsrunde i 2013-14 påviste vi at det er ulik praksis blant landets barnehager når det gjelder hjemmelsgrunnlag for bruk av verktøy for å kartlegge barnas ferdigheter. Mange baserte bruken på

samtykke fra de foresatte, mens andre mente at de hadde adgang til å gjøre slik kartlegging uten de foresattes samtykke. Vi uttrykte for så vidt et ønske om avklaring av dette spørsmålet, men forslaget som er fremmet går i en helt annen retning enn vi hadde håpet. Istedenfor å styrke de foresattes involvering i saker som gjelder deres barn, legger forslaget opp til en praksis hvor det er fare for at de foresatte blir enda mindre involvert enn i dag.

Saken er ikke ferdigbehandlet i Stortinget.

Utredning om fremtidens skole

I juni leverte Ludvigsenutvalget sin utredning om fremtidens skole. Her tar de for seg ulike typer analyser og målinger av elever, men helt uten noen form for konsekvensanalyse når det gjelder personvernet.

Det er stadig vanligere at opplysninger innhentet for et formål, blir brukt til andre formål uten at de opplysningene gjelder får noen innvirkning på dette. Når utvalget foreslår å bruke læringsanalyse og måling av sosiale og emosjonelle ferdigheter hos barn som et verktøy for måle barns utvikling, er det særlig viktig å vurdere personvernet i slike verktøy.

Dessverre er det en svakhet ved utredningen at den ikke tar opp personvernproblematikk. Den gir heller ikke anbefalinger om hvilke plikter man har etter personvernregelverket når læringsanalyse tas i bruk og når sosiale og emosjonelle ferdigheter vurderes.

Utredning om mobbing i skolen

I juni 2015 kom også Djupedalutvalgets utredning, NOU 2015:2 «Å høre til. Virkemidler for et trygt psykososialt skolemiljø».

I vår høringsuttalelse til denne utredningen viste vi til våre erfaringer fra saksbehandlingen. De tilsier at det er stort behov for veiledning når det gjelder hvordan skolen skal håndtere den innledende fasen hvor mistanke om mobbing eller trakassering oppstår og undersøkelser skal gjøres. Vi har for eksempel fått melding om elever som blir innkalt enkeltvis på rektors kontor og bedt om å logge inn på sin private Facebook-konto for at rektor skal undersøke hvorvidt vedkommende er involvert i trakassering av en medelev. Denne typen framgangsmåte må unngås, og en veileder bør inneholde forslag til rutiner som sørger for det.

Vi understreket viktigheten av at presset til å avdekke mobbing ikke må bli så stort at det resulterer i tiltak som bryter med barnas grunnleggende rett til privatliv, selv om skolen har et stort ansvar når det gjelder å ivareta elevers psykososiale miljø. Skolens ansatte må være gode rollemodeller for barn når det gjelder å respektere grensene for hva man har lov til å be om å få se og ikke.

Vi foreslår i høringsuttalelsen at Kunnskapsdepartementet tar grep for å sørge for at landets skoler får et mer bevisst forhold til hvilke personopplysninger de ber om fra elevene, og hvordan de behandler personopplysningene de registrerer. Et steg i riktig retning vil være å utarbeide klare retningslinjer for hva skolen kan tillate seg når det gjelder inngrep i elevenes private sfære for å avdekke mobbing.

Saksbehandling og sentrale nemndavgjørelser

På skoleområdet har vi i 2015 mottatt flere meldinger om avvik som har dreid seg om uautorisert utlevering av personopplysninger, uautorisert innsyn i personopplysninger og eksponering av personopplysninger på internett. Dette er saker som vi mener illustrerer behovet for bedre rutiner

for internkontroll og informasjonssikkerhet, og som vi har påpekt både under tilsyn og i arbeidet for en norm for bedre personvern i skolen. Vi vil spesielt trekke frem disse sakene:

Avlysning av skoledagen via Mobilskole

Mange skoleeiere har valgt å ta i bruk en applikasjon som heter Mobilskole, og som skal erstatte ranselpost. En skoleeier fikk i 2015 advarsel fra en person om at sikkerheten i denne løsningen ikke var optimal. Skolen på sin side forsikret om at sikkerheten var god nok. Deretter opplevde de at personen som hadde gitt dem advarsel hacket Mobilskole og sendte ut beskjed til alle elever og foresatte om at skoledagen var avlyst.

Endring av karakterer via læringsplattform

I 2015 behandlet vi flere saker som underbygger vårt krav 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.

Nasjonale prøver

Bruken av resultater fra nasjonale prøver ble i 2015 problematisert i forbindelse med en søknad om konsesjon til et forskningsprosjekt. Forskerne skulle bruke resultater fra nasjonale prøver som en del av sitt forskningsmateriale. Vi stilte spørsmål ved om elever og foresatte var kjent med at barnas resultater fra nasjonale prøver kunne utleveres til forskning.

Vi hadde dialog med Utdanningsdirektoratet i saken, noe som resulterte i at direktoratet utarbeidet ny informasjon som skulle deles ut i forbindelse med gjennomføring av nasjonale prøver høsten 2015. Nå får elever og foresatte informasjon om hvordan resultatene fra Nasjonale prøver blir håndtert og hvem som får tilgang til dem.

Øvrige aktiviteter

Arbeidsgruppe om håndtering av dokumentasjon i barnevernet

I 2015 har vi deltatt i en arbeidsgruppe i regi av KS (kommunenes arbeidsgiver-, interesse- og medlemsorganisasjon). Gruppen arbeider med en veileder for hvordan dokumentasjon i barnevernet skal håndteres forsvarlig. En særlig problemstilling er bruk av filmopptak basert på samtykke fra foresatte og Riksarkivets vedtak om at disse filmene skal bevares. Dette er en problemstilling vi forsøker å løse i fellesskap med Riksarkivet.

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. Dette er et arbeid som aktørene i sektoren enda ikke har omfavnet. Det har imidlertid vært holdt møter i meldingsåret med sentrale aktører, og 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.

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 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.

Som et ledd i regjeringens Handlingsplan mot radikalisme og voldelig ekstremisme (OB 21-14, tiltak 27) og skolens pågående arbeid mot mobbing og krenkende ytringer, fikk IKT-senteret ansvar for å lage et opplegg for unge om uønskede hendelser på nett. Vi brukte våren og sommeren mye ressurser på dette arbeidet:

- Det ble opprettet to nye temasider for ungdom der det tas opp utfordringer ved ulike former for uønskede hendelser på nett. Dette skal både bidra til økt kunnskap og refleksjon, samt gi konkrete råd om tiltak og handlinger når den enkelte opplever eller observerer slike hendelser. Det informeres også om sentrale egenskaper ved ulike personverninnstillinger, og ulike varslings- og rapporteringsmuligheter.
- Det ble utarbeidet innhold for lærere og andre voksne som jobber med barn og unge, samt en egen nettside for skoleeier/skoleleder. Dette ble gjort for å tydeliggjøre deres ansvar for personvern og opplæringen av barn og unge i digital dømmekraft.
- Videre ble det laget eget innhold for de foresatte der det gis råd og veiledning om hvordan man snakker med sine barn om problematikken, og veiledning til håndtering av uønskede hendelser. I mange sammenhenger opplever dessuten barn og unge at de foresatte selv er en utfordring for personvernet deres. Denne problematikken belyses nærmere på nettsiden.
- Det ble laget to nye kortfilmer om uønskede hendelser på nett basert på statistikk og informasjon fra tjenesten Slettmeg.no.
- Undervisningsheftene til målgruppene 9-13 år og 13-18 år ble fornyet og trykket opp på både bokmål og nynorsk.

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.

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 digitaliseringene 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/virksomheter, nasjonalt ID-kort og bruk av biometri til autentisering og identifisering. Bruk av felleskomponenter, der deling av data og offentlige stordata (Big Data) er sentrale elementer, er også viktig å følge med på.

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

Vi utarbeidet i 2013 «Strategi for godt personvern i digitaliseringen av offentlig sektor». Strategien revideres jevnlig og danner fremdeles grunnlaget for 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 ti 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 lyktes dessverre heller ikke i 2015 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 få en plass.

Tilsyn

I 2015 gjennomførte vi kontroller med 15 forskjellige offentlige virksomheter; ti kommuner, to fylkeskommuner, to fylkesmannsembeter og en namsfogd. Dette var både stikkprøvekontroller, risikobaserte kontroller og etterkontroller, i den forstand at enkelte av kommunene ble kontrollert som en oppfølging av brevkontroller fra 2011. For samtlige kontroller 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 offentlige virksomheter ikke har tilfredsstillende rutiner for å oppfylle pliktene i personvernloven. 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,
- ha oversikt over databehandlere og ha tilfredsstillende databehandleravtaler med disse.

Vi har ikke kunnet fastslå at det er signifikante forskjeller knyttet til skillet mellom stat og kommune, 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 ivaretagelse av personvernet og oppfyllelse av pliktene i personopplysningsloven. Imidlertid mener vi å kunne se at virksomheter som har personvernombud, gjennomgående har en bedre ivaretagelse 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

Datatilsynet har i 2015 hatt fire høringer innenfor temaet digitalisering. Vi har ikke hatt innvendinger til noen av disse. I den grad vi har gitt kommentarer, har det kun vært for å uttrykke støtte til det som var foreslått, eller for å understreke punkter som var berørt eller behandlet.

To av de mest sentrale høringene har vært høringen knyttet til ny postlov og postforskrift, samt forslag til ny lov om folkeregister. Når det gjelder postlov med forskrift ga vi en tydelig tilbakemelding om at vi mente det var behov for en regulering av de offentlige digitale postboks-tjenestene. Dette gjelder «Sikker digital post» og postboks-tjenesten i Altinn. Vi mener det er uheldig at disse ikke er tilstrekkelig regulert med hensyn til kommunikasjonsvern og ansvar som øvrige post- og ekom-tjenester.

I forbindelse med forslaget til ny folkeregisterlov, var vi spesielt opptatt av at kvaliteten på opplysningene ikke må gå på bekostning av effektivitet, mulighetene for å skille på bostedsadresse/postadresse og digital adresse i registeret. Vi påpekte også viktigheten av at det gjøres grundige vurderinger knyttet til eventuell bruk av biometri når det gjelder folkeregisteropplysninger.

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.

Det har også blitt ilagt i alt fem overtredelsesgebyr; tre til kommuner, ett til et departement og ett til et annet statlig organ. Dette var knyttet til forhold som vi anså som alvorlige brudd på personopplysningslovens bestemmelser om internkontroll og informasjonssikkerhet. Tre av disse gebyrene er godtatt, mens de to siste virksomhetene har klaget på vår avgjørelse til Personvernemnda. Disse ble oversendt så sent på året at det ikke er fattet noen avgjørelse i dem enda.

Bakgrunnen for å ilegge gebyr var at det var forhold vi anså for å være alvorlige brudd på pliktene etter personopplysningsloven. 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.

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.

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 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 er et arbeid vi har stor tro på, og som vil materialisere seg tidlig i 2016.

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 har også i meldingsåret pekt på betydningen av at også de offentlige digitale postboksløsningene får sin regulering. Dette ble fra vår side først påpekt ved at vi mente en slik regulering hørte hjemme sammen med øvrig regulering av posttjenester, og ikke som en del av eforvaltningsforskriften. Vi opplevde å få gjennomslag for dette. Når endringen til postloven ble hørt i 2015, var regulering av elektroniske posttjenester med i forslaget, men etter høringsrunden ble dette tatt ut av forslaget til ny postlov som ble oversendt Stortinget. Dessverre ser vi nå at disse tjenestene ikke er, eller på kort sikt blir, regulert med hensyn til kommunikasjonsvern og ansvar. Dette ser vi på som uheldig og som et hinder mot en forsvarlig digitalisering av offentlig sektor. Vi vil jobbe videre for å få en tilfredsstillende regulering av disse tjenestene.

Helse og velferd

Helse- og velferdsområdet omfatter blant annet behandling av opplysninger innen helse- og omsorgstjenestene og NAV, i tillegg til sekundærbruk av opplysninger i helseregistre, helseforskning og samfunnsforskning.

Opplysningene som behandles innen dette området er blant de mest sensitive, og befolkningen selv anser opplysningene for særlig beskyttelsesverdige. Innen Datatilsynets ansvarsområde behandles det opplysninger om befolkningen i alle livsfaser, og ønsket om bruk og gjenbruk av våre opplysninger til stadig flere formål øker.

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

Videre er det en utfordring at helse- og omsorgstjenesten er preget av mange aktører og flere ulikt organiserte virksomheter med forvaltningsansvar og beslutningsmyndighet. Leverandører og databehandlere har ofte sentrale roller. I spesialisthelsetjenesten har kontroller vist at viktige deler av databehandlingsansvaret, slik som tilgangsstyring i helseforetakene, synes å være overført til enheter eller underselskaper som er opprettet av de regionale helseforetakene, for eksempel Helse-Vest IKT eller Sykehuspartner. Slike endringer i ansvarsforholdene skaper uklarheter, og begrenser de reelt ansvarlige helseforetakenes muligheter til å overholde sine plikter.

En annen aktuell utfordring er den økte utvekslingen av helseopplysninger som følger av helse- og omsorgsreformen. Flere opplysningskategorier om den enkelte vil gjøres tilgjengelig for et økende antall helse- og omsorgsarbeidere. 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.

Endringer i lovgivningen gir mulighet for å gi tilgang til pasientinformasjon på tvers av virksomhetsgrenser, men stiller nye krav til systemenes evne til å ivareta sikkerheten, slik at opplysninger ikke gjøres tilgjengelige utover det som er nødvendig og relevant for den helsehjelpen som skal ytes.

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. Datatilsynet oppfatter det slik at ansvarsforholdene i disse tjenestene har vært uklare.

Gjennomførte aktiviteter

Tilsyn

I 2015 gjennomførte vi til sammen 13 tilsyn innen området – fire med felles pasientdatabase i regi av helseforetakene i helseregion Vest, og ni tilsyn med virksomheter som driver med samfunnsforskning.

Tilgang til helseopplysninger etter ny pasientjournallov

De nye lovene om helseregistre og pasientjournaler trådte i kraft 1. januar 2015. Den nye pasientjournalloven inneholder hjemmel for å tillate tilgang til helseopplysninger på tvers av virksomhetsgrenser, og det er gitt en forskrift som regulerer slike tilganger nærmere. Forskriften stiller strenge krav til forutsetninger som må være på plass før virksomhetene kan gi slik tilgang, blant annet til pasientenes rett til å sperre for tilganger i forskjellige nivåer.

Lovens § 9 erstatter forskriften om felles journalsystemer i formaliserte arbeidsfellesskap, og den gir hjemmel for å opprette felles journaler mellom samarbeidende virksomheter. Helse Vest RHF annonserte våren 2015 at de nå hadde et system hvor virksomhetene i det regionale helseforetaket hadde felles journal. Vi iverksatte brevkontroll med foretakene i Helse Vest RHF, for å undersøke hvordan opplysninger gjøres tilgjengelige mellom foretakene, hvilke bestemmelser som hjemler de eventuelle tilgangene og hvorvidt lovens og forskriftens forutsetninger for behandlingen av opplysninger var ivarettatt. Kontrollen er ikke avsluttet på rapporttidspunktet.

Helse Nord-Norge og Helse Midt-Norge har for øvrig også tatt i bruk de nye mulighetene for tilgjengeliggjøring og deling av pasientopplysninger.

Tilsyn med samfunnsforskning

Vi vurderer jevnlig søknader om konsesjon til behandling av personopplysninger i samfunnsforskning. Et fellestrekk ved disse prosjektene er at det ofte behandles opplysninger om store deler av eller hele Norges befolkning, og at det er ønskelig å koble opplysninger mellom mange store registre.

I disse store prosjektene er det sjelden eller aldri opplysninger som gjør de registrerte direkte identifiserbare, men det anføres i søknadene at det er mulighet for indirekte identifisering. Vi ser imidlertid en tendens til at det er ønske om data på lave geografiske nivåer slik som for eksempel kommune, grunnkrets og til og med koordinater ned til en meters nøyaktighet. Det skal også ofte benyttes store mengder data på et meget detaljert nivå, noe som vil medføre at identifisering av enkeltindivider blir forholdsvis enkelt.

Vi ser at mange av disse store prosjektene ender opp med å være registerlignende, både med tanke på varighet og omfang, og at det lages underprosjekter og delprosjekter basert på opplysningene i hovedprosjektet.

I meldingsåret gjennomførte vi flere tilsyn innenfor denne sektoren. Vi var på tilsyn hos NTNU Samfunnsforskning, IRIS og Høyskolen i Oslo og Akershus. I tillegg gjennomførte vi seks brevkontroller med andre institusjoner som driver med samfunnsforskning. Kontrollrapportene er foreløpig ikke klare.

Sentrale høringsuttalelser

Vi ga en rekke høringsuttalelser på dette området i 2015, men særlig høringen om Kommunalt pasient- og brukerregister (KPR) var viktig og omfattende. Vi begrenser derfor vår omtale her til denne høringen.

Kommunalt pasient- og brukerregister (KPR)

Datatilsynet ga høringsuttalelse til forslaget om endringer i helseregisterloven § 11, og etableringen av et nytt sentralt helseregister (KPR) med opplysninger fra den kommunale helse- og omsorgstjenesten. Formålet med dette registeret skal blant annet være å gi grunnlag for planlegging, styring, finansiering og evaluering av kommunale helse- og omsorgstjenester. Dataene i registeret skal være en viktig kilde for statistikk, helseanalyser, kvalitetsforbedringsarbeid, beredskap, forebyggende arbeid og forskning.

Vi var i høringsvaret positive til at sekundærbruk av opplysninger fra de kommunale tjenestene reguleres på en bedre måte enn det gjøres i dag. Vi var imidlertid kritiske til den manglende detaljeringsgraden i forslaget. Vår største innvending var at det ikke ville være mulig for Stortinget å vurdere personvernkonsekvensene av dette forslaget, uten at det informeres mer detaljert hvordan opplysningene skal behandles i KPR.

Departementet presiserte at det kun skal samles inn relevante og nødvendige opplysninger i KPR. Vi mente imidlertid at det ikke er mulig å vurdere hvilke konsekvenser forslaget vil medføre for personvernet. Vi påpekte at det er svært uheldig at ikke detaljene for KPR foreligger når Stortinget skal ta stilling til om lovforslaget skal vedtas eller ikke. Den reelle vurderingen vil først skje på forskriftsnivå, og vi mente at den demokratiske kontrollen Stortinget skal utføre, vil være svært begrenset slik forslaget foreligger.

I det nye registeret skal det samles inn opplysninger om kommunens innbyggere i mange forskjellige situasjoner, ikke bare knyttet til at man mottar helsehjelp. Det skal for eksempel registreres opplysninger fra helsestasjonen. Uten nærmere beskrivelse av hvilke opplysninger man ønsker å inkludere fra denne tjenesten, ser vi et potensiale for en omfattende registrering av oss helt fra svangerskapsomsorgen – uavhengig av om vi er syke eller friske. Dersom en innbygger faktisk har behov for helse- eller omsorgstjenester, kan innholdet i KPR bli omfattende om hver enkelt.

Vi savner en diskusjon knyttet til om det i det hele tatt skal behandles opplysninger i dette omfanget, og ikke bare hvordan opplysningene skal beskyttes når de først er samlet inn.

Saksbehandling og sentrale nemndavgjørelser

Datatilsynet har hatt mange saker til behandling i meldingsåret. Vi har mottatt og behandlet flere 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.

Gjennom saksbehandlingen har vi sett at det i mangel av sentrale kvalitetsregistre for kommunehelsetjenesten, er ønske om å bruke eksisterende primærregistre opprettet for andre formål, for å hente ut informasjon i forsknings- og kvalitetssikringsformål. For eksempel har vi behandlet flere konsesjonssaker hvor det skal benyttes data fra HELFOs register KUHR (Kontroll og utbetaling av helserefusjon) som er opprettet for å forvalte behandlingsrefusjon og er hjemlet i folketryktdloven.

Vi har også sett at eksisterende registre utvides, og at opprinnelig avgitte samtykker strekkes langt og tolkes utvidende. Personvernemnda har i de siste årene kommet med flere avgjørelser som har betydning for vår saksbehandling av konsesjonssøknader knyttet til rekkevidden av samtykker, plikten til å gi informasjon, vilkår knyttet til informasjonsplikt og vår konsesjonskompetanse.

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.

Personvernemndas avgjørelse PVN-2014-21: Norsk Brannskaderegister

I Nyrebiopsisaken fra 2014, mente Personvernemnda at foreldres samtykke på vegne av barn rettslig sett var gyldig også etter at barna var gamle nok til selv å bestemme. Vi mente at personvernulempene for disse barna ville være for store med denne forståelsen av foreldresamtykkenes varighet. Vi satte derfor som vilkår for at opplysninger i Norsk Brannskaderegister skulle kunne lagres videre, at mindreårige pasienter fikk bestemme selv når de ble gamle nok.

Vedtaket vårt ble påklaget, og Personvernemnda ga medhold til klagen. Nemnda uttalte at Datatilsynet ikke har anledning til å stille vilkår som i realiteten begrenser rekkevidden av et ellers gyldig samtykke.

Personvernemndas avgjørelse PVN-2015-02: SmerteReg

I forbindelse med innvilgelse av konsesjon til opprettelse av et kvalitetsregister, stilte Datatilsynet vilkår om at det skulle informeres individuelt til de registrerte hvordan opplysningene om dem i registeret blir brukt i fremtiden. Vilkåret vårt ble ansett å være nødvendig for å redusere ulempene deltakelse ellers ville ha medført for de registrerte. Helse Bergen HF påklagde vedtaket, men Personvernemnda ga ikke medhold. Nemnda var enige med Datatilsynet i at dette var et lovlig vilkår, og at det er nødvendig for å redusere ulempene ved deltakelse i registeret.

Øvrige aktiviteter

Innen helsesektoren er det flere store prosesser i gang, og vi har i 2015 hatt løpende kontakt med Helsedirektoratet blant annet i forbindelse med Nasjonal kjernejournal, En innbygger – en journal, Min Helsejournal 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). Etter ny lovgivning har det vært behov for oppdateringer av allerede eksisterende materiell.

I tillegg har vi deltatt i en referansegruppe i forbindelse med utarbeidelse av veilederen «Personvern og informasjonssikkerhet - medisinsk utstyr». Veilederen ser særlig på to aspekter ved informasjonssikkerhet: manglende evne til å behandle helse- og personopplysninger i tråd med lovverket og dermed en trussel mot pasientens personvern, samt hvordan medisinsk utstyr kan beskyttes mot angrep på digital infrastruktur.

Vi har også deltatt i referansegruppen som har utarbeidet «Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter». Den skal bidra til å

begrense truslene mot informasjonssikkerhet og personvern som tilgang til helseopplysninger mellom virksomheter kan medføre.

Velferdsteknologi

Velferdsteknologi har vært et sentralt tema for Datatilsynet de siste årene, så også i 2015. 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. Veilederen ble utgitt i 2014, og det er planlagt en ny versjon i løpet av 2016. 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. Det er etter vår oppfatning naturlig at veilederen vil omfatte disse temaene.

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.

Mange kommuner er i etableringsfasen med å ta i bruk velferdsteknologi, og vi opplever et stort behov for informasjon og veiledning om personvernutfordringer ved teknologien. Ansatte i Datatilsynet er etterspurte foredragsholdere, og vi har i 2015 holdt en rekke foredrag om dette temaet i forskjellige fora.

NAV

En utfordring innen NAV-systemet er at det i stor grad benyttes eksterne leverandører for å oppfylle de oppgavene NAV skal ivareta. Datatilsynet har oppfattet at ansvarsforholdene ved bruk av eksterne leverandører, har vært uklare. Etter å ha forsøkt å få klarhet i dette gjennom korrespondanse med NAV over lang tid, mente vi det var nødvendig å gjennomføre kontroll med NAVs bruk av tiltaksarrangører i 2014.

NAV har vurdert at tiltaksarrangørene er behandlingansvarlige for den behandlingen av opplysninger de gjør på oppdrag fra NAV, og at NAV ikke kan anses som ansvarlig. Vi har vært uenig i denne konklusjonen, og etter kontrollene vi gjennomførte, påla vi NAV å utrede nærmere hvor behandlingsansvaret er plassert.

I 2015 har NAV fulgt opp konklusjonene og påleggene vi har gitt, og det arbeides nå med å lukke avvikene.

Fremtidige utfordringer

Med ny lovgivning har det blitt lettere å kunne gi tilgang til pasientopplysninger på tvers av virksomhetsgrensene. Forskrift om tilgang til helseopplysninger mellom virksomheter inneholder få krav til fagsystemene, og slike krav er en forutsetning for å sikre at det ikke gis en utilsiktet og ulovlig tilgang til personopplysninger. 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.

Pasientjournalloven åpner også for at det kan opprettes behandlingsrettede helseregistre mellom samarbeidende helsepersonell, og det er gitt forskriftshjemmel til å regulere disse forholdene. Uten at slik forskrift gis, er vi bekymret for hvordan praksisen vil utvikle seg på dette området.

Innen helsetjenesten skjer det en omfattende behandling av helseopplysninger, en behandling 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.

Den nye pasientjournalloven § 9 åpner for samarbeid om pasientjournaler mellom virksomheter, og samtidig åpnes det for at intern kvalitetssikring med den svake hjemmelen i helsepersonellovens § 26 utvides til å dekke alle innen slike samarbeid. Dette kan medføre en økt risiko for at det deles og tilgjengeliggjøres pasientopplysninger uten at hjemmelen er tilstrekkelig dekkende for behandlingen som i praksis skjer. Vi planlegger derfor å gjennomføre kontroller med sykehusenes behandling av pasientopplysninger til intern kvalitetssikring. Formålet med kontrollene er i hovedsak å få kunnskap om praksis knyttet til behandling av opplysninger som er ansett lovhjemlet i helsepersonelloven § 26.

På velferdsteknologiområdet mener vi at det ligger en personvernrisiko i at det ikke foreligger sentrale føringer for bruken i nevneverdig grad. Normens veileder vil gi noen retningslinjer, men det er fortsatt et stort behov for kommunikasjon av klare rammer for hvordan informasjon som genereres fra velferdsteknologi skal behandles.

Annen vesentlig aktivitet

Arbeidsliv

Det behandles nødvendigvis store mengder personlige opplysninger i arbeidslivet. Aktuelle problemstillinger er særlig ulovlig innsyn i e-post, elektronisk sporing, kameraovervåking og øvrige kontrolltiltak. Sektoren har ikke vært et prioritert område for Datatilsynet i 2015, men likevel er det gjennomført en håndfull tilsyn, og det har vært behandlet et relativt høyt antall saker.

Tilsyn

I løpet av meldingsåret gjennomførte vi fire tilsyn med behandling av personopplysninger i arbeidslivet som tema:

Skatteetatens rutiner og praksis for opprettelse og lukking av epostkasser og personlige hjemmeområder, ble undersøkt i første halvdel. Vi mente at å rutinemessig avslutte e-postkontoer først 20 dager etter at den ansatte har sluttet, ikke er i overensstemmelse med personopplysningsforskriften. De få avvikene som ble avdekket, ble imidlertid raskt fulgt opp av Skatteetaten, og dermed ble det ikke nødvendig å fatte noe vedtak om pålegg.

Statoil fikk i samme periode kontrollert sine rutiner for opprettelse og avslutning av e-postkasser og hjemmeområder, og også i denne saken ble avvikene raskt fulgt opp slik at det ikke var nødvendig å fatte vedtak.

Rutiner og praksis for opprettelse og lukking av e-post og personlige hjemmeområder var også tema for en kontroll ved Universitetet i Bergen (UiB). Kontrollen omfattet også arbeidsgivers innsyn i e-post og hjemmeområde. Vi varslet pålegg om å slette innholdet i e-postkasse og privat hjemmeområde for ansatte senest seks måneder etter arbeidsforholdets opphør. Vi varslet også pålegg om å deaktivere studenters e-postkonto senest to måneder etter at studieretten opphører, og om å slette innhold i studenters e-postkasse og hjemmeområde senest seks måneder etter at e-postkontoen er avsluttet. Beslutningen om fristen på seks måneder, har en særlig begrunnelse i ansettelsesforholdet for vitenskapelige stillinger ved universitetet, og er fristen som er hovedregelen i vår praksis. UiB bekreftet at avvikene var blitt rettet opp, og vi avsluttet dermed saken.

Vi gjennomførte også en kontroll hos Namsfogden i Oslo. Kontrollen resulterte i pålegg om at namsfogden må etablere internkontroll, og at de må utarbeide oversikt over hvilke personopplysninger som behandles om de ansatte og til hvilke formål, samt det rettslige grunnlaget for behandlingene. I tillegg ble Namsfogden pålagt å dokumentere rutiner for ivaretagelse av de registrertes innsynsrettigheter og rutiner for retting og sletting av personlige opplysninger. Namsfogden har frist til mars 2016 med å rette opp påleggene.

Saksbehandling og sentrale nemndavgjørelser

I meldingsåret endte ni saker med overtredelsesgebyr i størrelsesordenen 75 000-100 000 kroner. Sakene gjaldt ulovlig innsyn i e-post, kameraovervåking på arbeidsplassen og bruk av elektronisk kjørebok. To av avgjørelsene ble påklaget og er til behandling i Personvernemnda.

Personvernemnda har behandlet to klagesaker om personvern i arbeidslivet i 2015. Den ene gjaldt plasseringen av behandlingsansvaret i en sak om GPS-registrering av kjøretøy som utførte oppdrag på bestilling fra en norsk kommune. Nemnda var uenig med oss i at behandlingsansvaret måtte ligge hos arbeidsgiveren, og sendte saken tilbake for videre saksbehandling. Den andre saken gjaldt sletting av opplysninger i personalmapper. Vi mente at vilkårene for sletting ikke var til stede, noe nemnda var enig i.

Øvrige aktiviteter

Vi deltar i arbeidet med en ny felles veileder om overvåking og kontroll i arbeidslivet sammen med Arbeidstilsynet, Petroleumstilsynet og partene i arbeidslivet. Prosjektet ble startet i 2015, og ledes av Arbeidstilsynet. Arbeidet fortsetter i 2016.

Finanssektoren

Banker, kredittopplysningsselskaper og forsikringsselskaper behandler personopplysninger om stort sett alle i Norge. Det er snakk om store mengder opplysninger om til dels veldig personlige og følsomme forhold. Selskapene leverer tjenester som hver og en av oss er avhengige av, og som er viktige for samfunnet. I møte med disse institusjonene er enkeltindividet på mange måter prisgitt at de lovene og reglene som er gitt for å beskytte deres interesser, blir fulgt og virker etter sin hensikt.

Finanssektoren har imidlertid ikke vært et prioritert område i 2015. Det har derfor vært noe begrenset aktivitet på området, men det har blitt gjennomført ett tilsyn med forsikringsselskapenes fellesregistre, ved Finans Norge. Kontrollens tema var forsikringsselskapenes sentrale skaderegister («FOSS»), og Finans Norges rutiner for etterlevelse av den eksisterende konsesjonen gitt av Datatilsynet i 2008. Kontrollen avdekket ingen avvik, og saken er avsluttet.

Vi har videre gitt løpende veiledning til virksomheter og til bransjeorganisasjoner, hatt ett kontaktmøte med Finanstilsynet og ett med Finans Norge, og har dessuten behandlet i underkant av 30 konsesjonssaker innenfor disse sektorene, inkludert norske kredittopplysningsvirksomheter.

Teknologi, internett og telekom

Arbeidet med å få oversikt over lagringen av personopplysninger innen telekom- og internettsektoren, fortsatte i 2015, og det har vært et godt samarbeid med Nasjonal kommunikasjonsmyndighet (Nkom). Berørte operatører har også gitt god informasjon om hva som lagres av trafikkdata, signaleringsdata (data som opplyser om hvilken radiocelle mobilen kommuniserer med på et gitt tidspunkt, og hvor denne befinner seg på et gitt tidspunkt. Signaleringsdata er de meta-trafikkdata og opplysninger nettet og mobilen bruker for å kunne fungere sammen) og liknende data, samt hva som er lagringstid og formålet med lagringen. Vi ser at det er en økende grad av lagring av opplysninger om hver enkelt, og grunnen til dette kan blant annet være håndtering av sikkerhet. Implikasjonen dette har på den enkelte av oss er større enn før, siden det nå for det meste er snakk om mobilt utstyr som vi bærer med oss hele døgnet. Arbeidet fortsetter i 2016.

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 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 – kunnskap som i utgangspunktet er for invaderende å logge bare for å fakturere oss eller for å få nettet til å virke.

Tilsyn med kryptering av datasentertrafikk

I 2015 gjennomførte vi tilsyn med tre store virksomheter som leverer datasentertjenester. Formålet var å undersøke om det var etablert kryptering av kommunikasjonen mellom leverandørens datasentre, og mellom kunde og datasenter. Blant annet har Snowden-avsløringene vist at ukryptert datasentertrafikk er en sårbarhet som må tas alvorlig, og dessverre har bransjestandarden her vært at slik trafikk blir kjørt ukryptert over blant annet fiberlinjer. Selv om det kreves en vesentlig innsats

for å avlytte og få tilgang til trafikken som går over slike linjer, er konsekvensene ved avlytting svært store, og kryptering er nødvendig. Sakene er fremdeles til behandling.

Kameraovervåking og kamerateknologi

I meldingsåret var kameraovervåking det temaet som var mest hyppig besøkt på våre nettsider. Vi fikk inn over 1000 henvendelser på e-post og telefon med spørsmål omkring bruk av kamera og personvern. 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 åtte kameratilsyn i løpet av 2015 innenfor utelivsbransjen, trenings- og velværebransjen, samt restaurant- og utelivsbransjen. Disse bransjene ble valgt på grunn av mange henvendelser angående bruken av kamera.

I 2015 har vi også sett særlig på kameraovervåking av offentlige områder. Vi ser tydelig at overvåkingsfrie rom i samfunnet er under press. Bruken av kameraovervåking som et middel for å dokumentere kriminalitet, overkjører regelmessig hensynet til privatlivets fred og enkeltpersoners frihet mot ubegrunnet personovervåking. Vi ser det som en utfordring at mesteparten av sosial og individuell adferd, blir registrert og kontrollert.

Både offentlige myndigheter og private virksomheter overvåker offentlige områder. Vi gjennomførte i 2015 et tilsyn i Brumunddal politidistrikt, og gikk i etterkant i dialog med Politidirektoratet for å avklare politiets bruk av kameraovervåking, samt behovet for overvåking i det offentlige rom. I tillegg gjennomførte vi tilsyn med en privat aktør som overvåket et spesifikt område i Oslo bestående både av butikker og private boliger. Vi ser et behov for å undersøke kommersielle aktørers bruk av kameraovervåking videre, for å hjelpe aktørene å overholde personopplysningsloven.

I meldingsåret skrev vi dessuten en intern rapport om intelligent videoanalyse. Formålet var å heve kompetansen internt når det kommer til ny kamerateknologi og bruksområdet for dette.

Energisektoren og smartmålere

I 2015 har mange virksomheter sett på mulighetene for å utnytte potensialet som nye smarte strømmålere legger til rette for, ofte i kombinasjon med annen teknologi for smarte hjem. Styring av strømforbruket med smartteknologi vil kunne få stor positiv effekt på forbruket. Imidlertid må man passe på at personvernet ikke svekkes. Også EU-kommisjonen har sett muligheten for at personvernet kan bli berørt, og krever at datatilsynsmyndighetene blir hørt. Kommisjonen har derfor laget et notat om håndtering av personvernkonsekvensene ved smarte strømmålere, med påfølgende rådgivningsarbeid for datatilsynene i Europa i årene som kommer. Vi har deltatt i dette arbeidet på europeisk nivå sammen med de øvrige personvernmyndighetene.

Biometri

I løpet av meldingsåret har vi sett en økt bruk av biometri. Det ble blant annet kjent at BankID samlet inn tastebiometri om bankkunder på vegne av bankene. Det ble lagt biometriske profiler på bankkundene basert på hvordan de tastet passord i påloggingsprosessen, uten at de fikk tilfredsstillende informasjon om dette. Vi har også hatt flere møter om biometri både med bransjen og ulike konsulenter.

Publisering av personopplysninger på internett

I 2015 har vi arbeidet med to kategorier innenfor området «personopplysninger på internett». Den første kategorien er indeksering i søkemotorer og retten til å bli glemt. Den andre er såkalte ratingsider, slik som for eksempel legelisten.no.

Retten til å bli glemt

EU-domstolen avgjorde i mai 2014, at enkeltpersoner kan få søketreff tilknyttet deres navn avindeksert dersom de får medhold i at søketreffet er belastende, misvisende eller irrelevant. Avindeksering innebærer at opplysningene ikke lenger vil være tilgjengelige ved søk på vedkommendes navn og blir derfor kalt «retten til å bli glemt». Vi har i 2015 mottatt 21 saker der Google har gitt avslag og der avslaget blir klaget inn til oss. Av disse har fem fått medhold og ni har fått avslag på klagen sin. Siden 2014 har to av våre avslag blitt påklaget til Personvernemnda.

	2014	2015
Medhold	4	5
Avslag	4	9
Veiledning/annet	2	7
Antall saker totalt	10	21

Ratingsider

Vi har i meldingsåret arbeidet videre med saker som gjelder «ratingsider» på nett. Dette er sider der brukere rangerer personer innenfor et yrke. Vi har blant annet behandlet klager knyttet til minLærer.no og legelisten.no. Vi har kommet frem til at norskdrøve nettsider som behandler opplysninger og vurderinger om navngitte enkeltpersoner, som utgangspunktet har behandlingsansvar for innholdet på siden, og må dermed følge personopplysningsloven. Vi har i 2015 vært i dialog med bransjen for å avklare hvor grensen går for hva slags type informasjon som er relevant og saklig, og som kan publiseres innenfor lovens rammer.

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 lokalisering av personer. Smarte byer og intelligente transportsystemer gir utfordringer for personvernet, og vi har i 2015 fortsatt arbeidet med ITS via samarbeid med andre etater, foredragsvirksomhet og veiledning.

Forskning og utvikling (FoU)

Formålet med Datatilsynets satsing på forsknings- og utviklingsarbeid, er å gjøre oss selv bedre til å sette personvern hensyn 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.

Partnerskapsavtale med CCIS

Den viktigste begivenheten på FoU-området i 2015, var inngåelsen av en partnerskapsavtale mellom CCIS (Center for Cyber and Information Security) og Datatilsynet. CCIS ved Høgskolen på Gjøvik (som inngikk i NTNU fra 1. januar 2016) 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.

Forskningsprogrammet Secure Societies

Datatilsynet ble i 2015 invitert til å delta i referansegruppen for forskningsprogrammet «Secure societies – Protecting freedom and security of Europe and its citizens», som går i regi av Forskningsrådet.

Forskningsprogrammet er en del av et omfattende forsknings- og innovasjonsprogram i EU, kalt «Horizon 2020». Programmet går over syv år (2014 til 2020), og har betydelige midler til rådighet. 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.

Referansegruppen består i hovedsak av universiteter, høyskoler, forskningsinstitusjoner og offentlige myndigheter innen justis- og beredskapssektoren. Vi ser det som viktig at også personverninteressene blir representert i forskningsprogrammet. Vi deltok i desember på referansegruppens første møte, og vil også i 2016 delta aktivt i referansegruppen. I tillegg deltar vi løpende i prosjektet via andre kanaler dersom det er behov for det.

Forskningsprosjekt om crowdsourcing

Vi er også representert i referansegruppen til forskningsprosjektet «Social Responsible Crowdsourcing for Environmental Research and Decision» (iResponse). Flere forskningsinstitutter og andre aktører samarbeider her om å utvikle såkalte crowdsourcing-verktøy. Prosjektet finansieres av Forskningsrådets program SAMANSVAR, som legger særlig vekt på ansvarlig innovasjon og Corporate Social Responsibility (CSR). Ivaretagelse av personvern hensyn er selvsagt viktig ved utvikling av slike verktøy. Vi deltok med én representant i den første og innledende workshopen i prosjektet, og har også bidratt med rådgivning underveis. Vår aktive deltakelse i prosjektet fortsetter også i 2016.

Bistand til mastergradsstudenter

Vi har også stilt vår kompetanse til rådighet for flere mastergradsstudenter som ønsket å skrive om personvern og vi har kommet med forslag til mastergradsoppgaver.

Forskning på internett

Våren 2015 fattet vi et vedtak i en sak som fikk mye medieoppmerksomhet. Det gjaldt forskning på internett. Debatten som fulgte bar preg av stort engasjement, og vi antar at dette var fordi saken gjaldt forskning på fremmedkrigere og ekstremisme. Også folkevalgte på Stortinget og medlemmer av regjeringen deltok i ordskiftet. Enkelte mente vi tolket regelverket for strengt, og det ble tatt til orde for regelverksendringer.

Vi hilser selvsagt en debatt som gjelder tolking av personopplysningsloven og Datatilsynets konsesjonspraksis velkommen. Vi mener imidlertid at det er viktig at debatten løftes til å gjelde generelle prinsipper for bruk av åpne kilder på internett i forskningen. En debatt basert på et ønske om å stoppe ekstremisme gjør at nyansene er vanskelige å få øye på. Vi har forståelse for at det er lett å si seg enig i at en person som står frem på sosiale medier som selverklært fremmedkriger, har diskvalifisert seg fra de rettssikkerhetsgarantier som personopplysningsloven gir. Vår hypotese er at det kanskje ikke er like lett å si seg enig i at enhver person som ytrer seg offentlig på internett, gir avkall på sine personvernrettigheter. Vi er opptatt av å understreke at det også på internett skal være et skille mellom allment tilgjengeliggjorte opplysninger og opplysninger som er ment for et mer begrenset publikum. En person som erklærer sin sorg på sin avdøde venns åpne Facebook-profil, vil fortsatt måtte regne med å bli kontaktet dersom en forsker ønsker å bruke vedkommendes utsagn i sin forskning.

Vi er for øvrig helt på linje med den nasjonale etiske komite for samfunnsforskning og humaniora (NESH), som har utarbeidet retningslinjer i forskningsetikk for forskning på internett. Disse retningslinjene ble vektlagt i vedtaket som ble fattet i 2015, og vil fortsatt være relevant for eventuelt nye saker vi får inn hvor forskning på åpne kilder på internett er tema.

Kommersiell utnyttelse av personopplysninger

I 2015 publiserte Datatilsynet rapporten «Det store datakappløpet. Hvordan kommersiell utnyttelse av personopplysninger utfordrer personvernet». Rapporten ble skrevet fordi vi er vitne til en utvikling der personopplysninger får stadig større kommersiell verdi i medie- og annonsemarkedet. Den harde globale konkurransen om annonsekronene fører til et datakappløp der den aktøren som sitter på mest data om den enkelte, er vinneren. Jo mer data aktørene har om den enkelte, jo bedre kan de tilpasse reklamen. Det er i dag nærmest umulig å bevege seg på nett uten å bli sporet. Vår rapport viste at det i gjennomsnitt er 43 ulike tredjeparter inne på en norsk nettvise og samler inn data om brukeren. Rapporten trakk frem følgende hovedutfordringer ved dagens digitale annonsemarked:

- Markedet er lukket, komplekst og vanskelig å få innsyn i for utenforstående.
- Internettbrukere utsettes for massiv sporing av tredjepartsaktører på nett.
- Det gis liten eller ingen informasjon fra nettstedseierne om hvilke aktører som er tilstede på sidene, hvilke data de samler inn og hvordan de brukes.
- Jo mer data som samles inn om den enkelte, jo høyere priser kan enkeltbrukere omsettes for på de globale annonsebørsene. Dette stimulerer til en omfattende kartlegging av den enkelte.
- Aktørene i verdikjeden hevder de kun benytter anonyme data. Datatilsynet mener derimot at det håndteres unike brukere på børsene og at det håndteres personopplysninger i verdikjeden.

Rapporten kommer med en rekke forslag til anbefalinger og tiltak. I 2016 vil vi jobbe videre med disse tiltakene og sørge for at de følges opp. De viktigste anbefalingene og tiltakene i rapporten er disse:

- Nettstedeierne må ta ansvar for tredjepartsaktørene de slipper til på sidene sine.
- Innsamling av personopplysninger til profilerings- og markedsføringsformål, må hvile på aktivt samtykke.
- «Take it or leave it»-løsninger må unngås.
- Samtykkeerklæringene må bli bedre
- Data må slettes.
- Det må gis innsyn i profilene.
- Tilpasset annonsering må ikke basere seg på sensitive opplysninger om for eksempel helseforhold

Rapporten fikk stor oppmerksomhet i pressen og av andre relevante aktører da den ble publisert, og i 2016 vil den lanseres også internasjonalt.

Den internasjonale personverndagen

Den internasjonale personverndagen 28. januar, ble for tredje gang markert i samarbeid med Teknologirådet. Tema for årets frokostseminar og tilhørende rapport var blant annet barn og unges personvern, digitalisering av skolen, tingenes internett og «livet etter Snowden». Seminaret ble raskt fulltegnet, med over to hundre deltakere. Vi mener at vi på denne måten har fått benyttet anledningen som den internasjonale personverndagen representerer, til å få satt personvern ekstra

på dagsorden, med oppmerksomhet og omtale også i mediene. Arrangementet, og samarbeidet med Teknologirådet, er vurdert som så vellykket at det vil bli gjentatt også i 2016.

Internet Sweep Day - personvern i apper for barn

For tredje året på rad deltok vi i Internet Sweep Day, i regi av det internasjonale samarbeidsnettverket GPEN (Global Privacy Enforcement Network). Temaet for 2015 var personvernet i apper rettet mot barn opp til 13 år. Datatilsynet undersøkte (sveipet) i den forbindelse 60 apper – både norskproduserte og internasjonale – som er populære blant norske barn.

Funnene ble beskrevet i en rapport lansert i september 2015. Her er de viktigste tallene fra det norske sveipet:

- 75 prosent av appene vi sveipet samler inn personopplysninger, og 62 prosent av de som samler opplysninger oppgir at de deler disse med tredjeparter.
- I omtrent halvparten av appene som behandler personopplysninger, er det uklart hvorfor de samler inn en eller flere av opplysningene.
- 70 prosent av appene vi sveipet hadde en personvernerklæring.
- Kun ti prosent av appene har mekanismer som hjelper barna med å ivareta personvernet sitt.

Personvernombudsordningen

Personvernombudsordningen er frivillig og gir virksomheter som velger å ha ombud fritak fra meldeplikten til Datatilsynet. Ombudet skal fungere som en ressursperson med spesialkompetanse på personvern i virksomheten, og skal ha oversikt over hvilke personopplysninger som blir behandlet til ulike formål. Personvernombudet vil derfor kunne hjelpe virksomheten til å håndtere personvernutfordringer som måtte oppstå.

Ved utgangen av 2015 hadde Datatilsynet registrert 271 personvernombud. Noen av disse er ombud for flere virksomheter, og til sammen representerer de 470 virksomheter.

Oversikt over utviklingen av personvernombudsordningen de siste årene:

	2012	2013	2014	2015
Personvernombud	203	210	233	271
Virksomheter med ombud	390	420	450	470

I 2015 gjennomførte vi flere kurs for personvernombudene; to grunnkurs, to juridiske påbyggingskurs, to påbyggingskurs i informasjonssikkerhet og internkontroll, og et dagsseminar for personvernombud fra helse- og forskningsvirksomheter. I tillegg ble en større fagdag med over 100 deltakere arrangert i oktober. Vi har merket økt interesse for kursene i meldingsåret, med opp mot 50 påmeldte på hvert av de kursene som ble arrangert på høsten.

Personvernombudene beskriver våre kurs og seminarer som viktige for deres mulighet til å gjøre en god jobb og relevant for arbeidet deres med personvern i virksomhetene.

EUs nye personvernforordning peker mot store endringer på personvernombudsfeltet, blant annet ved at ordningen blir obligatorisk for en del virksomheter. I 2015 var det fremdeles uklart akkurat hva endringene vil innebære, men vi har startet arbeidet med å forberede oss internt og eksternt på at det nye regelverket kommer.

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 2015 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, og møter med en representant for ledelsen i Datatilsynet. Det er avholdt fem møter i Artikkel 29-gruppen i 2015, og Datatilsynet har vært representert på alle.

Blant annet har Artikkel 29-gruppen kommet med kommentarer til C-SIG Code of Conduct on Cloud Computing. Dette er et veldig aktuelt tema, ettersom mange benytter skytjenester og vi får mange spørsmål om dette. Vi har over tid etterspurt en internasjonal standard.

Naturligvis har året dessuten vært preget av arbeidet med det nye felles europeiske personvernregelverket, og Artikkel 29-gruppen har jevnlig avgitt uttalelser til EU-kommisjonen om forskjellige spørsmål i den anledning.

Safe Harbor-saken

Safe-Harbor avgjørelsen har naturlig nok også preget mye av arbeidet i Artikkel 29-gruppen etter at avgjørelsen kom i oktober.

EU-domstolen avgjorde 6. oktober at EUs Safe Harbor-beslutning fra 2000 er ugyldig. Beslutningen hadde inntil da gitt grønt lys for selskaper som ønsker å overføre persondata til amerikanske selskaper som er Safe Harbor-sertifisert. Listen over kjente amerikanske IT-giganter på Safe Harbor-listen er lang, men etter at rammeverket ble kjent ugyldig, er konsekvensen at man ikke kan belage seg på denne mekanismen når man skal overføre data om personer til USA. Slike dataoverføringer skjer både helt målrettet, som for eksempel via eposter adressert til mottakere i USA, men også mer indirekte, for eksempel ved bruk av skytjenester, sosiale medier, web-analyseprogramvare og apper.

Domstolen uttalte også at de nasjonale datatilsynenes uavhengighet står i veien for at EU-kommisjonen fatter eksklusive beslutninger om hvorvidt beskyttelsen i et ikke-medlemsland er tilfredsstillende etter europeiske standarder eller ikke. Til nå har datatilsynsmyndighetene i Europa, inkludert Datatilsynet i Norge, vært svært tilbakeholdne med å vurdere tredjeland på egenhånd, men det kan nå komme til å endre seg. Avgjørelsen føyer seg inn i en lang rekke saker der datatilsynsmyndighetenes uavhengighet blir fremhevet som et essensielt element i europeisk personvern.

Konsekvensen for norske dataeksportører blir merkbare. Ettersom Safe Harbor ikke lenger kan benyttes som grunnlag for å overføre data fra Norge, må man finne andre løsninger, eller avstå fra å eksportere persondata til USA. I 2016 skal personvernmyndighetene i EU se på hvilke konsekvenser dommen får for overføring av personopplysninger i medhold av andre rettsgrunnlag, som EUs standardkontrakter og bindende konserninterne regler (BCR).

Vi var raskt ute med å informere om den endrede rettstilstanden. Vi sendte blant annet ut skriftlige orienteringer til samtlige 110 virksomheter som har meldt inn til oss at de overfører persondata til aktører i USA i medhold av Safe Harbor-ordningen, og hadde fyldig informasjon tilgjengelig på våre nettsider.

Technology Subgroup

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. Datatilsynet har vært representert på samtlige møter avholdt i 2015 med en erfaren teknolog.

Future of Privacy Subgroup (FOP)

Dette har vært det første året som medlem av denne undergruppen til Artikkel 29-gruppen. Ved siden av å øke Datatilsynets synlighet, vurderte vi det som viktig å være med i denne undergruppen da mye av diskusjonene om den nye forordningen ville skje her. Det har vist seg svært verdifullt for oss. Vi har blant annet evnet å være en god samtalepart for både Justisdepartementet og Kommunal- og moderniseringsdepartementet om den ny forordningen. Vi er representert med én jurist i denne undergruppen, og vi har vært med på alle møter som har vært holdt siden vi ble medlem.

Berlinggruppen

Berlinggruppen er et 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 Berlinggruppen. Som et tiltak for å bli mer synlig på den internasjonale arena, har vi jobbet aktivt for å få møtet i 2016 til Oslo. Det er nå bestemt, og i 2015 startet vi opp planleggingen av møtet.

Den internasjonale personvernkonferansen

Datatilsynet er medlem av den internasjonale personvernkonferansen, og i 2015 støttet vi en resolusjon som ble vedtatt på konferansen. Vårt engasjement på konferansen var en videreføring av jobben med Big Data-resolusjonen som vi fremmet året før.

Temaet for årets konferanse var «Building Bridges» - hvordan jobbe for bedring av personvernet i grensedragningen mellom Europa og USA. Temaet er svært aktuelt slik dommen fra EU-domstolen viste senere på året. Vi deltok med et innlegg i en sesjon om barn og unges personvern, der vi fortalte om vårt arbeid i Du Bestemmer-prosjektet. I forkant av konferansen ble det også utarbeidet et «paper» der Du Bestemmer ble grundig beskrevet på engelsk.

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.

Schengen Coordination Group (SCG)

Vi er fullverdig medlem av Schengen-koordinasjonsgruppen som møtes i EU-parlamentet i Brussel. Vi har deltatt på to møter i 2015.

I tillegg deltok en ekspert fra Datatilsynet i tilsynsteamet som inspiserte Schengen informasjonssystem i Tyskland sommeren 2015. Vi planlegger også fremover å være med på kontroller av andre Schengen-land.

Eurodac og Visumsamarbeidet i Europa

Vi er fullverdig medlem av begge disse kontrollgruppene. De har som regel møter sammen, i og med at temaene for fingeravtrykk og visum i stor grad retter seg mot samme gruppe personer. Vi deltok på begge møtene som ble avholdt i 2015.

Samarbeid med de nordiske datatilsynsmyndighetene

Det nordiske datatilsynsmøtet ble arrangert i Helsinki i mai 2015. Hovedtemaet var ny forordning og hvordan de nordiske landene planla å implementere de nye reglene. Møtet i mai ble fulgt opp av et nytt møte senere på høsten, der vi utvekslet planer for dette arbeidet.

Det er i tillegg jevnlig kontakt med de nordiske datatilsynsmyndighetene i form av uformelle samtaler og på andre internasjonale møter. Ny personvernforordning har vært et tema som vi stadig har utvekslet erfaringer om.

Internasjonal presentasjon av kommersialiseringsrapporten

Rapporten om kommersialisering av personopplysninger har blitt presentert for forskjellige internasjonale institusjoner og i forskjellige fora. Vi har fått gode tilbakemeldinger på både denne rapporten og på den tidligere rapporten om Big Data. Vi mener vi har lyktes godt med de initiativene vi har tatt internasjonalt. Rapporten ble i 2015 presentert i Berlingruppen, for EUs datatilsyn – European Data Protection Supervisor og for den norske EU-delegasjonen. Arbeidet med å påvirke internasjonale aktører vil fortsette i 2016.

Bistand til personvernmyndigheten i Makedonia

Det norske Utenriksdepartementet ga i desember 2014 fortsatt finansiell støtte til Republikken Makedonia til utvikling av landets personvernmyndighet. Datatilsynets makedonske søsterorganisasjon arbeider nå med å ferdigstille sitt opprinnelige prosjekt, som hovedsakelig dreier seg om personvern i sosiale nettsamfunn og om utfordringer knyttet til bruk av skytjenester. I tillegg er prosjektmandatet blitt utvidet til også å utvikle et nærmere samarbeid mellom flere lands personvernmyndigheter på Vest-Balkan. Målet er å dra nytte av de positive erfaringene som er gjort i vårt samarbeidsprosjekt så langt. Ikke minst gjelder dette etableringen av en veiledningstjeneste for de som opplever seg krenket på internett, etter inspirasjon fra vår norske tjeneste slettmeg.no. Denne tjenesten vil lanseres i Makedonia i februar 2016.

Vårt bidrag har i 2015 hovedsakelig bestått i å organisere et studiebesøk til Norge. I september tok vi mot en delegasjon på ti personer som, foruten Makedonia, representerte personvernmyndighetene i Bosnia Herzegovina, Albania, Serbia, Montenegro og Kosovo. Våre gjester besøkte da Norsk senter for informasjonssikring (NorSIS) på Gjøvik, som presenterte slettmeg.no. I tillegg orienterte vi fra vår side om våre erfaringer med nordisk samarbeid, undervisningsopplegget Du bestemmer og flere andre temaer.

De makedonske personvernmyndighetene arbeider for å etablere en årlig samarbeidskonferanse for personvernmyndighetene på Vest-Balkan. Vi vil, sammen med NorSIS, stille med foredragsholdere og aktive deltakere på konferansen som arrangeres i februar 2016.

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 (tidligere Post- og teletilsynet) og Arbeidstilsynet.

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.

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 Høgskolen 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).

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 trafiksikkerhet, 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.

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.

Referansegruppe for policyutvikling for bruk av skytjenester

Kommunal- og moderniseringsdepartementet (KMD) etablerte høsten 2014 en interdepartemental arbeidsgruppe som skal kartlegge hindringer i regelverket for bruk av skytjenester. KMD har samtidig

etablert en ekstern referansegruppe med interessenter, potensielle brukere og eksperter fra relevante områder, for å se på policyutvikling for bruk av skytjenester i offentlig sektor.

Datatilsynet deltar med én representant i referansegruppen. Det har vært avholdt tre møter i 2015.

Arbeidet knyttet til forslaget om ny personvernforordning i EU

Datatilsynet har vært aktive i Justis- og beredskapsdepartementet (JD) sin referansegruppe i forbindelse med nasjonal representasjon i Brussel. I denne gruppen har også representanter for KMD vært med. Vår bistand har bestått i å være diskusjonspart med representanter for fagavdelingene i KMD og JD, i forbindelse med de mange forslagene som har vært oppe til behandling i DAPIX (Working Party on Information Exchange and Data Protection). DAPIX er en arbeidsgruppe i EU som forhandler om innholdet i den nye forordningen.

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.

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.

Samarbeidsprosjektet Du Bestemmer

Du Bestemmer er en læringsressurs som drives i samarbeid mellom Senter for IKT i utdanningen og Datatilsynet, og som ble lansert i januar 2007. Målet med opplegget 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. Ungdommene skal lære seg å ta kontroll over egne personopplysninger, men samtidig respektere andres opplysninger. Opplegget er til nå tatt i bruk i over 16 andre land.

Årets aktiviteter er nærmere beskrevet under *Årets viktigste aktiviteter, Barn, skole og utdanning*.

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.

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 2015 jobbet særlig med høringen om ny folkeregisterlov og også deltatt i møter med alle interessenter, der vi har redegjort for våre tilbakemeldinger på ny lov. Tilgang til opplysninger fra folkeregisteret er en problemstilling vi jevnlig må forholde oss til.

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.

Bransjenorm for utredningsvirksomhet for forsikringsbransjen

Bransjenormen ble ferdig i 2015. Vi fikk den til uttalelse og skal gi bransjen en tilbakemelding på hva vi mener om den. Det er viktig for oss å presisere at vår rolle nå ikke er å godkjenne normen, men å gi en tilbakemelding.

Bransjenorm for sikkerhetsbransjen

NHO Service har tatt initiativ til å utarbeide en bransjenorm for sikkerhetsbransjen. Arbeidet med normen startet i 2015, og vil fortsette i 2016. Datatilsynet har to representanter i arbeidsgruppen og to i styringsgruppen.

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 deltar med én representant i forumet.

Arbeidsgruppe sikkerhet og abuse

Nkom har sammen med Samferdselsdepartementet (SD) et nasjonalt ansvar for elektronisk kommunikasjon, inkludert internett i Norge. Nkom utøver tilsyn med sikkerhet og beredskap i samferdselssektoren, inkludert logisk sikkerhet på internett. Arbeidsgruppen arbeider med å fremme bransjenormer for internettsikkerhet og i samarbeid med aktørene sørge for bedre sikkerhet i domenenavnsystemet. Datatilsynet deltar med én representant i gruppen.

VURDERING AV FRAMTIDSUTSIKTER

Internasjonalt

I desember 2015 ble det politisk enighet om et nytt personverndirektiv i EU. Etter vår vurdering er det et godt regelverk som vil pålegge virksomhetene nye plikter, gi borgerne nye rettigheter og tilsynsmyndighetene nye virkemidler. Særlig viktig er at virksomhetene nå er forpliktet til å ta hensyn til innebygd personvern, de må i en del tilfeller drøfte utviklingsprosjekter på forhånd med Datatilsynet, og flere virksomheter må opprette personvernombud.

Den nye forordningen vil naturligvis være en høyt prioritert oppgave for oss de neste to årene, og vi anslår at vi vil bruke til sammen ti årsverk fordelt på to år på dette arbeidet. Budsjettet vårt ble vesentlig styrket i 2016. Dette gjør at vi er trygge på at implementeringsarbeidet vil komme i mål og at Datatilsynet er godt forberedt når det nye regelverket trer i kraft.

Vi er mer bekymret for norske virksomheter og offentlige etater. Som nevnt tidligere er vårt hovedinntrykk at kjennskapen til regelverket er relativt dårlig. Det er grunn til å frykte at den ikke vil bli bedre med nytt regelverk. Likevel er det grunn til en viss optimisme. Vi opplever svært stor interesse for personvern generelt, og den nye lovverket spesielt. Bare det siste halvåret har vi holdt et titalls foredrag om forordningen. Advokatfirma, foreninger, organisasjoner og bedrifter arrangerer seminarer og kurs for sine kunder/medlemmer, og vil være en viktig kilde til informasjon om det nye regelverket. Datatilsynet vil prioritere å stille opp på slike seanser.

En usikkerhetsfaktor er hvor mange saker som skal inn for det såkalte European Data Protection Board (EDPB), og hvilken innflytelse Datatilsynet får her. Dette organet vil ha en viktig funksjon, blant annet ved å påse at praksis i de ulike landene er lik, utarbeide retningslinjer og lignende. Det er derfor viktig at vi får en rolle der vi faktisk har innflytelse. I tillegg er det en viss fare for at EDPB ikke bemannes i tilstrekkelig grad, slik at sakene som skal inn for organer vil forsinke saksbehandlingen vesentlig.

Nasjonalt

Men selv med en ny EU-forordning vil de fleste sakene vi behandler fortsatt være av ren nasjonal karakter. Vi opplever å ha god dialog med og gode relasjoner til både virksomheter og offentlige etater. Likevel utfordres personvernet betydelig på en rekke områder.

I justissektoren opplever vi for eksempel at grensene for økt overvåkingstrykk, flyttes gradvis. Det har ikke vært noen samlet gjennomgang av personvernets kår på justissektoren, og Datatilsynet har derfor foreslått at det opprettes en personvernkommisjon på denne sektoren. I tillegg er vi opptatt av at det ved alle inngripende tiltak må foretas en grundig personvernutredning, og at forholdet til Den europeiske menneskerettskonvensjonen (EMK) også må vurderes.

Vi er opptatt av å fremme prinsippene for innebygd personvern. I offentlig sektor forutsetter dette at vi får delta i de fora der det treffes viktige beslutninger om digitalisering, og at det legges inn som en føring i sentrale dokumenter at prinsippene skal følges. Det er beklagelig at innebygd personvern ikke er nevnt overhodet i digitaliseringsrundskrivet. Vi mener også at Datatilsynet burde hatt en naturlig plass i samarbeidsorganet SKATE. Dette blir ikke mindre viktig når forordningen trer i kraft, og det blir et krav i lovverket at man skal følge disse viktige prinsippene.

Regelverksetterlevelsen i offentlig sektor gir også grunn for bekymring. De siste årene har vi gjennomført flere titalls kontroller i kommuner og ved skoler, og vi har avdekket til dels store mangler, særlig når det gjelder internkontroll og informasjonssikkerhet. Vår strategi har vært, ved hjelp av tilsyn, å synliggjøre utfordringene i sektoren, for så å få sektoren til selv å ta ansvar. På skolesektoren har dette lyktes ved at Senter for IKT i Utdanningen har fått i oppdrag å utarbeide en norm for personvern og informasjonssikkerhet. I kommunesektoren generelt håper vi å få kommunenes interesseorganisasjon (KS) til å være en pådriver for bedre etterlevelse av regelverket. Vi vil følge utviklingen tett, og bidra konstruktivt inn i de prosessene som settes i gang.

Den teknologiske utviklingen går svært raskt og utfordrer personvernet, men den gir også nye muligheter. I meldingsåret la vi fram rapporten «Det store Datakappløpet – om kommersiell bruk av personopplysninger». Vi er det første datatilsynet i verden som analyserer markedet for automatisert annonsesalg på en så grundig måte, og har store ambisjoner om å snu en utvikling som har gått i feil retning lenge. Målet er å tvinge fram mer åpenhet, bedre valgfrihet og sporingsfri løsninger. Vi er avhengige av god kompetanse, samarbeid med andre myndigheter og ikke minst stabile ressurser for å kunne gå inn i et slikt marked. Det er krevende, men har tro på at vi skal lykkes.

Oppsummert er vi av den oppfatning at Datatilsynet er godt rustet til å møte framtidens utfordringer. Vi har dyktige og dedikerte medarbeidere, en tilfredsstillende ressursituasjon, høy troverdighet og vi oppfattes som en konstruktiv samtale- og samarbeidspartner. Vi vil lykkes med implementering av den nye forordningen, og vi er sikre på at vi med et nytt regelverk vil være enda bedre rustet til å møte utfordringene som møter oss i årene som kommer.

VEDLEGG

Gjennomførte kontroller

Saksnr.	Tilsynsobjekt	Type virksomhet
14/01426	Kommunekontroll IK IS - Troms Fylkeskommune	Offentlig
14/01427	Prosjekt - Reisebransje - Helsereiser AS	Reiseselskap
14/01433	Prosjekt - Reisebransje - Hurtigruten AS	Reiseselskap
14/01434	Prosjekt - Reisebransje - Ving Norge AS	Reiseselskap
14/01435	Prosjekt - Reisebransje - TUI Norway Holding AS	Reiseselskap
14/01437	Etterkontroll - Brevkontroll hos Narvik kommune	Andre
14/01440	Kommunekontroll IK IS - Gran Kommune	Offentlig
15/00003	Uanmeldt kontroll hos Restaurant Sjakk Matt Vika AS - Kameraovervåking	Kamera
15/00021	Kontroll ved Hvite Busser AS i Porsgrunn 03032015 - Internkontroll og informasjonssikkerhet	Reiseselskap
15/00184	Kontroll hos Fylkesmannen i Oslo og Akershus 26032015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00201	Kontroll av Rixvaksiner.com hos GlaxoSmithKline AS 13032015	Helse
15/00209	Kontroll hos Ankerskogen svømmehall Hamar KF 17032015 - kameraovervåking i virksomhetens lokaler	Kamera
15/00246	Kontroll hos Skatteetaten 09042015 - Ansattes e-post og hjemmeområder	Arbeidsliv
15/00261	Kontroll hos Universitetet i Bergen 15042015 - Ansatte og studenters e-post og hjemmeområder	Arbeidsliv
15/00263	Kontroll hos Statoil 14042015 - Ansattes e-post og hjemmeområder	Arbeidsliv
15/00267	Kontroll hos Kripos 19052015 - DNA-registeret	Justis
15/00283	Kontroll hos Namsfogden i Oslo 15042015	Offentlig
15/00322	Kontroll hos Horten kommune 24042015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00352	Brevkontroll med Helse Bergen HF - Felles pasientdatabase i Helse Vest	Helse
15/00361	Kontroll hos Finans Norge 23042015 - Forsikringsselskapenes sentrale skaderegister FOSS	Finans
15/00385	Brevkontroll med Helse Fonna HF - Felles pasientdatabase i Helse Vest	Helse
15/00386	Brevkontroll med Helse Førde HF - Felles pasientdatabase i Helse Vest	Helse
15/00387	Brevkontroll med Helse Stavanger HF - Felles pasientdatabase i Helse Vest	Helse
15/00436	Kontroll hos Fylkesmannen i Nord-Trøndelag 15062015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00437	Kontroll hos Steinkjer kommune 15062015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00499	Kontroll hos Kongsvinger kommune 18052015 - Internkontroll og informasjonssikkerhet	Offentlig

Saksnr.	Tilsynsobjekt	Type virksomhet
15/00500	Kontroll hos Våler kommune 18052015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00501	Kontroll hos Østfold Fylkeskommune 28052015 - Internkontroll og informasjonssikkerhet	Offentlig
15/00528 15/01310	Kontroll hos XO Bar i Stavanger 17062015 - Publisering av kameraovervåking på Internett	Kamera
15/00535	Kontroll hos 24-7 Treningssenter Mariero AS 17062015 - Timoteiveien - Kameraovervåking	Kamera
15/00743	EVRY - Brevkontroll - Kontroll med kryptering hos databehandlere	Kryptering
15/00753	Basefarm - Brevkontroll - Kontroll med kryptering hos databehandlere	Kryptering
15/00754	Sykehuspartner - Brevkontroll - Kontroll med kryptering hos databehandlere	Kryptering
15/00858	Kontroll hos Tusenfryd 21082015 - Kameraovervåking	Kamera
15/00918 15/01532	Kontroll hos NTNU - Institutt for samfunnsforskning 06102015	Forskning
15/00920	Kontroll hos Høgskolen i Oslo og Akershus 09102015 - Velferdsforskningsinstituttet NOVA	Forskning
15/00921 15/01533	Kontroll hos IRIS Samfunnsforskning 07102015	Forskning
15/00922 15/01458	Brevkontroll med Institutt for samfunnsforskning	Forskning
15/00923 15/01456	Brevkontroll med Forskningsstiftelsen FAFO - Samfunnsforskning	Forskning
15/00924 15/01462	Brevkontroll med Frischsenteret - Samfunnsforskning	Forskning
15/00932 15/01319	Kontroll hos Tjuvholmen Drift AS 24092015 - Kameraovervåking av det offentlige rom	Kamera
15/00982	Etterkontroll hos Husbanken 19112015 - Registrering av personopplysninger etter ny hjemmel i bostøtteloven	Andre
15/00983 15/01370	Kontroll hos Trondheim kommune 27112015 - Digitalisering av elevmapper - Tilgangsstyring	Andre
15/00984 15/01443	Kontroll hos Biblioteksystemer AS - Nasjonalt lånekort og kryptering av fødselsnummer	Andre
15/00999 15/01303	Kontroll hos Triaden Lørenskog Storsenter 15102015 - Kameraovervåking	Kamera
15/01035	Kontroll hos Verdal kommune 09112015 - Internkontroll og informasjonssikkerhet	Offentlig
15/01036	Kontroll hos Levanger kommune 09112015 - Internkontroll og informasjonssikkerhet	Offentlig
15/01038	Kontroll hos Stjørdal kommune 10112015 - Internkontroll og informasjonssikkerhet	Offentlig
15/01041	Kontroll hos Vestby kommune 04112015 - Internkontroll og informasjonssikkerhet	Offentlig
15/01043	Kontroll hos Nittedal kommune 24112015 - Internkontroll og informasjonssikkerhet	Offentlig
15/01086 15/01313	Kontroll hos Ringsaker Lensmannskontor 04112015 - Kameraovervåking	Kamera

Saknr.	Tilsynsobjekt	Type virksomhet
15/01156 15/01455	Brevkontroll med Uni Research Rokkansenteret - Samfunnsforskning	Forskning
15/01157 15/01460	Brevkontroll med Telemarksforskning - Samfunnsforskning	Forskning
15/01158	Brevkontroll med SINTEF - Samfunnsforskning	Forskning

Saker sendt til Personvernemnda

Tabellen viser alle sakene Datatilsynet har sendt til Personvernemnda for klagebehandling og som er registrert hos nemnda i 2015:

Sak	Klager	Tittel	Dato DT	Sak PVN	Vedtak i PVN
14/00700	Helse-direktoratet	Klage på delvis avslag om konsesjon til å behandle helseopplysninger til forskning - Utredning av behandlingstilbud for personer med kjønnsdysfori og transseksuelle	05.12.2014	PVN-2015-01	
14/00076	Haukeland universitetssykehus - Helse Bergen HF	Klage på vilkår i konsesjon gitt til Nasjonalt kvalitetsregister for smertebehandling - SmerteReg	18.12.2014	PVN-2015-02	Klagen tas ikke til følge
14/00232	Håkon Henriksen	Klage på vedtak om avslag på innsyn i skolens aktivitetslogg	18.12.2014	PVN-2015-03	Klagen tas ikke til følge
14/00071	FaVer AS	Klage på vedtak om pålegg og overtredelsesgebyr	09.01.2015	PVN-2015-04	
13/00330	AS Skan-kontroll	Klage på vedtak om ileggelse av overtredelsesgebyr	21.01.2015	PVN-2015-05	
14/00908	Privatperson	Klage på vedtak om avslag på sletting av treff i søkemotoren Google	22.01.2015	PVN-2015-06	Vedtaket oppheves
14/00518	Dialog Advokater	Klage på vedtak om avslag på krav om innsyn i personopplysninger hos arbeidsgiver - Sommerlys skole - Tromsø kommune	19.03.2015	PVN-2015-07	
14/00028	Windsor Door AS	Klage på ileggelse av overtredelsesgebyr for å ha sammenstilt GPS-data og innleverte timelister uten rettslig grunnlag	27.03.2015	PVN-2015-08	
14/00962	Advokatfirmaet Stiegler ANS	Klage på avslag om dekning av saksomkostninger etter forvaltningsloven § 36 - Kameraovervåking på privat eiendom	28.05.2015	PVN-2015-09	Klagen tas ikke til følge
14/01282	Sykehuset Østfold	Klage på vilkår - Forutsetning om oppfyllelse av informasjonsplikt	02.07.2015	PVN-2015-10	
14/00490	Vardø kommune	Klage på vedtak om overtredelsesgebyr - Internkontroll og informasjonssikkerhet, kontroll	13.08.2015	PVN-2015-11	

Sak	Klager	Tittel	Dato DT	Sak PVN	Vedtak i PVN
14/01228	Universitetet i Oslo	Klage på avslag på søknad om konsesjon til å behandle helseopplysninger - Sammenstilling av helseopplysninger fra Reseptregisteret	31.08.2015	PVN-2015-12	
12/00947	Trønder Taxi AS	Klage på pålegg om opphør av opptak av telefonsamtaler	28.08.2015	PVN-2015-13	
14/00838	Viken Økonomi	Klage på vedtak om overtredelsesgebyr - Innsyn i tidligere arbeidstakers e-post	18.09.2015	PVN-2015-14	
14/01190	Mona Lisa Huset	Klage på vedtak om pålegg og overtredelses - Bruk av kameraovervåking	15.10.2015	PVN-2015-15	
14/01041	Walhalla Shop Ltd	Klage på vedtak om overtredelsesgebyr - Publisering av kameraovervåking på Internett	16.09.2015	PVN-2015-16	
15/01066	Bisnode Norge AS	Klage på avvisningsvedtak - Søknad om endring av kredittopplysningskonsesjon	16.11.2015	PVN-2015-17	
15/01365	Norgesgruppen ASA	Klage på avslag på søknad om utvidet lagringstid for kameraopptak av Bank i Butikk - BIB	16.12.2015		

Høringer

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

	Dok. nr.	Tittel	Til/fra
1	15/00903-2	Høringsuttalelse - Endringer i a-opplysningsloven - Utvidelse av arbeids- og velferdsetatens tilgang til opplysninger i a-ordningen	Arbeids- og sosialdepartementet
2	15/00953-2	Høringsuttalelse - Endringer i universitets- og høyskoleloven - Nasjonal vitnemålsbank	Kunnskapsdepartementet
3	15/01193-3	Høringsuttalelse - Forsendelse og salg av legemidler over internett	Helse- og omsorgsdepartementet
4	15/00758-2	Høringsuttalelse - Utredning av konsekvenser ved en mulig lisensordning for pengespill	Kulturdepartementet
5	15/00972-2	Høringsuttalelse - Forslag til endringer i verdipapirfondloven mv. (UCITS V)	Finansdepartementet
6	15/01059-2	Høringsuttalelse - Forslag til endringer i psykisk helsevernloven - Kontroll for å hindre innføring av legemiddel - rusmiddel - skadelige stoffer - farlige gjenstander og rømningshjelpemiddel	Helse- og omsorgsdepartementet
7	15/00729-2	Høringsuttalelse - Utkast til forskrifter om straffegjennomføring i Nederland	Justis- og beredskapsdepartementet
8	15/00654-2	Høringsuttalelse - NOU 2015:8 Fremtidens skole - Fornyelse av fag og kompetanser - Kunnskapsdepartementet	Kunnskapsdepartementet
9	15/00799-3	Høringsuttalelse - Noark 5 tjenestegrensesnitt - Riksarkivet	Riksarkivet
10	15/00723-2	Høringsuttalelse - Nytt kommunalt pasient- og brukerregister	Helse- og omsorgsdepartementet
11	15/00728-2	Høringsuttalelse - Forslag om endring av forskrift om IT-standarder i offentlig forvaltning - 2015	Direktoratet for forvaltning og IKT
12	15/00761-2	Høringsuttalelse - Forslag til endringer i reglene for telefonsalg	Barne- likestillings- og inkluderingsdepartementet
13	15/00588-2	Høringsuttalelse - Forskningsetiske retningslinjer for samfunnsvitenskap humaniora juss og teologi	De nasjonale forskningsetiske komiteer
14	15/00556-2	Høringsuttalelse - Forslag til endringer i sikkerhetsloven - Forsvarsdepartementet	Forsvarsdepartementet
15	14/01380-3	Høringsuttalelse - Overføring av forvaltningsoppgaver fra Toll- og avgiftsetaten til Skatteetaten - særavgift for uregistrerte og innførselsmerverdiavgift	Finansdepartementet
16	15/00721-2	Høringsuttalelse - Endringer i byggesaksforskriften - Nye krav til sentralt godkjente foretak mv - Kommunal- og regionaldepartementet	Kommunal- og regionaldepartementet
17	15/00677-2	Høringsuttalelse - Gjennomføring av forordning (EU) nr 376/2014 om rapportering av luftfartshendelser mv - endring av luftfartsloven kapittel XII - Samferdselsdepartementet	Samferdselsdepartementet

	Dok. nr.	Tittel	Til/fra
18	15/00520-2	Høringsuttalelse - Forslag om endringer vedrørende bilbeskatning - Skattedirektoratet	Skattedirektoratet
19	15/00625-2	Høringsuttalelse - Tilleggshøring om Elhub - Endring i avregningsforskriften - Norges vassdrags- og energidirektorat - NVE	Norges vassdrags- og energidirektorat
20	15/00374-2	Høringsuttalelse - Opplysningsplikt om finansiell informasjon på skatteområdet	Finansdepartementet
21	15/00373-2	Datatilsynets høringsuttalelse - Forslag til ny folkeregisterlov - Finansdepartementet	Finansdepartementet
22	15/00345	Høringsuttalelse - NOU 2015:2 Å høre til - Virkemidler for et trygt psykososialt skolemiljø	Kunnskapsdepartementet
23	15/00336-2	Høringsuttalelse - EPJ standard del 2	Helsedirektoratet - Avdeling Standardisering
24	15/00114-2	Høringsuttalelse - Rapport 2.0 for Kritisk informasjon for kjernejournal - En nasjonal standard for integrasjonen mot kjernejournal	Helsedirektoratet
25	15/00059-3	Høringsuttalelse - Forslag til endringer i forskrift om skikkethetsvurdering i høyere utdanning - Kunnskapsdepartementet	Kunnskapsdepartementet
26	15/00287-2	Høringsuttalelse - Revisjon av Statens standardavtaler 2014/15	Direktoratet for forvaltning og IKT
27	15/00072-2	Høringsuttalelse - Forslag til retningslinjer for vurdering av dokumentasjon på identitet	Nasjonalt ID-senter
28	14/01359-4	Høringsuttalelse - NOU 2014:10 Skyldevne sakkyndighet og samfunnsvern	Justis- og beredskapsdepartementet
29	15/00176-2	Høringsuttalelse - Endring i straffegjennomføringsloven	Justis- og beredskapsdepartementet
30	14/00255-4	Høringsuttalelse - Forslag til endringer i forskrift om Lånekassens adgang til innhenting av opplysninger	Kunnskapsdepartementet
31	14/01386-2	Høringsuttalelse - Veileder for rusmestringsenhetene	Kriminalomsorgsdirektoratet
32	14/01350-2	Høringsuttalelse - Forslag til ny skatteforvaltningslov	Finansdepartementet
33	14/01436-2	Høringsuttalelse om endring av førerkortforskriften vedlegg 1 om helsekrav	Statens vegvesen - Vegdirektoratet
34	14/01399-2	Høringsuttalelse - Forslag om å utvide a-opplysningslovens virkeområde til å omfatte utbetaling av pensjonsytelser etter lov om individuell pensjonsordning og etter pensjonsavtale etter skatteloven - Skattedirektoratet	Skattedirektoratet
35	14/01412-2	Høringsuttalelse - Forslag til lov om intelligente transportsystemer innenfor vegtransport og for grensesnittet mot andre transportformer (ITS-loven) samt utkast til forskrifter	Statens vegvesen - Vegdirektoratet
36	14/01246-2	Høringsuttalelse - utkast til ny postlov og postforskrift	Samferdselsdepartementet
37	14/01335-2	Høringsuttalelse - Forslag til endringer i barnehageloven og tilhørende forskrifter - Lovhjemmel for barnehagers behandling av personopplysninger i forbindelse med dokumentasjon og vurdering	Kunnskapsdepartementet

	Dok. nr.	Tittel	Til/fra
38	14/01391-2	Høringsuttalelse - Forslag til endringer i politiloven og ekomloven - mobilregulerte soner mv	Justis- og beredskapsdepartementet
39	15/01315	Høringsuttalelse - Advokatutvalgets utredning NOU 2015:3 - Advokaten i samfunnet	Justis- og beredskapsdepartementet

Ilagte sanksjoner

Mottaker	Vedtaksbrev	Størrelse	Kommentar	Stikkord
Fjell kommune	27.03.2015	100.000	Avsluttet	<i>Ulovlig utlevering av personopplysninger</i>
Norgesregnskap Viken Økonomi AS	16.04.2015	75.000	Klagesak i PVN	<i>Ulovlig innsyn i e-post</i>
Walhalla Shop Ltd	23.04.2015	25.000	Klagesak i PVN	<i>Ulovlig publisering av bilder fra overvåkingskamera</i>
Justis- og beredskapsdepartementet	30.04.2015	100.000	Avsluttet	<i>Mangelfull internkontroll</i>
Vardø kommune	30.04.2015	50.000	Klagesak i PVN	<i>Mangelfull internkontroll</i>
Hovedredningssentralen Nord-Norge	30.04.2015	50.000	Klagesak i PVN	<i>Mangelfull internkontroll</i>
Flekkefjord kommune	30.04.2015	50.000	Avsluttet	<i>Mangelfull internkontroll</i>
Eigersund kommune	30.04.2015	150.000	Avsluttet	<i>Mangelfull internkontroll</i>
Mona Lisa huset	22.06.2015	150.000	Klagesak i PVN	<i>Ulovlig/Skjult kameraovervåking</i>
Unique Cinema Systems - UCS	03.07.2015	100.000	Avsluttet	<i>Ulovlig utlevering av sensitive opplysninger</i>
Trønder Taxi AS	07.07.2015	100.000	Avsluttet	<i>Opplysninger brukt til et uforenlig formål.</i>
Gant Store Stortingsgaten i Tønsberg	19.10.2015	25.000	Avsluttet	<i>Ulovlig kameraovervåking</i>
Farsund Resort AS	20.10.2015	100.000	Avsluttet	<i>Ulovlig innsyn i e-post</i>
Vaktmester Andersen AS	16.11.2015	100.000	Klagesak i PVN	<i>Arbeidsliv - Bruk av elektronisk kjørebok</i>
Justis- og beredskapsdepartementet	30.11.2015	25.000	Avsluttet	<i>Ulovlig publisering av bilder fra overvåkingskamera</i>
Synkron Meida AS	08.12.2015	75.000	Ikke avsluttet	<i>Ulovlig innsyn i e-post</i>