

Datatilsynets strategi 2011 – 2016

11.11.2011



Innholdsfortegnelse

Dette er Datatilsynet	Side 3
Visjon, verdier og overordnede mål	Side 4
Hva er personvern?	Side 6
Personvern i dag	Side 10
Roller og bruk av virkemidler	Side 16
Strategiske satsinger	Side 19

Dette er Datatilsynet

Datatilsynet ble opprettet i 1980 og er et uavhengig forvaltningsorgan underlagt Fornyings- administrasjons og kirke departementet. En hovedoppgave er å føre tilsyn med blant annet personopplysningsloven, helseregisterloven og helseforskningsloven. I tillegg til å behandle enkeltsaker og drive tilsynsarbeid skal Datatilsynet identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses. Datatilsynet skal også holde seg orientert og informere om den nasjonale og internasjonale utviklingen i behandlingen av personopplysninger, og om de problemene som knytter seg til slik behandling.

Datatilsynet har også en viktig ombudsrolle. I den forbindelse drives rådgivning og informasjon overfor enkeltpersoner som tar kontakt med tilsynet. Vi skal, som ledd i dette, også delta aktiv i persovnerndebatten.

Visjon, verdier og overordnede mål

Visjon

Vår visjon kan enkelt oppsummeres i følgende ti ord:

***Datatilsynet – i front for retten til
selvbestemmelse, integritet og verdighet***

Verdier

Verdiene skal prege måten Datatilsynet arbeider på, hvordan vi opptrer overfor hverandre som kollegaer og hvordan vi utøver våre roller som henholdsvis forvaltningsorgan og ombud for personvernet. Ledelse og medarbeidere må derfor, når det er nødvendig, minne hverandre på de verdiene vi er blitt enige om at skal prege vår virksomhet, slik at disse blir mer enn bare fagre ord.

Datatilsynets verdigrunnlag:

Uredd

- Vi skal være en modig og tydelig stemme i personverndebatten og en sterk forsvarer av grunnleggende personvernprinsipper
- Vi skal tørre å innrømme feil
- Vi skal ha en åpen tilbakemeldingskultur internt

Entusiastisk

- Vi skal beholde og videreutvikle en kultur som gjør at alle medarbeidere opplever Datatilsynet som en stimulerende og meningsfull arbeidsplass
- Vi skal oppfordre hverandre til nytenking og initiativ
- Vi skal ha toleranse for at det er lov å feile

Troverdig

- Vi skal være lydhøre og møte andre med interesse, respekt og dialog
- Vi skal være tydelige på når vi utøver vår forvaltningsrolle og når vi utøver vår ombudsrolle
- Vi skal sørge for at våre avgjørelser, uttalelser og vurderinger er solid forankret i faglig kunnskap, dokumentert praksis og erfaringer

Kunnskapsrik

- Vi skal være fremtidsrettede og godt orientert om teknologiutvikling og andre samfunnsmessige trender og utviklingstrekk
- Vi skal ha god kunnskap om ulike brukergrupper og målgruppers behov og synspunkter
- Vi skal stimulere til, og gi medarbeidere reell mulighet til å videreutvikle seg faglig

Overordnede mål

- Vi skal sette borgeren i stand til å ivareta sitt eget personvern
- Vi skal aktivt kontrollere at lover og regler følges
- Vi skal være Norges mest kompetente fagmiljø på personvern
- Vi skal ha stor synlighet i personverndebatten

Hva er personvern?

Personvern er et begrep med mange nyanser og ulike forståelser av. Det finnes derfor ikke én presis og god definisjon på hva personvern er. Mange kan imidlertid være enige om at det enkelt sagt handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.

Retten til privatlivets fred

Alle mennesker har en ukrenkelig egenverdi. Som enkeltmenneske har du derfor rett på en privat sfære som du selv kontrollerer - hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker. Retten til privatlivets fred er blant annet forankret i Den Europeiske Menneskerettighetskonvensjonen artikkel 8, hvor det heter:

Vi har alle noe vi ikke ønsker å dele med andre. Ikke fordi vi gjør noe ulovlig, eller har noe å skjule, men rett og slett fordi vi vil være i fred. Personvern handler om at man har grenser for hvor nært innpå seg man vil slippe andre. Retten til privatliv har en verdi som er vanskelig å måle. Mange av oss ser verdien først når personopplysninger er på avveie og vi opplever at vår integritet er truet.

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse».

Personvern er ikke bare en viktig menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet og privatliv. Personvern er også viktig for å sikre felles goder i et demokratisk samfunn. Uten retten til å ha et privatliv vil det ikke være mulig for det enkelte menneske å skape seg et rom til å utvikle refleksjoner og vurderinger på et selvstendig grunnlag, uten å bli forstyrret eller kontrollert av andre. Et dårlig ivaretatt personvern vil også sette demokratiet i fare ved at borgerne begrenser sin deltakelse i åpen meningsutveksling og politisk aktivitet. Den enkelte kan frykte at opplysninger om personlige forhold kan bli trukket frem og gjort til allmenn oppmerksomhet. Man kan også sette begrensninger på seg selv fordi man frykter at myndighetene registrerer og

lagrer opplysninger om ens kommunikasjon med andre, ens ferdsel, interesser eller uttrykk for holdninger.

Retten til å bestemme over egne personopplysninger

Personvernbegrepet refererer ikke bare til vernet av privatlivets fred og den enkeltes personlige integritet. I norsk forståelse innebærer begrepet i stor grad også vernet av individers rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Den enkelte skal i størst mulig grad kunne bestemme over egne personopplysninger.

Grunnleggende personvernprinsipper

Den norske personvernlovgivningen bygger på en kjerne av grunnleggende personvernprinsipper som har sitt utgangspunkt i en europarådskonvensjon(1), retningslinjer fra OECD(2) og EU sitt personverndirektiv. Disse er allment benyttet og henvist til i norsk personvernlitteratur(3). Respekten for den enkeltes selvbestemmelse, integritet og verdighet oppnås først og fremst ved å minimalisere registrering og bruk av personopplysninger til det strengt nødvendige. Dernest bør man i størst mulig grad basere seg på samtykke fra den enkelte. Det handler rett og slett om å respektere den enkeltes rett til i størst mulig grad å kunne ha kontroll over egne personopplysninger.

Samtykke eller annet rettslig grunnlag

Behandling av personopplysninger skal i størst mulig grad være basert på frivillig, uttrykkelig og informert samtykke. I mange tilfeller krever imidlertid fellesskapet at det behandles opplysninger om deg enten du vil eller ikke, for eksempel ved ileggelse av skatt og utbetaling av trygd. Dersom behandlingen av personopplysninger ikke baseres på samtykke må det foreligge et annet rettslig grunnlag.

¹ Europarådskonvensjon nr 108 av 1981

² *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*

³ *Fremstillingen nedenfor er blant annet bygget på Teknologirådets gjengivelse av prinsippene i Rapport 1:2005 – "Elektroniske spor og personvern", side 25, og Personvernkomisjonens rapport, NOU 2009:1 – "Individ og integritet" side 291, jf også Schartum og Bygrave, "Personvern i informasjonssamfunnet", Fagbokforlaget 2004*

Proporsjonalitet

All innsamling og videre behandling av personopplysninger må skje i overensstemmelse med lovverket, og på en måte som anses rimelig i forhold til den registrerte. Med dette menes at behandlingen ikke må medføre urimelig belastning for den enkeltes selvråderett eller integritet. Man må balansere hensynene til de ulike involverte partene og påse at registreringen av opplysninger står i proporsjonalitet med formålet. I valget av to alternative løsninger ved behandling av personopplysninger skal man velge det alternativet som er minst personverninnngripende.

Formålsbestemthet

Personopplysninger må samles inn og benyttes kun for bestemte og legitime formål. I tråd med dette prinsippet skal opplysningene ikke senere brukes til andre formål som er uforenlige med det opprinnelige formålet. Dette gjelder med mindre det innhentes samtykke, eller det foreligger et annet rettslig grunnlag.

Relevans

Personopplysninger skal bare innhentes, lagres og benyttes i den grad det er nødvendig for å oppnå det legitime formålet med behandlingen av opplysningene. Har man strengt tatt ikke behov for å registrere personopplysninger skal man heller ikke gjøre det. Overskuddsinformasjon skal unngås. Innsamlede data som ikke lenger er nødvendige for det angitte formål må slettes eller anonymiseres. Under dette prinsippet ligger også det hensyn at enkeltindivider av og til må gis mulighet til å legge fortiden bak seg og begynne med blanke ark, for eksempel når det gjelder straffbare forhold eller betalingsanmerkninger.

Fullstendighet og kvalitet

Personopplysninger må være relevante, korrekte og fullstendige i forhold til det formål de skal benyttes til. Dette innebærer at opplysninger som ligger til grunn for behandling skal være oppdaterte og nøyaktige, og ikke inneholde irrelevant informasjon. Opplysninger som er lagret i et register skal ofte brukes som grunnlag til å fatte beslutninger om de registrerte. Dette prinsippet skal dermed sikre at beslutninger ikke blir fattet på et ufullstendig eller feilaktig grunnlag.

Informasjon og innsyn

Prinsippet springer ut av forståelsen om det opplyste individ. I dette ligger det en rett til å bli informert om innsamling og bruk av personopplysninger.

Dernest ligger det en rett til kostnadsfritt å få innsyn i de opplysninger som er registrert om seg selv. Det skal også gis mulighet til å få slettet eller korrigert opplysninger som er feilaktige eller misvisende. Den registrerte har videre rett til å få en manuell vurdering av avgjørelser som fullt ut er basert på automatisert behandling av personopplysninger, dersom den avgjørelse som taes er av vesentlig betydning for vedkommende.

Informasjonssikkerhet

De som oppbevarer personopplysninger må treffe nødvendige tiltak for å sikre opplysningene mot uautorisert tilgang, endring, ødeleggelse og spredning.

Opplysningene må også beskyttes mot ødeleggelse som følge av uhell. Man må også sikre at personopplysningene faktisk er tilgjengelig for de som skal ha lovlig tilgang til opplysningene, for eksempel når den registrerte ber om innsyn i egne opplysninger.

Særlig strenge regler ved behandling av sensitive personopplysninger

Behandling av sensitive personopplysninger er underlagt særlig strenge regler.

Personopplysningsloven nevner følgende kategorier av opplysninger som sensitive: rasemessig eller etnisk opphav, politisk, religiøs eller filosofisk oppfatning, medlemskap i fagforeninger, helse og seksuelle forhold. Videre opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling.

Anonymitet og sporfri ferdsel

Det er i utgangspunktet registreringen som skal begrunnes. Hvis man ikke trenger å registrere identifiserende opplysninger har enkeltindividet rett til å være anonym. Dette følger også av prinsippet om rettslig grunnlag og proporsjonalitet. Individet har krav på at det minst personverninngripende tiltaket anvendes for å oppnå et bestemt formål. Hvis formålet kan oppnås uten bruk av personidentifiserbare opplysninger, er det dette alternativet som skal anvendes.

Personvern i dag

Datatilsynet manøvrerer i et krevende landskap i stadig forandring. Dagens teknologidrevne samfunn gjør det enkelt å samle inn, systematisere, analysere og bruke personopplysninger til mange ulike formål. Den enkelte borger er dessuten registrert i en lang rekke private og offentlige registre. Vi ser stadig eksempler på formålsutglidning, som innebærer at opplysninger innsamlet for et formål brukes til et annet. Dette er ingen ny problemstilling, men aktualiseres ytterligere når teknologien gjør det svært enkelt å endre bruken av opplysningene som er samlet inn. Også muligheten for å koble opplysninger og registre er betydelig større enn for bare få år siden.

Datatilsynet observerer at selve begrepet personvern utfordres og at stadig nye formål forsøkes presset inn i personvernbegrepet. Det argumenteres med at personvernet er ivaretatt bare opplysningene er sikkert oppbevart. Dette bryter med den tradisjonelle personverntenkningen som er nedfelt i personvernprinsippene.

Etter Datatilsynets erfaring brytes det viktige prinsippet om retten til å få opplysninger slettet fordi det ofte er billigere å lagre opplysninger enn å slette dem. Stadig mer data lagres dessuten i nettskyen. Ofte vet ikke den enkelte hvor dataene lagres, hvem som har tilgang, hvor sikker lagringen er, eller om dataene slettes. I mange tilfeller er store multinasjonale selskaper ansvarlig for lagringen og databehandleravtalene er i stor utstrekning standardkontrakter uten forhandlingsrom. Dette endrer den tradisjonelle tenkningen som ligger bak personvernlovgivningen om den behandlingsansvarlige som den sterke part i forholdet.

Et sporbart liv

Et fremtredende trekk med dagens samfunn er at stadig flere transaksjoner skjer elektronisk. Kontant betaling og manuell behandling forsvinner gradvis. I kollektivtransporten har utviklingen entydig gått i retning av færre alternativer for kontant betaling og mulighet for anonym ferdsel. Manuell betaling i

bomringer er forsvunnet. Våre trafikkdata registreres i stor skala. Det er også en politisk målsetting at flere og flere transaksjoner skal skje elektronisk. Levering av selvangivelse og bestilling av frikort for helsetjenester kan tjene som eksempler. Det tas også til orde for at alle økonomiske transaksjoner skal skje elektronisk og at mynt og sedler skal fases ut.

Det er selvsagt mange fordeler med en slik utvikling. Elektroniske transaksjoner er ofte billigere for den næringsdrivende og mange vil oppleve det som enklere å bruke ulike typer automatiserte løsninger. Et langt stykke på vei må borgeren også akseptere at det registreres personopplysninger. Har man avtale med en bank må det selvsagt skje en registrering av uttak fra minibank og betaling av regninger. Teleselskapene må også, av faktureringshensyn, ha oversikt over hvor deres kunder har ringt.

Samtidig innebærer denne utviklingen at borgeren i løpet av en dag legger igjen en rekke elektroniske spor. Disse kan i sin tur avsløre hvor hun har vært, hva hun har brukt penger på og hvem hun har vært i kontakt med.

Det er et viktig utgangspunkt at den enkelte selv kan velge om han eller hun ønsker en anonym eller registrert løsning. I dag er dette ofte ikke et reelt valg. Det er derfor viktig for Datatilsynet å verne om, og jobbe for, de anonyme alternativene. Dette innebærer ikke at vi ønsker oss tilbake til et samfunn med kun kontanter og papirbilletter, men at anonyme løsninger må bygges inn i elektroniske systemer gjennom for eksempel anonyme reisekort, påfyllingskort og lignende.

Dernest har Datatilsynet gjennom mange år erfart at det samles inn og behandles mer personopplysninger enn det som trengs for å utføre tjenesten. Gjennom dataminimalisering og innebygget personvern kan dette forhindres. Videre vil det alltid være en relativt stor krets av personer som kan ha tilgang til registrerte data. Det kan være de ansatte i de ulike selskapene borgerne inngår avtaler med, eller ansatte hos de som utvikler og vedlikeholder datasystemene. De fleste vil oppfatte det som krenkende dersom uvedkommende får

tilgang til for eksempel hvilke økonomiske transaksjoner vi foretar, hvilke reiser vi gjør, eller hvilken helse vi har.

Teknologiens uendelige muligheter

Vi bruker i dag teknologi i nær sagt alle våre gjøremål. Dette har utvilsomt mange fordeler for den enkelte. Samtidig utfordrer ny teknologi personvernet. Tredje fase i internettutviklingen, web 3.0, skaper nye utfordringer. I web 2.0 var brukermedvirkning og involvering viktige stikkord. Web 3.0 kalles ofte 'tingenes Internett'. Applikasjoner, sensorteknologi og at gjenstander har internettadresse og kommuniserer direkte med brukerne, er eksempler på dette. Intelligente datamaskiner kartlegger våre bevegelser og søk og danner svært detaljerte mønstre om hvordan vi opptrer på nettet. Dette bygger man tjenester på, og opplysningene selges videre til tredjeparter og brukes til å skreddersy reklame. Det krever stor kompetanse og innsikt for å følge med på utviklingen og å være aktuell i forhold til de problemer som oppstår.

Stadig flere prosesser automatiseres. Dette gjelder også i offentlig forvaltning, der mange vedtak treffes uten at en saksbehandler har sett på saken. Dette skaper særlig utfordringer i forhold til kvalitet på avgjørelsen, og at folk ikke har kjennskap til at avgjørelsen faktisk er automatisert.

Befolkningen blir eldre og teknologien blir bedre. Bruk av teknologi i omsorgssektoren, som for eksempel GPS-sporing, fallsensorer og 'elektroniske gjerder' er i stadig utvikling. Dette er også et satsingsfelt både i politikk og forskning. Fra et personvernståsted er det stor forskjell mellom kontinuerlig overvåking av den eldre, og en sensor som aktiveres ved fall. Datatilsynet er derfor opptatt av at teknologi brukes på en mest mulig personvernvennlig måte. Innenfor velferdsteknologien og andre teknologiløsninger bør derfor prinsippet om 'innebygget personvern' legges til grunn. Særlig viktig er kravet om at den personvernvennlige løsningen skal være førstevalg, at løsningene skal være brukervenlig og at personvernløsningen må bygges inn fra personopplysningens vugge til grav.

Internett og sosiale medier

Folk legger i dag igjen store mengder elektoriske spor og åpne personopplysninger om seg selv på Internett. Det kan imidlertid stilles spørsmål ved om hvor frivillig dette egentlig er. For å surfe på nett må man bruke en søkemotor. Mange føler dessuten et sterkt sosialt press for om å være med i et sosialt nettsamfunn. Datatilsynet mottar dessuten henvendelser fra arbeidstakere som opplever pålegg fra arbeidsgiver om å melde seg inn i sosiale nettsamfunn.

Opplysninger vi legger igjen på nettet er potensielt avslørende for våre interesser og våre bevegelser, men brukes også, ofte uten vår viten, til å skreddersy reklame. Personopplysninger er blitt en handlevare med stor økonomisk verdi. Dessuten er vi bare i begynnelsen på de sosiale mediernes tidsalder. Facebook ble etablert i 2006 og er fortsatt et ungt selskap. Vi må derfor være på vakt ikke bare mot hvordan de og andre sosiale nettsamfunn samler inn og bruker personopplysninger i dag, men også hva de vil bruke opplysningene til i framtida.

Personvern og offentlig sektor

Borgernes rett til medbestemmelse er et viktig personvernprinsipp. Datatilsynet opplever imidlertid at personopplysninger ofte behandles uten at dette prinsippet oppfylles. Dette kan ha gode grunner for seg. Samtidig er det viktig å være særlig oppmerksom i situasjoner der den enkelte har et avhengighetsforhold til den behandlingsansvarlige, eller der behandlingen er hjemlet i lov. Det gjelder særlig i offentlig sektor, som for eksempel i helsetjenesten, i Forsvaret og i kommunal sektor.

Ofte dreier det seg om sensitive personopplysninger. Det er da særlig viktig at den behandlingsansvarlige har gode rutiner for behandling og god oversikt over hvilke opplysninger som behandles. Datatilsynet utførte en kartlegging mot norske kommuner som viste at kommunene gjennomgående hadde for dårlig oversikt over hvilke personopplysninger de behandlet og hvilke regelverk som gjelder på de ulike områdene. Internkontrollsystemene var også mangelfulle. Dette underbygges av erfaringen fra Datatilsynets klagesaksbehandling og tilsynsvirksomhet. Vi avdekker jevnlig svikt i offentlig sektors behandling av

personopplysninger, for eksempel ved at sensitive opplysninger havner i postjournalene.

Etter Datatilsynets vurdering er det særlig viktig at det gis god informasjon om hva slags opplysninger som behandles, og hva de brukes til. Datatilsynet har erfaring med at offentlige etater gjennomgående er lite flinke til å opplyse om hva slags personopplysninger de behandler og hva de gjør med opplysningene. Dette er særlig alvorlig ettersom behandlingen ikke er basert på samtykke. Opplysningsplikten er derfor svært viktig når det offentlige behandler personopplysninger.

Regler om taushetsplikt og tilgangsstyring skal ivareta borgernes konfidensialitet. Datatilsynets rapport 'Sviktende tilgangsstyring i elektroniske pasientjournaler' (april 2009), dokumenterte store mangler i tilgangsstyringen i helseforetakene. Tilsvarende funn er gjort både i kommunal sektor og etter tilsyn mot NAV-kontorer.

Offentlig sektor er avhengig av borgernes tillit. Et viktig bidrag for å bygge tillit er at det gis god informasjon, at konfidensialiteten sikres og at regelverket følges når offentlig sektor behandler personopplysninger.

Kriminalitetsbekjempelse og kontroll med borgerne

Justissektoren håndterer store mengder personopplysninger. Det er et gjennomgående trekk at borgeren har minimalt med autonomi og har begrenset kunnskap om hvilke opplysninger som samles inn og hva de brukes til. Dette er utfordrende fra et personvernståsted, særlig fordi sektoren har hjemmel til å bruke tvangsmidler.

Ethvert personverninngrepende tiltak må vurderes ut fra et proporsjonalitetsprinsipp, det vil si at inngrepet må være proporsjonalt i forhold til det man skal oppnå med tiltaket. Dette er særlig viktig i justissektoren, ettersom vi ser klare tendenser til at nye trusler ofte møtes med mer overvåking og kontroll.

Datatilsynet opplever dermed at grensene for kontroll og overvåking flyttes. Datalagringsdirektivet ble vedtatt i 2011 og legger opp til lagring ut fra et føre –

var-prinsipp. Det er vanskelig å se hvor man skal trekke den logiske grensen for kontroll og overvåking når man først har åpnet for lagring også i tilfeller der det ikke foreligger en mistanke mot en konkret person.

Respekten for privatlivets fred og retten til fri kommunikasjon er sentralt i personvernet. Datatilsynet frykter en utvikling der kontroll og overvåking oppfattes som så omfattende at folk avstår eller viser forsiktighet med å kommunisere. Dette gjelder særlig de som lever i den såkalte 'randsonen'. Deres handlinger kan være fullt lovlige, men de kan for eksempel ha en seksuell preferanse eller politisk oppfatning som avviker fra flertallets. Dersom den enkelte gjør en risikovurdering før de sender en e-post eller tekstmelding mister vi en vesentlig verdi i vårt samfunn.

Den internasjonale arena

Det internasjonale aspektet blir stadig mer fremtredende. Sentrale deler av personvernlovgivningen er bygget på EU-direktiver, og EU-organer er sentrale i fortolkning av regelverket. Multinasjonale selskaper som Google, Apple og Facebook behandler enorme mengder personopplysninger. Det er utfordrende både å få kunnskap om hva de faktisk gjør og ikke minst komme i inngrep med dem. At disse selskapene er ofte lokalisert utenfor Norge og Europa stiller oss også overfor utfordringer i forhold til jurisdiksjon.

Roller og bruk av virkemidler

Datatilsynets virksomhet kan i hovedsak inndeles i to hovedroller. På den ene siden er Datatilsynet et forvaltnings- og tilsynsorgan som treffer enkeltvedtak og utøver myndighet etter personvernlovgivningen. I tillegg skal Datatilsynet også ivareta en ombudsrolle, med mandat å ivareta og styrke personvernet som samfunnsinteresse. Datatilsynet skal som ledd i dette bidra til debatt og oppmerksomhet om personvernspørsmål, herunder kritisere både offentlige myndigheter og private aktører når de, etter Datatilsynets vurdering, utfordrer personverninteressene. Dette er eksplisitt nevnt i lovforarbeidene til personopplysningsloven. Her sies det at Datatilsynet, i de tilfellene hvor tilsynet ikke finner det mulig eller hensiktsmessig å bruke sin påleggskompetanse, skal *”komme med kritikk og sette søkelyset på problemstillinger som er viktig ut fra personvern hensyn”*(4). Dette gjelder også i saker hvor virksomhetens behandling av personopplysninger faller utenfor Datatilsynets myndighetsområde (i juridisk fagterminologi benevnt som ”kompetanse”). Datatilsynet skal altså samtidig ivareta rollen som håndhever av en eksisterende personvernlovgivning og rollen som opinionsdanner.

Datatilsynet har i hovedsak følgende virkemidler til disposisjon til utøvelse av sin virksomhet:

- Saksbehandling
- Tilsyn- og annen kontrollvirksomhet
- Informasjonsvirksomhet
- Organisatoriske, tekniske og økonomiske virkemidler (5)

Tilsynsvirksomheten knyttes i hovedsak til forvaltningsrollen. Det samme gjelder den rene juridiske saksbehandlingen, for eksempel behandling av

⁴ NOU 1997:19 *Et bedre personvern – forslag til lov om behandling av personopplysninger*

⁵ *For eksempel deltakelse i råd og utvalg, utvikling av bransjenormer, personvernombudsordning, arbeid med personvern fremmende teknologi, illeggelse av overtredelsesgebyr mv*

klagesaker og konsesjonssøknader. Når det gjelder informasjonsvirksomheten knytter den seg naturligvis i betydelig større grad til utøvelsen av begge rollene. Datatilsynet veileder og informerer i forhold til eksisterende personvernlovgivning og Datatilsynets forvaltningspraksis. Samtidig benyttes informasjon som virkemiddel til å skape debatt og å påvirke opinionen. Tilsvarende benyttes avgivelse av høringsuttalelser og deltakelse i råd og utvalg til å gi vurderinger i forhold til eksisterende personvernlovgivning, men i stor grad også til å komme med innspill til spørsmål som ligger utenfor Datatilsynets formelle myndighetsområde.

Gjennom tilsynsvirksomhet og saksbehandling (dvs rollen som forvaltnings- og tilsynsorgan) tilegner Datatilsynet seg erfaring og kunnskap om hvordan personvern hensyn i praksis blir ivaretatt i ulike sektorer og bransjer. Denne kompetansen er av stor betydning for en god utøvelse av Datatilsynets ombudsrolle. Datatilsynet kan på denne måten basere sine synspunkter om hvordan personvernet bør ivaretas ut fra en erfaringsbasert kunnskap om hvordan personvernlovgivningen faktisk blir etterlevd ute i den praktiske hverdagen.

De to rollene utfyller altså hverandre. Gjennom tilsynsarbeid og behandling av over 11 000 henvendelser hvert år opparbeider Datatilsynet en unik kunnskap om personvernets kår i dagens Norge. Denne kunnskapen er helt avgjørende for å utøve ombudsfunksjonen på en god måte, det vil si bidra med faglig kunnskap og faglig basert debatt i det offentlige rom.

Går vi den motsatte veien – fra ombudsrollen til forvalterrollen blir det imidlertid mer utfordrende, slik Personvernkommissjonen og DIFI er inne på i sine respektive rapporter⁶. I saker hvor Datatilsynet i kraft av sin ombudsrolle har gått ut i det offentlige rom og hevdet en sterk vektlegging av personverninteressene, kan det naturlig nok stilles spørsmål ved hvorvidt vi ved en eventuell senere behandling av den aktuelle saken som forvaltningsorgan vil foreta en objektiv interesseavveining. Dette fordrer en særlig aktsomhet fra Datatilsynets

⁶ *NOU 2009:1 – Individ og integritet og Difi-rapport 2011:8 - Datatilsynet, mellom forvaltningsorgan og interessepolitisk aktør*

side. Datatilsynet skal derfor ha en meget høy bevissthet omkring våre ulike roller og være tydelige på når vi er i forvaltnings- og tilsynsrollen og når vi utøver ombudsrollen. Vi skal bidra med våre faglige argumenter i den offentlige debatt. Vi skal være en interessepolitisk aktør, men selvsagt ikke posisjonere oss slik at vi blir oppfattet å være partipolitiske.

Om kombinasjon av virkemidler

Den overordnede målsettingen for Datatilsynets virksomhet er enkelt sagt å bidra aktivt til å ivareta og utvikle et best mulig personvern for norske borgere. For å realisere denne målsettingen har Datatilsynet som nevnt ulike virkemidler til disposisjon. Ved å kombinere disse på en god måte oppnår vi en betydelig bedre effekt enn vi skulle satse på ett eller få virkemidler alene. Ved å analysere og planlegge ut fra informasjon vi henter inn fra blant annet tilsynsvirksomhet, saksbehandling og publikumskontakt kan Datatilsynet iverksette informasjonstiltak, ta initiativ til regelverksutvikling, eller benytte andre virkemidler. Her kan for eksempel ytterligere tilsynsvirksomhet, opplæringstiltak og initiativ til forskning, være aktuelle tiltak.

Ved å ha kontinuerlig oppmerksomhet på hvordan vi kan kombinere de innsatsfaktorene og virkemidlene vi til enhver tid har til rådighet, kan Datatilsynet oppnå et bedre personvern i samfunnet enn om vi satser på ett eller få virkemidler alene. For å få dette til er vi avhengig av å ha en gjennomarbeidet og godt forankret strategi og øvrige planer for vårt arbeide, hensiktsmessige rutiner og gode arbeidsverktøy. Fremfor alt er det å ha høyt kvalifiserte og motiverte medarbeidere en avgjørende suksessfaktor for at Datatilsynet skal kunne få til en god utnyttelse av våre ressurser og virkemidler.

Strategiske satsinger

1. Datatilsynet skal identifisere farer for personvernet og være synlig og tydelig i den offentlige debatt

Tiltak:

- Vi skal være ledende når det gjelder kunnskap og kompetanse om personvern. Dette skal vi gjøre gjennom eget analyse og utredningsarbeide, og ved å ha kontakt med forsknings- og utviklingsmiljøer
- Vi skal ha god produksjon av kronikker, leserinnlegg og fagartikler
- Vi skal identifisere saker som kan skape oppmerksomhet om personvernspørsmål, og ha høy tilgjengelighet for pressen
- Vi skal gjøre aktiv bruk av ombudsrollen og utfordre premisene for politikk og lovgivning som kan ha betydning for personvernet
- Vi skal vektlegge viktigheten av langsiktig tenkning omkring personvernutfordringer

2. Datatilsynet skal bidra til økt kunnskap og interesse for personvern og jobbe aktivt for at andre aktører legger vekt på personvern hensyn

Tiltak:

- Vi skal avklare vår egen strategi for personvernombudsordningen
- Vi skal videreutvikle datatilsynet.no til å bli den viktigste kanalen for veiledning og informasjon
- Vi skal fortsatt utvikle tiltak som setter den enkelte i stand til å ivareta eget personvern og respektere andres. Vi skal legge vekt på god veiledning
- Vi skal ha systematisk og jevnlig kontakt med sentrale aktører innen politikk, næringsliv, offentlig forvaltning og forsknings- og utviklingsmiljøer.
- Vi skal bidra til at det iverksettes forskningsprosjekter på personvernområdet . Vi skal også delta i referansegrupper

- Vi skal skape egne arenaer for å fremme debatt og dialog om personvern, for eksempel ved konferanser og pressefrokoster
- Vi skal promotere de fordeler virksomheter i offentlig og privat sektor oppnår ved å basere seg på prinsippet om innebygget personvern

3. Datatilsynets forvaltning og håndhevelse av regelverket skal kjennetegnes av god juridisk metode, tydelighet, proporsjonalitet, kvalitet og etterprøvbarehet

Tiltak:

- Vi skal håndheve regelverket gjennom risikobasert tilsynsvirksomhet og god kvalitet i behandlingen av forvaltningssaker
- Vi skal utvikle en god og enhetlig forvaltningspraksis som skal formidles aktivt til relevante miljøer og publikum
- Vi skal være bevisste og konsekvente på bruk av sanksjonsmidler
- Vi skal reagere raskt på alvorlige overtredelser som avdekkes. Resultatet av reaksjoner skal formidles til publikum og sakens parter
- Vi skal utarbeide kriterier for prioritering av forvaltningssaker

4. Datatilsynet skal være bevisst på riktig bruk av roller og balansert virkemiddelbruk

Tiltak:

- Vi skal ha fokus på hvordan Datatilsynet kan kombinere de ulike virkemidlene på en best mulig måte
- Vi skal ha oppmerksomhet på vår forvaltningsrolle og vår ombudsrolle og hvordan disse to rollene til enhver tid utøves
- Vi skal jobbe strategisk med utvikling av eget regelverk og ved behov ta initiativ til regelverkendringer på andre områder av betydning for personvernet
- Vi skal utarbeide en årlig virksomhetsplan med de viktigste prioriteringene og satsingene
- Vi skal ha fokus på effektiv saksbehandling og god saksflyt

5. Datatilsynet skal delta aktivt i internasjonalt samarbeid

Tiltak:

- Vi skal delta i de sentrale internasjonale fora som er viktig for å følge med på, og så langt mulig også påvirke agendaen og utviklingen i disse
- Vi skal bidra til utredninger for internasjonale fora
- Vi skal delta aktivt i standardiseringsarbeid
- Vi skal være en pådriver i det nordiske samarbeidet på personvernområdet
- Vi skal ha aktiv dialog med internasjonale aktører, gjerne i samarbeid andre personvernmyndigheter
- Vi skal gjøre vårt arbeid kjent internasjonalt

6. Datatilsynet skal ha høy kompetanse og motiverte medarbeidere

Tiltak:

- Vi skal legge til rette for at medarbeiderne i Datatilsynet får interessante og varierte arbeidsoppgaver og etablere en god tilbakemeldingskultur
- Vi skal stimulere til at medarbeidere i Datatilsynet deltar på kurs, konferanser og hospitering nasjonalt og internasjonalt
- Vi skal klargjøre roller og forventninger til alle medarbeidere i Datatilsynet
- Vi skal utarbeide kompetanseplaner både på individuelt nivå og for Datatilsynet som organisasjon
- Vi skal etablere et kompetansefond
- Vi skal gjennomgå saksflyt, oppgaveløsning, arbeidsverktøy, kunnskapsdeling og organisering
- Vi skal legge til rette for intern opplæring. Dette skal vi gjøre gjennom gode introduksjonsprogrammer for nyansatte, jevnlig faglig påfyll og kunnskapsdeling på tvers av faggruppene
- Vi skal synliggjøre og utvikle medarbeidernes kompetanse ved at de gis anledning til å representere Datatilsynet eksternt

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: postboks 8177 Dep
0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50