Organisering og ansvar etter personopplysningsloven i et forvaltningsorgan

Skrevet av:

Ivar Berg-Jacobsen

Laila Enerstvedt Fimreite

Frank Hermansen Grjotheim

Katrine Ore

Marius Raugstad

Innholdsfortegnelse

1.0 Innledning

Dette er en anonymisert utgave av den innleverte prosjektoppgaven i faget DRI3001 vårsemesteret 2009. I forhold til den originale teksten har vi her erstattet navnet på oppdragsgiver med "forvaltningsorganet". I tillegg har vi strøket over de ord, setninger mv. vi mener kan være med på å identifisere oppdragsgiver.
Det kapittelet som beskriver oppdragsgivers oppbygging og historie valgte vi å fjerne da teksten ville bli for usammenhengene ved bruk av samme anonymiseringsmetode som i resten av oppgaven.
Ved spørsmål knyttet til denne anonymiserte utgaven av oppgaven, kontakt veileder Dag Wiese Schartum.

1.1 Bakgrunn for valg av oppgave/tema

Sommeren 2008 gjennomførte to av gruppens medlemmer en personvernundersøkelse på oppdrag for Avdeling for forvaltningsinformatikk. Denne gikk i korte trekk ut på å kartlegge etterlevelsen av lov om behandling av personopplysninger (personopplysningsloven) i sentralforvaltningen.[1] På bakgrunn av denne undersøkelsen ville gruppens medlemmer gjøre en mer kvalitativ undersøkelse ved å se på hvordan et bestemt forvaltningsorgan gjennomfører kravene personopplysningsloven stiller til organisering i praksis. I samråd med veileder tok vi kontakt med et større forvaltningsorgan. Dette organet så vi på som interessant både på grunn av det store omfanget av personopplysninger som behandles og fordi større deler av behandlingen foregår elektronisk.

1.2 Avgrensning

Formålet med dette arbeidet er å finne en måte å praktisere personopplysningsloven på som kan være effektiv og praktisk gjennomførbar i et forvaltningsorgan. Vi skal i denne rapporten gå gjennom forvaltningsorganets indre struktur og legge vekt på hvordan de har organisert roller i forhold til personvernlovgivningen. Dette er roller/ansvarsområder som ikke alltid er åpenbare ut ifra lovens ordlyd. Hvordan man skal organisere seg vil være avhengig av en konkret vurdering i hvert enkelt tilfelle. Vår oppgave i denne sammenhengen vil være å sette oss inn i dagens organisering i

[1] URL: http://www.kunnskapsnettverk.no/C7/C1/Ressursnettverk%20for%20eforvaltni/Document%20Library/Personvern%20i%20sentralforvaltningen.pdf (lest 16.05.09)

forvaltningsorganet, og se loven med deres øyne. Til slutt vil vi se på om det kan være andre måter å organisere disse rollene på som vil være mer formålstjenlige og/eller i større grad samsvarer med lovgivningen basert på hva vi erfarer underveis. For å avgrense omfanget av oppgaven har vi hovedsakelig gjort to valg. For det første har vi valgt å fokusere på roller og funksjoner knyttet til behandlingsansvaret og sett på noen av de pliktene loven legger på behandlingsansvarlig, herunder internkontroll, informasjonssikkerhet og opplysningskvalitet. Siden forvaltningsorganet er en stor og kompleks organisasjon har vi for det andre valgt å fokusere på en av tre prosesser som utgangspunkt for vår drøfting. Denne prosessen er "hovedprosessen" i forbindelse med forvaltningsorganets virksomhet.

1.3 Tilnærming og metode

I denne rapporten har vi i hovedsak benyttet to former for kilder: tekster og intervjuer. Tekstene vi har benyttet er både fagbøker om elektronisk forvaltning og personopplysningsvern, offentlige utredninger, lover og informasjonsmateriell fra forvaltningsorganet. Tekstene utgjør mange forskjellige sjangre som krever forskjellige lesestrategier, og er lest på en slik måte at de belyser rapportens tema.

I tillegg til det skriftlige materialet har vi også benyttet intervjuer. Intervjuteknikken vi har benyttet er basert på det Macionis og Plummer omtaler som "a series of questions a researcher addresses personally to respondents".[2] Intervjuspørsmålene ble utarbeidet før vi gjennomførte intervjuene med ansatte i forvaltningsorganet. Totalt intervjuet gruppen 4 ansatte i forvaltningsorganet på forskjellige nivåer i organisasjonen. Forvaltningsorganet bestemte selv hvilke ansatte som skulle intervjues på bakgrunn av forespørsler fra gruppen. Gruppens ønske om å intervjue styreleder ble ikke etterkommet. Intervjuene fungerte som et viktig supplement til de tekstlige kildene vi har benyttet. De ga klare fortolkninger av det skriftlige materialet vi fikk utlevert under et av de første møtene vi hadde med forvaltningsorganet. I tillegg fikk vi et innblikk i hvordan forvaltningsorganet har tolket bestemmelsene i personopplysningsloven med tilhørende forskrift. I rapporten har vi behandlet intervjuene på en forskningsetisk måte ved å pseudonymisere informantene ved omtale. Intervjuene ble gjort tilgjengelig for informantene i tekstvariant. Alle fikk

[2] Macionis & Plummer (2005) s. 56

mulighet til å komme med kommentarer på våre skriftlige versjoner av intervjuene før de ble benyttet i rapporten. Opplysninger om forvaltningsorganets faktiske forhold er i stor grad basert på en samlet vurdering av fremlagt dokumentasjon, samt intervjuer av ansatte og ledelse. I tilfelle motstrid mellom informasjon fra informanter, har vi valgt å legge til grunn opplysninger fra de personer som er nærmest problemet i praksis. Der den skriftlige dokumentasjonen ikke samsvarer med opplysninger gitt i intervjuene, har vi lagt mest vekt på sistnevnte.

1.4 Om forvaltningsorganet (Unntatt offentlighet)

Grunnet taushetserklæring er hele dette kapittelet fjernet fra denne versjonen av rapporten.

2.0 Organisatoriske spørsmål ved etterlevelse av personopplysningsloven

Vi ønsker å starte dette avsnittet med å stadfeste at personopplysningsloven gjelder for dette forvaltningsorganet. Dette fremkommer av pol §§ 3 og 4 om saklig og geografisk virkeområde. Pol § 3 (saklig virkeområde) første ledd bokstav a presiserer at loven gjelder for de behandlinger av personopplysninger som helt eller delvis foretas med elektroniske hjelpemidler. Personopplysning blir i pol § 2 nr 1 definert som: "opplysninger og vurderinger som kan knyttes til en enkeltperson".[3] Hovedoppgaven til [redacted].[4] Vi kan derfor konstatere at forvaltningsorganet møter personopplysningslovens krav til saklig virkeområde. Videre tilsier pol § 4 første ledd (geografisk virkeområde) at loven gjelder dersom behandlingsansvarlig er etablert i Norge.

I og med at personopplysningsloven er en generell lov vil den dekke mange flere problemstillinger enn det vi har fokus på i denne sammenhengen. Vi vil derfor kun fokusere på de delene av loven som er relevante i forhold til vår problemstilling.

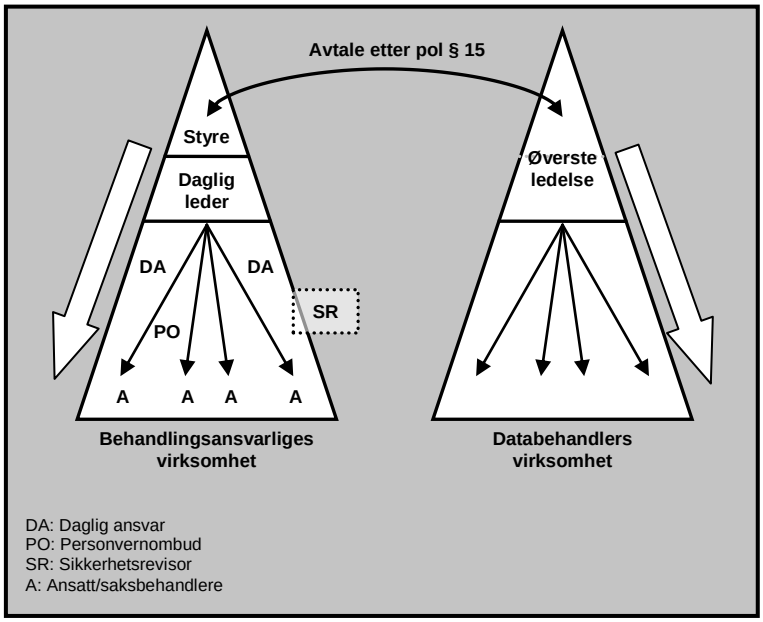
Formålet med personopplysningsloven er å påse at ingens personvern blir krenket gjennom behandling av personopplysninger, jf. pol § 1 første ledd. Ved tolkning av de ulike bestemmelsene i personopplysningsloven, vil formålsbestemmelsen kunne gi en viktig pekepinn på hvordan loven skal forstås. Den er med på å gi loven en fleksibilitet som gjør den i stand til å håndtere ulike endringer i den teknologiske utviklingen. Ved tvil om hvordan en bestemmelse skal forstås, kan formålsbestemmelsen si noe om hvordan den aktuelle problemstillingen bør løses.[5]

God organisering av ansvar er en viktig forutsetning for etterlevelse av personopplysningsloven på alle nivåer i en organisasjon. Dette vil være med på å

[3] Jf pol § 2 nr.1
[4] [redacted]
[5] Schartum og Bygrave (2004) s. 105

tydeliggjøre ansvars- og myndighetsforhold i den daglige driften til en institusjon som behandler personopplysninger. For å legge til rette for en organisering i tråd med lovens formål finner vi både i lov og forskrift en del organisatoriske roller. Noen av disse fremkommer eksplisitt, mens andre ligger mer implisitt i bestemmelsene. Enkelte av rollene fremstår ikke som krav, men bør med fordel vurderes implementert i organisasjonsstrukturen.

Loven setter en person eller en virksomhet ved en person som øverste ansvarlig for behandlingen av personopplysninger. I en del tilfeller kan det være vanskelig å klart definere hvem som har denne kompetansen da denne personen skal ha det endelige beslutningsansvaret. Loven legger videre opp til at denne personen har instruksjonsmyndighet. Med instruksjonsmyndighet menes den myndigheten en person innehar til å instruere underordnede i sin virksomhet.[6] Den med det endelige beslutningsansvaret kan også delegere kompetanse.



Figur 2 – Forhold mellom aktørene

Pyramiden til venstre i figur 2[7] illustrerer hvordan personopplysningsloven organiserer denne delegeringen. Øverst har vi den som vil ha det endelige beslutningsansvaret (her representert ved styret[8]). Vedkommende vil ha mulighet til å delegere instruksjonsmyndighet og kompetanse til den som har den daglige ledelsen

[6] Eckhoff og Smith (2003) s. 113
[7] Fritegning basert på figur av Schartum, Dag Wiese, første veiledningstime i DRI3001 våren 2009
[8] Det vil være styre v/styreleder

i virksomheten. Denne personen kan deretter delegere kompetansen til underordnede som vil få et daglig ansvar for å oppfylle de kravene den øverste lederen har etter personopplysningsloven. Deretter vil de ansatte/saksbehandlere bli instruert til gjennomføringen av ulike tiltak mv. Figuren viser også forholdet mellom behandlingsansvarlig og databehandler, og vi kan se at databehandlers øverste leder har muligheter for å delegere oppgaver og kompetanse innen egen virksomhet.

3.0 Behandlingsansvar

Det rettslige grunnlaget for behandlingsansvaret finner man i pol. § 2 nr. 4. Her blir den behandlingsansvarlig definert som "den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes". I utgangspunktet vil med andre ord den som har myndighet til å bestemme formål og hjelpemidler sannsynligvis også være behandlingsansvarlig. Denne personen eller organet vil besitte beslutnings- og instruksjonsmyndighet for behandlingen av personopplysninger. Med denne myndigheten kommer også muligheten til å delegere kompetanse og oppgaver knyttet til behandlingsansvaret lengre ned i organisasjonsstrukturen.

> Den behandlingsansvarlige kan imidlertid ikke fraskrive seg sitt "rettslige" behandlingsansvar ved delegeringen. Det er bare kompetansen som delegeres, ikke ansvaret.[9]

Dersom den behandlingsansvarlige lar avgjørelser om formål og hjelpemidler bli tatt på et lavere organisatorisk nivå, vil han altså fortsatt sitte med det rettslige ansvaret.[10]

Schartum og Bygrave skriver at "den behandlingsansvarlige er "*hovedpersonen"* i loven ved at en rekke plikter og rettigheter er knyttet til vedkommende"[11] (vår kursiv). Blant annet skal den behandlingsansvarlige påse at det foreligger et rettslig grunnlag for å behandle personopplysninger[12], og at det er fastsatt et formål for behandlingen av disse. Som vi kan se i pol § 11 første ledd bokstav b, d og e skal formålet være utrykkelig angitt og begrunnet. Videre kan vi lese at personopplysningene skal være relevante, dekkende, samt oppdaterte og nøyaktige. Behandlingsansvarlig skal også ha ansvar for informasjonssikkerheten og internkontroll i virksomheten, jf. pol §§ 13 første ledd og 14 første ledd. Lovens bestemmelse om informasjonssikkerhet gir imidlertid bare en overordnet beskrivelse av dette arbeidet, mens forskriftens kapittel 2 kommer med mer utfyllende krav.

[9] Coll og Lenth (2000) s. 37
[10] Coll og Lenth (2000) s. 37
[11] Schartum og Bygrave (2004) s. 124
[12] Jf pol §§ 8 og 9

Forvaltningsorganet oppfatter plasseringen av behandlingsansvaret entydig. I all den dokumentasjonen[13] vi har fått utlevert som omtaler behandlingsansvaret, legges dette til direktøren. Også under intervjurunden ble det bekreftet at forvaltningsorganet mener at direktøren har behandlingsansvaret.

Accenture, som er utviklere av forvaltningsorganet nye systemer, foreslo i forbindelse med moderniseringsprosessen en tredeling av behandlingsansvaret; overordnet ansvar, premissgiveransvar og utførende ansvar.[14] Dokumentasjonen forklarer det overordnede ansvaret som et mer helhetlig ansvar på virksomhetsnivå, og plasserer dette hos direktøren. Premissgiveransvaret, som legges til fagdirektøren, tillegges et litt mer spesifikt ansvar. Dette mener forvaltningsorganet ikke var hensiktsmessig i praksis. I et intervju[15] fikk vi vite at forvaltningsorganet skal gå helt bort fra "premissgivende behandlingsansvarlig". Samtidig understrekes det at begrepet "premissgivende" fremdeles vil bli brukt om de tre prosesseierne[16], men ikke som en del av behandlingsansvaret etter personopplysningsloven. Det utøvende ansvaret innebærer helt konkrete oppgaver. Heller ikke dette blir i dag sett på som en del av behandlingsansvaret etter personopplysningsloven. Informant A forklarer at det ansvaret som følger av den enkelte ansattes stilling tilsvarer det som i dokumentasjonen blir kalt utøvende behandlingsansvar. Med andre ord vil hver enkelt ansatt ha et personlig ansvar for det daglige arbeidet de utfører.

I utgangspunktet kan denne tredelingen være en fornuftig delegering av kompetanse og ansvar nedover i organisasjonen. Problemet slik vi ser det består derfor hovedsakelig ikke av selve inndelingen i nivåer, men av den potensielt forvirrende begrepsbruken. Det kan etter loven kun være én behandlingsansvarlig, men loven har andre roller som kan tilsvare det som her blir referert til som premissgivende og utøvende behandlingsansvar.

Vi finner imidlertid lite i dokumentasjon og intervju som beskriver noen diskusjon rundt plasseringen av behandlingsansvaret. Vi har ikke inntrykk av at noen annen

[13] [redacted]
[14] [redacted]
[15] Jf intervju B
[16] [redacted]

plassering har vært vurdert. Som et alternativ til dagens organisering med direktøren som behandlingsansvarlig finner vi det nødvendig å også se på styrets rolle i forvaltningsorganet.

Forholdet mellom de forskjelllige ledelsesnivåene i forvaltningsorganet har vært under stadig endring siden forvaltningsorganet ble opprettet.

> [redacted] er et ordinært forvaltningsorgan uten særskilte fullmakter. Virksomheten var opprinnelig en filial under [redacted], og forekomsten av både grunnfond og eget styre gjorde at [redacted] kunne betraktes som et selvstendig rettssubjekt. Styret for [redacted] hadde fra starten [redacted] meget vide fullmakter, blant annet til å fastsette samlet [redacted].[17]

I Ot.prp. [redacted] omtales forvaltningsorganet styre på denne måten:

> Etter gjeldende ordning for [redacted] er det styret som er det øverste organet for institusjonen. En av styrets viktigste oppgaver er å sørge for at institusjonen blir ledet og administrert på en så optimal måte som mulig.[18]

St.meld. nr. [redacted] drøfter hvorvidt forvaltningsorganet skal ha et styre på bakgrunn av andre offentlige utredninger.[19] Disse utredningene fremhever at forvaltningsorganer ikke bør ha styrer. St. meld [redacted] presiserer likevel at Regjeringen etter en samlet vurdering vil videreføre ordningen med et eget styre for forvaltningsorganet,[20] noe av grunnen til dette er at

> departementet har lagt opp til at nåværende styre skal ta aktivt del i moderniseringsarbeidet, slik at departementet i en viktig fase kan trekke på den kompetansen nåværende styre innehar.[21]

---

[17] URL: [redacted] s. 17 (lest 28.04.09)
[18] URL: [redacted] s. 41 (lest 11.05.09)
[19] Disse utredningene er St.meld.nr.35 ”Om statens forvaltnings- og personalpolitikk” og Rapport 2003:18 ”Styring med styrer”
[20] URL: [redacted] s. 18 (lest 28.04.09)
[21] URL: [redacted] s. 17 (lest 28.04.09)

I tillegg ble det sett på som verdifullt å ha [redacted] representert for å videreføre den gode dialogen mellom disse og myndighetene. Det er altså ikke gitt at styret i forvaltningsorganet vil være en del av organiseringen i fremtiden, men da de i skrivende stund har et styre må dette være vårt utgangspunkt i den videre drøftingen.

I Rapport 2003:18 "Styring med styrer" refereres det til forskning omkring styreroller. Det nevnes fem styrelederroller:

> Partneren – som den typiske komplementære rollen til direktør, Sjefen – som instruerer direktøren om hva denne skal gjøre, Mentoren – som fungerer som rådgiver og støttespiller, Konsulenten – som forventer å få henvendelser om å gi råd og Den fjerne – som oppfatter rollen som begrenset til å lede styremøtene.[22]

I den dokumentasjonen vi har hatt tilgang til finner vi flere ulike beskrivelser av styrelederrollen. I to arbeidsdokumenter[23] fra 2004 er styrelederen den eneste som ikke er nevnt i drøftelsen av behandlingsansvaret. Forholdet mellom rollene styreleder og direktør i forvaltningsorganet oppfatter informantene[24] å være av en slik art at styreleders aktiviteter i forvaltningsorganet begrenser seg til å lede styremøter, og kan derfor sies å være karakterisert av styrelederrollen "den fjerne". Vedtektene for forvaltningsorganet [25] tegner opp et annet bilde av styrets rolle. Her fremkommer det blant annet at styret er forvaltningsorganet øverste myndighet og "er ansvarlig for den samlede virksomhet". Vi mener at vedtektene beskriver en styreleder som skal ta en aktiv del i virksomheten (partneren/sjefen). Blant annet ser vi at styret skal "trekke opp linjene for [redacted] virksomhet", samt "følge opp virksomheten og påse at den foregår i samsvar med lover og forskrifter(…)" Slik vi ser det kan dette tale for at behandlingsansvaret må anses å ligge hos styret ved styreleder. Det vil i denne sammenhengen igjen være viktig å presisere at vedtektene er gitt av [redacted]. De resterende dokumentene vi bygger oppgaven på er utarbeidet av forvaltningsorganet internt. Dersom disse dokumentene ikke er i full overensstemmelse med vedtektene, må vedtektene bli tillagt størst vekt siden

[22] URL: www.difi.no/Rapport_2003-18_4qNk-.pdf.file s. 54 (lest 05.05.09)
[23] „[redacted]
[24] Jf informant A og B
[25] [redacted]

[redacted] har full organisasjonsmyndighet ovenfor forvaltningsorganet.

For at personopplysningsloven skal kunne etterleves på best mulig måte er det viktig at man tar formålsbestemmelsen med i betraktning ved tolkning av lovens bestemmelser, herunder bestemmelsene om organisering. Denne finner vi som nevnt i pol § 1. For å sikre at personvernet ikke blir krenket ved behandling av personopplysninger, kan det være formålstjenelig at man har behandlingsansvaret så nær den faktiske behandlingen av personopplysninger som mulig. Slik vi forstår informantene vi har intervjuet og dokumentasjonen fra forvaltningsorganet, har styret i forvaltningsorganet en perifer rolle, og dermed ikke kontroll med det daglige arbeidet. Isolert sett kan formålsbestemmelsen derfor tale for at man legger behandlingsansvaret hos direktøren. Det vil være administrasjonen i forvaltningsorganet ved direktøren som forbereder sakene som skal opp til behandling i styret. På denne måten vil direktøren kunne være med å utforme og opplyse de sakene styret skal ta seg av. For eksempel vil administrasjonen i forvaltningsorganet kunne foreslå hvem som skal inneha ulike posisjoner i organisasjonen for å ivareta kravene etter personopplysningsloven. Imidlertid vil styret så ut fra egne vurderinger enten godta eller ikke godta forslagene fra administrasjonen.

For å få en indikasjon på hvem som er organisasjonens behandlingsansvarlig må man som nevnt se på hvem som definerer formålet og hvilke hjelpemidler som skal benyttes ved behandlingen av personopplysninger. I tilfellet til forvaltningsorganet er formålet satt gjennom lov, og det eneste behandlingsansvarlig kan råde over er hjelpemidler. forvaltningsorganet interne saksbehandlingssystem ([redacted]) er et eksempel på et slikt hjelpemiddel. I den pågående moderniseringsprosessen er endringer av [redacted] en stor del av arbeidet. Prinsipielle beslutninger som angår utforming av [redacted] vil trolig ligge hos behandlingsansvarlig. Informant A opplyser at prinsipielle spørsmål om f. eks penger og sikkerhet blir tatt av direktøren. I tillegg kommer det frem at direktøren står fritt til å for eksempel velge databehandlere. Denne fremstillingen gir inntrykket av at behandlingsansvaret kan ligge hos direktøren.

På den andre siden er det, slik vi tolker vedtektene fra departementet, lagt opp til en vesentlig mer aktiv deltagelse fra styret. I St.meld. nr. [redacted] blir det beskrevet at styret skal ta en aktiv del i moderniseringsprosessen. Etter vanlig organisering med styrer er det naturlig at de tar del i den daglige driften i større grad enn opplysningene fra forvaltningsorganet kan tyde på. Styret vil vanligvis få en rolle hvor de har kontroll på virksomheten og tar med seg de deler av administrasjonen de ønsker for å oppnå sine mål. Det vil med andre ord ikke være noe i veien for at organiseringen kan fungere noenlunde slik det er i dag. Forskjellen blir at man flytter det formelle ansvaret og gir øverste organ en mer aktiv rolle i arbeidet med etterlevelse av personopplysningsloven. Dette mener vi i større grad enn dagens ordning samsvarer med de signaler som er gitt fra departementet, jf. vedtektene. I tillegg vil et mer aktivt styre kunne få nærmere innblikk i behandlingen av personopplysninger. På denne måten vil de bedre kunne fylle sin rolle som eventuell behandlingsansvarlig i tråd med personopplysningslovens formålsbestemmelse. Det vil være ønskelig å plassere behandlingsansvaret så nær behandlingen som mulig. Det vil likevel være uheldig om behandlingsansvarlig da har en overordnet med myndighet til å overprøve behandlingsansvarliges avgjørelser. En årsak til at det kan være vanskelig å definere hvem som har det endelige behandlingsansvaret er beskrevet i Schartum og Bygrave. De sier at det vil

> være meningsløst å tillegge behandlingsansvar til en person eller virksomhet som *bare* har bestemmelsesrett med hensyn til formål og hjelpemidler. Imidlertid kan slik bestemmelsesrett være en indikasjon på rett til å bestemme også over de mange andre forhold som loven regulerer.[26]

I vurderingen av hvem som skal ha behandlingsansvaret, kan det derfor være hensiktsmessig å ta i bruk noen ”hjelpestørrelser”. En av disse kan være hvem som har søksmålskompetanse ved brudd på personopplysningsloven. I faglitteraturen er det en del oppfatninger rundt straffeansvaret i pol § 48, som sier at ”*den* som forsettelig eller grovt uaktsomt…” (vår kursiv) kan straffes for brudd på de bestemmelser som listes opp i denne paragrafen. Dette gjelder kun brudd på konkrete bestemmelser som gir lite rom for tolkninger, jf. legalitetsprinsippet. Det kan

[26] Schartum og Bygrave (2006) s. 29

være tvil om hvem loven henviser til med "den". Schartum og Bygrave mener i denne forbindelse at

> spørsmålet er om (…) enkeltpersoner skal være hjemfallen til straff, eller om straffeansvaret skal ligge på den person som er den øverste lederen for den behandlingsansvarlige virksomheten.[27]

Coll og Lenth argumenterer for at det vil være den behandlingsansvarlige som har det strafferettslige ansvaret utad for at personopplysninger behandles på lovlig vis, og vil derfor besitte søksmålskompetanse ved eventuelle søksmål.[28] Dette understrekes også av Datatilsynet som sier at "Den behandlingsansvarlige må derfor være en som har søksmålskompetanse/sivilprosessuell partsevne".[29] Vi oppfatter dette som hensiktsmessig fordi det vil være den behandlingsansvarlige som etter loven har et overordnet ansvar for at loven følges. Også Schartum og Bygrave mener det kan "oppfattes som for tilfeldig og urettferdig om den øverste ledelsen kan fordele straffeansvaret gjennom sin arbeidsorganisering".[30] I forlengelsen av dette mener de at straffesanksjonen bør ligge hos behandlingsansvarliges øverste leder. Slik dagens ordning i forvaltningsorganet er med direktøren som behandlingsansvarlig, ville direktøren kunne pådra seg straffeansvar for beslutninger tatt av styret.

Datatilsynet bemerker også i sin årsrapport fra 2004 at ansvaret for behandlingen av personopplysninger i mange tilfeller delegeres rundt i organisasjonen og sier:

> Ingen tilsynsorganer forventer at virksomhetens øverste leder selv skal gjennomføre de pålagte pliktene. Den ansvarlige skal imidlertid sørge for å utløse handling. Ofte delegeres store deler av arbeidet med tilpasning til regelverket til mellomledere i virksomheten[31]

[27] Schartum og Bygrave (2006) s. 40
[28] Coll og Lenth (2000) s. 33
[29] URL: http://www.datatilsynet.no/upload/Dokumenter/veiledere/forskningsinfo_del_ii_1_0.pdf s. 5 (lest 07.05.09)
[30] Schartum og Bygrave (2006) s. 40
[31] URL: http://www.datatilsynet.no/upload/Dokumenter/publikasjoner/aarsmeld/Datatilsynet_manus_aarsm2004.pdf s. 23-24 (lest 10.05.09)

Videre kommenterer Datatilsynet fordeling og delegering av behandlingsansvar på denne måten: ”Dette kan være både en hensiktsmessig og riktig strategi, men det fritar imidlertid ikke den øverste ledelse for sitt ansvar og plikt til oppfølging”.[32]

Det er to roller som er nært knyttet opp til behandlingsansvarlige sin virksomhet; daglig leder og daglig ansvarlig.[33] Disse fremkommer i større eller mindre grad eksplisitt av lov med forskrift.[34] For det første har vi en daglig leder, dette vil normalt være den øverste operative lederen.[35] Etter pofs § 2-3, første ledd, kommer det fram at den personen som er ansvarlig for virksomhetens daglige ledelse, også har ansvaret for å følge informasjonssikkerhetsbestemmelsene i forskriftens kapittel 2. Disse bestemmelsene vil imidlertid være for omfattende til at vi går spesifikt inn på hver enkelt i vår sammenheng. Schartum skriver at ”daglig leder av virksomheten (…) betegner posisjonen som for eksempel direktør, administrerende direktør mv…”.[36] I forvaltningsorganets dokumentasjon og i intervju med informant A kom det frem at direktøren har full beslutningsmyndighet. Derfor finner vi det naturlig å plassere rollen som daglig leder hos direktøren.[37]

I pol § 32 første ledd bokstav c kommer det frem at meldingen for behandlingen som sendes til Datatilsynet skal inneholde opplysninger om hvem som har det daglige ansvaret for påse at den behandlingsansvarliges rettslige forpliktelser realiseres. I flere tilfeller vil behandlingsansvarlig være et kollegialt organ. Derfor pålegger loven at det også skal være minst en person som er daglig ansvarlig for at lovens krav blir fulgt opp.[38] Dette vil gjerne være en person som er ”nærmere der det skjer”. Det kan i mange tilfeller være ulike personer med dette ansvaret dersom det blir foretatt flere ulike meldepliktige behandlinger. Imidlertid er det viktig å passe på at det ikke blir så mange daglige ansvarlige at ansvaret blir pulverisert.[39]

---

[32] URL: http://www.datatilsynet.no/upload/Dokumenter/publikasjoner/aarsmeld/Datatilsynet_manus_aarsm2004.pdf s. 24 (lest 15.05.09)
[33] Schartum, og Bygrave (2006) s. 28
[34] Schartum, og Jansen (2005) s. 109
[35] Schartum, og Bygrave (2006) s. 34
[36] Schartum, og Jansen (2005) s. 112
[37] Jf intervju A
[38] Schartum, og Jansen (2005) s. 112
[39] Schartum og Bygrave (2006) s. 34

I forvaltningsorganets meldeskjema til Datatilsynet[40]. er rollen som daglig ansvarlig lagt til direktøren. Vi mener det kunne vært fordelaktig om dette ansvaret ble flyttet lenger ned i organisasjonen, gjerne fordelt på de ulike underdirektørene. Disse vil være mer i kontakt med den daglige behandlingen, og derfor ha et mer praktisk grunnlag for å kunne tilfredsstille lovens krav. Det er her viktig å understreke at det er den med det daglige ansvaret som har det løpende ansvaret for at jobben blir gjort. Ofte har denne personen medarbeidere under seg som utfører arbeid på instruks. Imidlertid vil ikke den daglige ansvarlige kunne fraskrive seg sin delegerte kompetanse, han kan kun instruere underliggende medarbeidere til å utføre de plikter og rettigheter daglig ansvarlig har etter personopplysningsloven med forskrift.

I små organisasjoner vil både behandlingsansvarlig, daglig ansvarlig og daglig leder kunne ligge hos en og samme person. Denne organiseringen er imidlertid uhensiktsmessig i større og mer komplekse organisasjoner.[41] Blant annet kan dette virke hemmende på den daglige driften ved at det kan medføre en for stor arbeidsmengde for én person å håndtere. Også dette kan tale for å legge det daglige ansvaret lenger ned i organisasjonen.

Slik vi ser det, vil det være mest hensiktsmessig å la styret ved styreleder ha rollen som behandlingsansvarlig. I tillegg mener vi at rollen som daglig leder passer godt inn under direktørens ansvarsområde. Når det gjelder rollen som daglig ansvarlig mener vi som nevnt ovenfor at denne bør delegeres til de respektive underdirektørene.

Dersom den behandlingsansvarlige vil kan denne etter personopplysningsforskriften bestemme å ansette et personvernombud. Dette er en valgfri ordning, og det er ulike oppfatninger om hva en slik rolle kan tilføre virksomheten. Før behandling av personopplysninger iverksettes, er den med det endelige beslutningsansvaret ansvarlig for at Datatilsynet er gitt melding, jf. pol § 31, første ledd. Denne meldingen skal sendes Datatilsynet senest 30 dager før behandlingen starter, jf. § 31 annet ledd. En av "fordelene" med et personvernombud er imidlertid at man kan omgå denne meldeplikten. I henhold til pof § 7-12, så kan man velge å ansette et uavhengig

[40] URL: [redacted] (lest 06.05.09)
[41] Schartum (2005) s. 110

personvernombud på samtykke fra Datatilsynet, og dermed omgås meldeplikten. Dette ombudet har som oppgave å tilse at organisasjonen følger personopplysningsloven med forskrift, samt føre oversikt over de opplysninger som er nevnt i pol § 32 – om meldingens innhold. Dersom denne ordningen ikke er tilstrekkelig uavhengig, så kan imidlertid Datatilsynet trekke samtykket tilbake.[42] Hva som anses som tilstrekkelig uavhengig kan være noe uklart.
En viktig side av denne uavhengigheten kan være at personvernombudet ved alvorlige brudd på bestemmelser i personopplysningsloven skal varsle, både Datatilsynet samt sin øverste overordnede. Det vil her være viktig at personvernombudet ikke lar seg binde av en slik lojalitet ovenfor arbeidsgiver at ombudet ikke varsler Datatilsynet. Imidlertid er det i praksis ombudets arbeidsgiver som setter rammene for hvor tett dialogen med Datatilsynet skal være.[43]

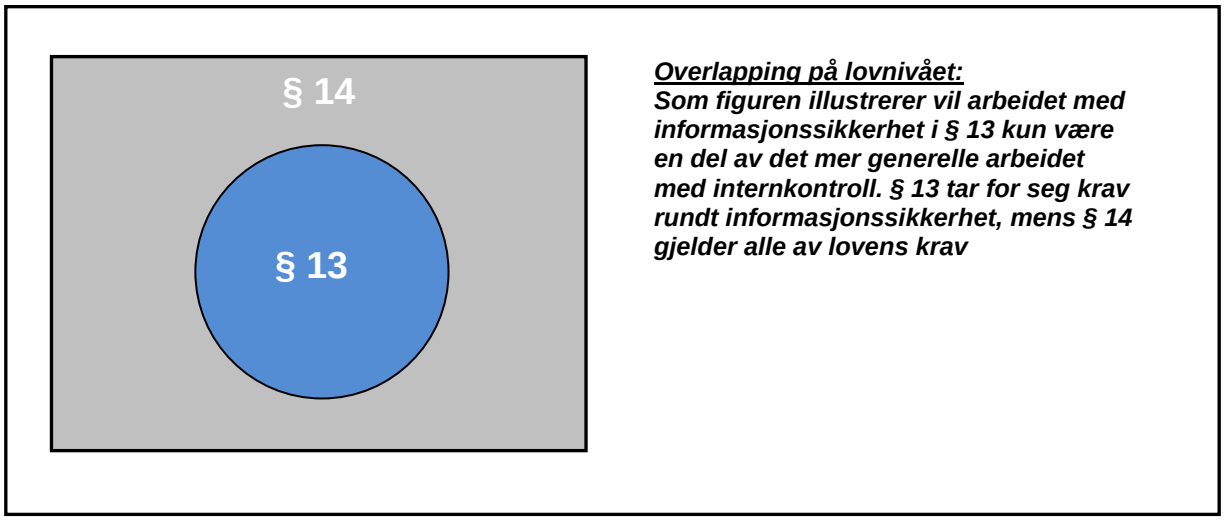
På direkte spørsmål opplyser informant A i forvaltningsorganet at de bevisst har valgt å ikke ha et personvernombud. Dette begrunnes ut fra deres filosofi om at enhver medarbeider skal føle et personlig ansvar for personopplysningsvernet. Ved opprettelse av personvernombud fryktes det en ansvarsfraskrivelse fra den enkelte medarbeider. Vi ser de umiddelbare fordelene bak denne filosofien, og det er veldig viktig at de som daglig behandler personopplysninger faktisk har en bevissthet rundt personopplysningsvern. Men innføring av et personvernombud i virksomheten trenger nødvendigvis ikke bety en ansvarsfraskrivelse. Ved opprettelse av et personvernombud vil man få et fast knutepunkt i virksomheten man kan henvende seg til ved eventuelle problemstillinger som måtte oppstå. Man kan altså fremdeles opprettholde et høyt individuelt kompetansenivå rundt personopplysningsvern, samtidig som man får en ”ekspert” å gå til ved vanskelige problemstillinger.

[42] Schartum (2005) s. 114
[43] Schartum (2005) s. 113-114

4.0 Ansvar for internkontroll

Som vi nevnte i kapittel 2 har behandlingsansvarlig ansvaret for internkontroll og informasjonssikkerhet i virksomheten. Vi har valgt å skrive om informasjonssikkerhet og internkontroll hver for seg. Dette skyldes at selv om de to bestemmelsene i stor grad overlapper hverandre på lovnivå, er de forskjellige på forskriftsnivå. I forskriften blir informasjonssikkerheten detaljert beskrevet, mens internkontrollen har få bestemmelser.

Paragrafene 13 og 14 i personopplysningsloven skal sammen "ivareta opplysningskvaliteten på et organisatorisk og teknisk nivå".[44]



Figur 3 – Forhold mellom internkontroll og informasjonssikkerhet i pol

Pol § 14 første ledd plasserer ansvaret for at det blir etablert et internkontrollsystem hos den behandlingsansvarlige i virksomheten. Coll og Lenth forklarer bestemmelsen om internkontroll, pol § 14, på denne måten:

> det skal etableres rutiner for å sikre at de kravene lov og forskrift stiller til behandling av personopplysninger (..) blir overholdt. Det skal særlig legges vekt på å sikre at opplysningenes kvalitet er god nok i forhold til formålet med behandlingen[45]

[44] Coll og Lenth (2000) s. 52
[45] Coll og Lenth (2000) s. 110

Disse rutinene skal videre dokumenteres og denne dokumentasjonen skal være tilgjengelig for den behandlingsansvarlige, databehandler samt Datatilsynet og Personvernnemnda, jf. pol § 14, annet ledd. Coll og Lenth påpeker at

> Ettersom den behandlingsansvarlige må dokumentere hvilke tiltak som gjennomføres, vil dette føre til en bevisstgjøring i forhold til behandling og regulering av personopplysninger.[46]

Denne dokumentasjonen kan altså bidra til større innsikt i blant annet personopplysningsloven og forskriftens krav til behandlingen av personopplysninger.

Lovgivers intensjon med reglene om internkontroll i personopplysningsloven med forskrift er å fremheve det ansvaret som den behandlingsansvarlige i en virksomhet har for å etterfølge disse bestemmelsene.[47] Pol § 14 første ledd fastsetter at

> Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.[48]

Ut fra lovens ordlyd er det særlig verdt å merke seg "nødvendig". Coll og Leth vurderer dette til at det skal gjennomføres en nødvendighetsvurdering på hvilke tiltak som må gjennomføres for oppfyllelse av lovens krav til behandling av personopplysninger. De fastslår videre at disse nødvendighetsvurderingene er et utgangspunkt for "(…)valget av organisatoriske og tekniske tiltak".[49] Det er i utgangspunktet den behandlingsansvarlige selv som avgjør hva som skal regnes som "nødvendig" for å gjennomføre de rettslige kravene til behandlingen.[50] Schartum skriver at "(…)det foreligger ingen plikt til å treffe tiltak på alle punkter".[51] Når en virksomhet etablerer en ny behandling av personopplysninger[52] må de

[46] Coll og Lenth (2000) s. 116
[47] Coll og Lenth (2000) s. 116
[48] Jf. pol § 14 første ledd
[49] Coll og Lenth (2000) s. 116
[50] URL: http://websir.lovdata.no/cgi-lex/wifthy4?LOV-2000-04-14-31-p14#map9 (lest 15.05.09)
[51] URL: http://websir.lovdata.no/cgi-lex/wifthy4?LOV-2000-04-14-31-p14#map9 (lest 15.05.09)
[52] Behandling av personopplysninger defineres i pol § 2 nr 2

analysere en rutine for internkontroll som ”(…) innebærer at den nye behandlingen blir vurdert i forhold til lovens (m.v.) krav”[53]

Datatilsynet presiser også at det er et ledelsesansvar å etablere internkontrollrutiner i virksomheten. ”Ledelsen har et spesielt ansvar for å (…) klarlegge intern organisering og ikke minst tydelig identifisere ansvar og myndighet” .[54] Internkontrollen skal være med på å oppnå en bedre informasjonssikkerhet og informasjonskvalitet. Som vi tidligere har vært inne på kan imidlertid den behandlingsansvarlige delegere og instruere denne kompetansen i tråd med den alminnelige organisasjons- og instruksjonsmyndigheten.

Den dokumentasjonen vi har fått fra forvaltningsorganet tegner opp et overordnet bilde rundt organiseringen av internkontroll. Ansvaret for at dette skjer på alle nivåer i organisasjonen er delegert fra behandlingsansvarlig ned til hver enkelt leder.[55] I et delprosjekt til [redacted]-prosjektet[56], ”[redacted]”, beskrives en overordnet organisering av arbeidet med internkontroll. Her beskrives ansvarsområdet for blant annet internkontroll for ulike nøkkelpersoner[57] i forvaltningsorganet. Det gis ikke noe detaljert fremstilling av innholdet i dette ansvaret, men heller en pekepinn på hvordan dette arbeidet skal organiseres. [redacted] får her et ansvar for et tilfredsstillende rammeverk for internkontroll i saksbehandlingen, mens [redacted] og [redacted] skal sørge for tilfredsstillende internkontroll innenfor sine respektive områder. [redacted] skal gjennomføre internkontroll etter gitte retningslinjer. Det som er nedfelt i denne dokumentasjonen er et godt utgangspunkt for videre arbeid med internkontroll, men gjennom intervjuene fikk vi inntykk av at dette per i dag ikke er realisert fullt ut i praksis.

I dokumentet ”[redacted]” kommer det frem at ”(…)ansatte skal ha riktig kompetanse til å løse tildelte oppgaver og til å forstå og etterleve mål,

[53] URL: http://websir.lovdata.no/cgi-lex/wifthy4?LOV-2000-04-14-31-p14#map9 (lest 15.05.09)
[54] URL: http://www.datatilsynet.no/upload/Dokumenter/internkontrollfiler/internkontroll08102001.pdf s. 1 (lest 07.05.09)
[55] Direktørens styringssignaler (2008) s. 7
[56] [redacted]-prosjektet er et fornyelsesprogram som gjennomføres i forvaltningsorganet, og består av flere mindre prosjekter.
[57] [redacted]

resultatkrav og krav til intern kontroll".[58] Forvaltningsorganet konstaterer at "Intern kontroll skal tilpasses risiko og vesentlighet".[59] Det skal blant annet gjennomføres risikovurderinger for viktige arbeidsprosesser og før implementering av endringer av teknisk og organisatorisk art, og disse skal dokumenteres. Basert på tilgjengelig dokumentasjon kan dette oppfattes som litt vagt, da det ikke fremkommer veldig detaljerte rutiner omkring internkontroll.[60] Informant C påpeker imidlertid at det er etablert et internkontrollsystem i forvaltningsorganet basert på [redacted]-prosjektet fra 2007.

Forvaltningsorganet har også et kvalitetsutvalg som er en del av det samlede internkontrollsystemet. Dette ble opprettet som et av resultatene fra [redacted]-prosjektet i 2007. Utvalget ble opprettet fra 1. januar 2008.[61] Slik vi forstår det er dette en gruppe som på årlig basis utfører stikkprøver som både sjekker generell datakvalitet og at saksbehandlingen blir korrekt utført. Utvalget går også gjennom hele regelverket og foretar risikoanalyser. Disse tiltakene danner grunnlaget for rapporter som i tillegg til å beskrive resultater også inneholder forslag til endringer. Rapportene blir så sendt til direktøren, for deretter å bli behandlet av fagavdelingen.[62]

Informant A mener at internkontroll er et overflødig begrep, og at dette på individnivå i stor grad er basert på sunn fornuft og gode skjønnsvurderinger. Dette vil gjøre etterkontroll unødvendig. Vi ser muligheten for at dette kan bidra til økt ansvarsbevissthet i organisasjonen, med dette fratar ikke behandlingsansvarlig de krav til rutiner og dokumentasjon som fremkommer av § 14 i pol.

Forskriftens kapittel 3 om internkontroll legger ingen føringer på hvorledes organiseringen av internkontroll skal foregå. Altså kan man formodentlig tolke dette til å bety at den person som innehar behandlingsansvaret kan delegere og instruere plikter og rettigheter som han selv vil, vedrørende organisering av internkontroll nedover i organisasjonen. Hvis denne organiseringen gjør at personopplysninger i virksomheten behandles i overensstemmelse med grunnleggende personvernhensyn

---

58 [redacted] s. 7
59 [redacted] s. 7
60 Jf intervju D
61 [redacted]-prosjekt [redacted] (2007) s. 29
62 Jf intervju D

mv. (jf. pol § 1 annet ledd) kan det sies at det er en formålstjenelig måte å organisere ansvar på. Vi ser en slik organisering som hensiktsmessig da det neppe er å forvente at den behandlingsansvarlige selv aktivt skal delta i gjennomføring av internkontrollrutiner. Imidlertid vil han alltid besitte ansvaret for at slike tiltak iverksettes og oppfølges, jf. pol § 14 første ledd. I forvaltningsorganets tilfelle kan det gjerne være fruktbart å delegere kompetansen rundt dette arbeidet til personer som har en nær kontakt med de ulike prosessene. Dette kan f eks være de forskjellige [redacted].

5.0 Ansvar for informasjonssikkerhet

Som allerede beskrevet i kapittel 2.0, er formålet med loven å hindre at den enkeltes personvern blir krenket gjennom behandling av personopplysninger. For å oppnå dette har loven bestemmelser som stiller krav til fokus på blant annet informasjonssikkerhet.

Pol § 13 tar for seg informasjonssikkerhet og "(…) regulerer særskilt sikring av enkelte sentrale sider ved behandlingen av personopplysninger".[63] Behandlingsansvarlig plikter å sørge for et akseptabelt nivå av informasjonssikkerhet gjennom forberedte og systematiske tiltak med tanke på ulike aspekt ved behandlingen av personopplysninger, jf pol § 13 første ledd. Coll og Lenth forklarer hvordan man avgjør hva som er et akseptabelt nivå:

> Hvilke organisatoriske og tekniske tiltak som må iverksettes for å oppfylle lovens krav, vil derfor bero på en konkret vurdering, hvor det legges vekt på hvilke personverntrusler opplysningene er utsatt for. Betydelige trusler vil kreve strengere sikkerhetstiltak før kravene er oppfylt.[64]

I henhold til pol § 13 annet ledd skal tiltakene også dokumenteres. Disse sikringstiltakene er nærmere beskrevet i pofs kapittel 2 om informasjonssikkerhet. Det skal sikres at ingen får uautorisert innsyn, at personopplysninger ikke endres av uvedkommende og at personopplysningene er tilgjengelige når det er nødvendig.[65] Som beskrevet under kapittel 3.0 er det den som fyller rollen som daglig leder som er ansvarlig for at bestemmelsene i pofs kapittel 2 *gjennomføres*, jf. pof § 2-3 første ledd. Imidlertid er det viktig å påpeke at lovens bestemmelse om informasjonssikkerhet sier at det er den behandlingsansvarlige som skal *sørge for* at informasjonssikkerheten i virksomheten er tilfredsstillende, jf. pol § 13 første ledd.

I pof § 2-5, kommer det frem at det jevnlig skal gjennomføres sikkerhetsrevisjon av informasjonssystemene der organisering, sikkerhetstiltak mv. skal vurderes.

---

[63] URL: http://websir.lovdata.no/cgi-lex/wifthy4?LOV-2000-04-14-31-p14#map9 (lest 15.05.09)
[64] Coll og Lenth (2000) s. 111-112
[65] Coll og Lenth (2000) s. 110

Det står verken her eller i loven eksplisitt nevnt at det skal opprettes en egen rolle med ansvaret for sikkerhetsrevideringen etter pofs § 2-5. Men som Schartum og Bygrave påpeker så innebærer forskriften "trolig bare et krav om intern sikkerhetsrevisjon, dvs. slik at den personen som leder et slikt arbeid (sikkerhetsrevisor) er del av den behandlingsansvarliges organisasjon".[66] På bakgrunn av dette tolker vi denne bestemmelsen dit hen at det kan være en løsning å oppnevne en bestemt person med særskilt ansvar for revisjonen.

I forvaltningsorganet er det ingen person med bestemt ansvar for at det gjennomføres sikkerhetsrevisjon. Slik det kommer fram av gjennomførte intervjuer av ansatte i forvaltningsorganet blir det heller ikke foretatt noen jevnlig sikkerhetsrevisjon av informasjonssystemene annet enn testing ved utvikling og implementering av nye systemer. Det er likevel viktig å understreke at det ofte blir foretatt endringer i systemene, noe som også medfører "jevnlig" testing. Dette blir utført av IT-avdelingen.[67] I følge informant B er det et mål å gjøre utviklingsarbeid så systematisk at direkte revisjon er unødvendig. Det kommer imidlertid frem gjennom intervju med Informant A at det snarlig kommer til å bli ansatt en person som skal ha et særskilt ansvar for IT-sikkerhet. Vi ser på dette som et positivt tiltak.

Alle informantene opplyser at forvaltningsorganet har oppnevnt et kvalitetsutvalg. Det understrekes av informant D at kvalitetsutvalget ikke er ansvarlig for informasjonssikkerheten, men kun er en del av internkontrollsystemet. Slik kvalitetsutvalget arbeider, kan dette fremstå som planlagte og systematiske rutiner for det generelle sikkerhets- og kvalitetsarbeidet, selv om vår mening er at disse kontrollene muligens bør gjennomføres på hyppigere basis. Vi tolker den funksjonen som kvalitetsutvalget skal besitte som en måte å fylle rollen som ansvarlig for sikkerhetsrevisjon på. Det vil være nærliggende å tenke at personen som leder dette utvalget, bør være sikkerhetsrevisor. Vi mener videre at det ligger et stort potensial i dette uvalget, men dette forutsetter at de enkelte medlemmer får avsatt nok tid til å følge opp dette arbeidet på en tilfredsstillende måte.

[66] Schartum og Bygrave (2006) s. 35
[67] Jf intervju A

Personell, eller saksbehandlere som jobber hos den behandlingsansvarlige må være autorisert for å benytte informasjonssystemet, og dette skal kun brukes til utførelse av fastsatte oppgaver, jf. pof § 2-8. I forvaltningsorganet er dette organisert gjennom et graderingssystem som går fra 2 til 8, der den med graderingsnivå 8 har alle rettigheter. Imidlertid er det slik at opplysninger om kunder som også er ansatt i forvaltningsorganet og kunder med hemmelig adresse mv. vil bli sperret for vanlige saksbehandlere. Dette er uavhengig av graderingsnivå, og behandles normalt av den enkelte [redacted].[68] Saksbehandler har også et selvstendig ansvar for å følge de rutiner forvaltningsorganet har. Eksempel på dette kan være at man er sikker på hvem man snakker med ved telefonisk publikumskontakt angående innsyn eller endringer av personopplysninger.[69] I dokumentet "Sikkerhet og beredskap i [redacted]" tydeliggjøres det blant annet at "Ansattes sikkerhetsbrudd behandles som tjenestefeil, og kan i alvorlige tilfeller få konsekvenser for ansettelsesforholdet".[70] I henhold til pofs § 2-9, er medarbeiderne hos behandlingsansvarlig bundet av taushetsplikt, og dette er meget viktig for å bevare konfidensialiteten og privatlivet til den enkelte borger som benytter seg av tjenester fra organet. Dette blir i forvaltningsorganet etterlevd ved at ansatte må undertegne taushetserklæringer.[71] Det bemerkes imidlertid at de ansatte får kurs i forvaltningslovens bestemmelser vedrørende dette og ikke i regler om informasjonssikkerhet etter personopplysningloven.[72]

Lesetilgang og innsyn i forvaltningsorganets personopplysninger reguleres som oftest av at de ansatte må logge seg på. Dette er en naturlig del av virksomhetens sikkerhetsarbeid med personopplysninger. I dokumentasjonen som beskriver forvaltningsorganet sikkerhetsarbeid sies det at "Brukergrupper defineres av systemeier ut fra tjenstlig behov. Alle brukere kan se og spørre om all informasjon i [redacted]. Men de får ikke endre og godkjenne."[73] Det er forventet at alle ansatte forstår sitt ansvar i forhold til de personopplysningene de får innsyn i, og samtlige ansatte har undertegnet taushetserklæring. I tillegg har forvaltningsorganet skallsikring. I denne sammenhengen innebærer skallsikring blant annet fysisk adgangskontroll til lokalene

[68] Jf intervju B og C
[69] Jf intervju D
[70] [redacted] s. 2
[71] Jf intervju B
[72] Jf intervju D
[73] [redacted]

da forvaltningsorganet fremdeles besitter papirarkiver på åpne hyller. Vi anser måten forvaltningsorganet har organisert dette på som tilfredsstillende i forhold til uvedkommendes fysiske tilgang til taushetsbelagt informasjon.

I dokumentet "[redacted]" legges det vekt på at "alle medarbeidere bidrar som avtalt, og at alle tar sin del av ansvaret for de oppgaver vi skal utføre."[74] Dette blir også fremhevet av informant A.

Ingen av de skriftlige dokumentene sier noe om forholdet mellom logging av ansattes lesetilgang og tilgangskontroll. Ved saksbehandling blir alle endringer midlertidig loggført, men idet det blir fattet et endelig vedtak, er det den som gjør dette som gir saken en signatur. Ytterligere endringer i etterkant vil bli loggført. Kikking på kundemapper blir derimot ikke loggført i systemet, og enhver som har systemtilgang kan i prinsippet kikke på ganske mange personopplysninger som det strengt tatt ikke er tjenestelig behov for å se. [75] En av informantene opplyste at vedkommende ikke har tilgang til [redacted], men kan gå til en ansatt i sin avdeling med tilgang for å hente ut informasjon.[76]

Denne måten å organisere systemtilgang på kan være problematisk. Systemtilgangen åpner for snoking. Eksempelvis kan en ansatt kikke på en tidligere kjæreste eller studiekamerat selv om vedkommende vet at dette ikke er lov, fordi opplysningen kan ha sosial verdi. En enkel måte å løse denne typen problemstillinger på kan være å sørge for automatisk loggføring hver gang noen ser på en kundemappe. Datatilsynet omtaler vid tilgang i forhold til tjenestebehov som et problem og sier at

> Datatilsynet har tidligere påpekt at ansattes taushetsplikt blir brukt som argument for at den som har ansvar for å sikre opplysninger i et datasystem ikke innfører tilstrekkelig tilgangskontroll til opplysningene. Datatilsynet ser på dette som en ansvarsfraskrivelse på systemnivå, og er bekymret for at personvernet kun skal være opp til den enkelte ansattes integritet og egne vurderinger.[77]

---

[74] [redacted] s. 3
[75] Jf intervju B og senere bekreftelse på e-post
[76] Jf intervju C
[77] URL: http://www.datatilsynet.no/templates/Page____2619.aspx (lest 13.05.09)

Tilgangskontroll må sies å være en viktig side av informasjonssikkerheten i forvaltningsorganet som behandlingsansvarlig er ansvarlig for.

Databehandler er en ekstern aktør[78], som i pol § 2 nr. 5 defineres som den eller de personer som arbeider med informasjonssystemer/registre som prosesserer personopplysninger for behandlingsansvarlige. Dette begrepet må ikke forveksles med interne saksbehandlere. I personopplysningsloven blir databehandler sett på som en oppdragstaker utenfor behandlingsansvarliges virksomhet.[79]
Av pol § 15 første ledd kommer det frem at det skal foreligge en skriftlig avtale mellom behandlingsansvarlig og databehandler. Vi kan her også lese at avtalen skal regulere databehandlers råderett over personopplysninger, og den skal videre inneholde de sikringstiltak databehandler må gjennomføre for en sikker behandling av personopplysninger etter pol § 13. Avtalen mellom behandlingsansvarlig og databehandler bør derfor være utformet så detaljert som mulig i henhold til personopplysningsloven. Altså kan man si at jo bedre avtalen er utformet jo klarere ansvarsområde vil databehandleren få.

Det kan se ut som om forvaltningsorganet på dette området tilfredsstiller de kravene loven oppgir i pol § 15. I forvaltningsorganets standardavtale[80] for databehandlere[81] kreves det at både databehandler og behandlingsansvarlig skal tilfredsstille krav til informasjonssikkerhet etter pol § 13 og pof kapittel 2. Videre stiller avtalen også spesifikke krav til teknisk og fysisk sikring vedrørende personopplysninger.

En stor utfordring mange virksomheter møter er at flere særlover som regulerer sikkerhet samvirker med personopplysningsforskriftens bestemmelser i kapittel 2. Schartum påpeker at

[78] Schartum og Jansen (2005) s. 112
[79] Schartum og Bygrave (2006) s. 37
[80] Databehandleravtale versjon 1.6
[81] [redacted]

> (…) forvaltningsorganer som planlegger systemer og rutiner for elektronisk kommunikasjon der det inngår personopplysninger, vil det for eksempel være nødvendig å sammenholde/etterleve minst to regelsett samtidig"[82]

I forvaltningsorganets tilfelle kan dette eksempelvis dreie seg om særlover som blant annet [redacted], lov om elektronisk signatur, og eForvaltningsforskriften mv.

Som vi har nevnt ovenfor, er det den daglige lederen som skal stå for den faktiske gjennomføringen av tiltak rundt informasjonssikkerhet, mens den behandlingsansvarlige har det øverste ansvaret for at dette skjer. I praksis vil nok den daglige lederen delegere gjennomføringen av dette til lavere nivåer i virksomheten (f eks til daglig ansvarlige). En slik løsning vil kunne være forenelig med lovens formålsparagraf.

[82] Schartum (2004) s. 137

6.0 Ansvar for opplysningskvalitet

Behandlingsansvarlig skal sørge for at de grunnkravene loven stiller til behandling av personopplysninger blir fulgt opp. Noen av disse kravene finner vi i pol § 11 første ledd. To av disse tar for seg opplysningskvalitet – henholdsvis bokstavene d og e. Her fremkommer det krav om at opplysningene skal være tilstrekkelige og relevante, korrekte og oppdaterte ut i fra formålet med behandlingen[83]. Når man vurderer hvor strengt disse kravene skal etterfølges må man se til formålet for behandlingen. Schartum og Bygrave beskriver dette slik:

> Jo større risiko for personvernkrenkelser (jf § 1) på grunn av formålet, jo strengere krav er det aktuelt å stille til kvaliteten av personopplysninger. Krav til kvalitet på adresseopplysninger vil f eks variere avhengig av om formålet er å sende ut reklame eller varsler om inkasso.[84]

Videre følger det av pol § 27 første ledd at behandlingsansvarlig skal korrigere uriktige opplysninger som måtte oppdages. Dette uavhengig av om man avdekker feilen selv, eller blir gjort oppmerksom på dette fra den registrerte[85]. Når formålet med behandlingen opphører, er behandlingsansvarlig pliktig til å sørge for at opplysningene slettes etter pol § 28 første ledd. Det er noen unntak fra denne sletteregelen, blant annet kan annen lovgivning pålegge videre lagring.[86]

I forvaltningsorganet hentes som nevnt opplysninger fra flere tredjeparter samt den registrerte selv.[87] Dersom tredjepart er et offentlig organ, antas opplysningene å være korrekte.[88] I de tilfeller det ikke er samsvar mellom opplysninger gitt av registrerte og opplysninger fra tredjepart, behandles [redacted] manuelt. Det ligger også i systemet kontrollfunksjoner for "lovlige" verdier av opplysninger som kommer fra registrerte selv. I de tilfeller der den registrerte oppgir verdier som går utenfor den "akseptable" grensen, vil saken bli sjekket manuelt.[89] For at forvaltningsorganet skal være sikker på at opplysninger om navn, adresse eller kontonummer alltid er korrekt

[83] Jf pol § 11 første ledd bokstav d og e
[84] Schartum og Bygrave (2004) s. 139
[85] "Registert" blir definert i pol § 2 nr 6
[86] F eks lov om arkiv av 12.april 1992 nr 126
[87] [redacted] s. 5
[88] Jf intervju C
[89] Jf intervju C

og oppdaterte, er det strenge rutiner for å endre disse. I tillegg blir blant annet opplysninger om adresse hyppig sjekket opp mot folkeregisteret.[90]

Gjennom [redacted]-prosjektet ble det blant annet foretatt en risikoanalyse i forhold til regelverket. Man så på hvilke deler av regelverket som kunne medføre feilaktig saksbehandling og dermed medføre at saksbehandlingen endte opp med feil resultat. [redacted][91]

Også i denne sammenhengen kan det være verdt å nevne forvaltningsorganets kvalitetsutvalg. Utvalgets mandat er blant annet å foreta kontroll av saksbehandlingen og foreslå tiltak til forbedringer ut fra egne erfaringer og funn i den kontrollerte saksbehandlingen.[92] Det vil her blant annet bli vurdert om innsamlet data er riktig.[93]

Når det gjelder organiseringen av arbeidet med opplysningskvalitet, er det ingen i forvaltningsorganet som er tildelt et særskilt ansvar for dette. Imidlertid legges det, som vi har vært inne på tidligere, et stort fokus på at alle ansatte skal ha den nødvendige kompetansen for å tilfredsstille de kravene loven kommer med.

Det er heller ikke vårt inntrykk at det eksisterer noen spesiell organisering for å sikre etterlevelse av slettereglene. Dette blir også bekreftet av alle informantene, som opplyser at det i forvaltningsorganet ikke er noen spesielle rutiner for sletting av personopplysninger. Informant A sier at opplysningene i praksis vil bli lagret til evig tid. Informant B opplyser i tillegg at opplysninger er relevante for forvaltningsorganet i lang tid da det eksisterer krav om å sjekke eventuelle tidligere kundeforhold. Det er i denne sammenheng verdt å ta i betraktning at det i forskrift om [redacted]

[90] Jf intervju B
[91] Jf intervju C
[92] Jf intervju D
[93] Jf intervju C

[redacted][94] står at opplysninger som er hentet inn av forvaltningsorganet skal behandles i samsvar med personopplysningsloven. Ut ifra dette leser vi at det er personopplysningslovens sletteregler som gjelder for alle personopplysninger forvaltningsorganet har innhentet.

På systemnivå vil derimot enkelte opplysninger bli slettet automatisk, f eks [redacted].

Som vi har sett blir store deler av kontrollen rundt personopplysningenes kvalitet og sletting foretatt maskinelt. Dette kan være litt problematisk da det ikke er noen som har et spesielt ansvar rundt disse oppgavene. Det er liten tvil om at det overordnede ansvaret alltid vil ligge hos behandlingsansvarlig i begge tilfeller. Ut over dette kan det med fordel delegeres kompetanse til å gjennomføre tiltak angående opplysningskvalitet og sletting til et lavere nivå i organisasjonen. Vår anbefaling vil være å la de ulike daglige ansvarlige få denne kompetansen. Dette kan igjen sies å være i tråd med lovens formålsbestemmelse.

94 [redacted]

7.0 Avslutning

Vi har gjennom arbeidet med denne rapporten fått et grundig innblikk i et moderne forvaltningsorgans virksomhet. Forvaltningsorganet er langt framme når det gjelder elektronisk forvaltning, [redacted].[95] Som et forvaltningsorgan med en så stor kundemasse, vil det være essensielt å ha et bevisst forhold til personopplysningsvern. Vårt fokus har vært på de organisatoriske sidene ved etterlevelse av lovverket. Vår erfaring er at arbeidet med personopplysningsvern i forvaltningsorganet er prioritert, og at det har vært lagt ned en del arbeid på dette området. Blant annet er det utarbeidet en stor mengde dokumentasjon vedrørende både organisering og rutinemessige tiltak for å sikre etterlevelse av lovverket. Imidlertid er det grunn til å bemerke at denne dokumentasjonen i varierende grad stemmer med praksis. Vi tror det kan være hensiktsmessig å gå gjennom dokumentasjonen og tilpasse den i til dagens situasjon.

Under vår gjennomgang av dokumentasjonen samt under intervjuene viste det seg at det muligens eksisterer en tolkning av begrepet ansvar som etter vårt skjønn ikke helt samsvarer med det loven har lagt opp til. Vi fikk inntrykk av at forvaltningsorganet i mange tilfeller oppfatter ansvarsbegrepet som oppgaver knyttet til en stilling. Slik vi forstår loven, vil ansvar være det juridiske ansvaret for å se til at en oppgave blir utført, uavhengig av om man gjør oppgaven selv eller overlater den til andre.

Basert på vårt helhetlige inntrykk ser vi det som fornuftig å plassere behandlingsansvaret hos styret ved styreleder. Dette vil kreve at styret inntar en mer aktiv rolle enn det vi har inntrykk av at de gjør i dag. Slik vi ser det vil dette også samsvare bedre med føringene gitt av [redacted]. Med behandlingsansvaret plassert hos styreleder vil rollen som daglig leder falle naturlig til direktøren. Med andre ord vil direktøren forstsatt ha det operative ansvaret for etterlevelse av loven.

[95] Imidlertid kan det være verd å merke seg at et annet forvaltningsorgan har tilbydd helautomatiske tjenester [redacted]

Det daglige ansvaret for behandlingsansvarliges plikter ser vi for oss delegert nedover til de ulike underdirektørene. Dette vil blant annet være [redacted] samt enkelte nøkkelpersoner i [redacted].

Personvernombud er en rolle forvaltningsorganet per dags dato ikke har, men vår anbefaling vil være å opprette en slik ordning. Denne rollen kan legges til en allerede eksisterende stilling.

Vi mener videre at kvalitetsutvalget kan passe godt til arbeidet med sikkerhetsrevisjon, og lederen for dette utvalget vil kunne fylle rollen som sikkerhetsrevisor. Vi ser også for oss at arbeidet med å oppdatere interne dokumenter som omhandler personopplysningsvern kan legges til dette utvalget. I dag er det tilført 20 prosent av en stilling til dette utvalget og vi ser at hvis dette skal kunne gjennomføres i praksis vil man kanskje måtte øke denne stillingsprosenten noe. Vi ser ikke at våre forslag til endringer vil medføre store kostnader for forvaltningsorganet, da de i stor grad allerede sitter på den kompetansen som trengs for en slik gjennomføring.

Litteratur og kilder

Bakka, Frode Jørgen, Fivelsdal, Egil og Nordhaug, Odd: (2003), Organisasjon og ledelse. Struktur, prosesser, læring og kultur, 4 utgave Oslo: Cappelen Akademisk Forlag

Christensen, Tom, Egeberg, Morten, Larsen, Helge O, Lægreid Per og Roness, Paul G. (2007): Forvaltning og politikk, Oslo: Universitetsforlaget

Coll, Line M og Lenth, Claude A (2000): Personopplysningsloven – en håndbok. Oslo: Kommuneforlaget

Databehandleravtale versjon 1.6. [redacted] 23.mars 2009

Datatilsynet (2009): *Temaer og tendenser i 2008*. URL: http://www.datatilsynet.no/templates/Page____2619.aspx [Lesedato 13.05.2009]

Datatilsynets årsmelding 2004. (2005). URL: http://www.datatilsynet.no/upload/Dokumenter/publikasjoner/aarsmeld/Datatilsynet_manus_aarsm2004.pdf [Lesedato: 10.05.2009 og 15.05.2009]

Direktørens styringssignaler. [redacted] 02.04.2008

[redacted] 23. juni 2003

Eckhoff, Torstein og Smith, Eivind (2003), Forvaltningsrett 7. utgave 2. opplag, Oslo, Universitetsforlaget

Etablering av internkontroll (2001). URL: http://www.datatilsynet.no/upload/Dokumenter/internkontrollfiler/internkontroll08102001.pdf [Lesedato 07.05.2009]

[redacted]

Forskrift om behandling av personopplysninger 15. desember nr. 1265

[redacted] 6. mars 2009

Jansen, Arild og Schartum, Dag Wiese (red.) (2007): ”Elektronisk forvaltning og jus” i Elektronisk forvaltning i Norden – praksis, lovgivning og rettslige utfordringer. Oslo, Fagbokforlaget

Lov om behandling av personopplysninger av 14. april 2000 nr. 31.

Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967 nr. 00.

Lov om rett til innsyn i dokument i offentleg verksemd av 19. mai 2006 nr. 16

[redacted]

[redacted] 08.11.2007

[redacted]
[Lesedato 08.05.2009]

[redacted]: URL:
[redacted] [Lesedato: 27.04.01.2009]

[redacted]: URL:
[redacted]
[Lesedato: 27.04.2009]

[redacted]: URL:
[redacted] [Lesedato 11.04.2009]

Macionis, John J. and Plummer, Ken (2005), Sociology. A Global Introduction, third edition. London: Pearson Education Limited

[redacted] [Lesedato 06.05.2009]

Ot.prp. nr. [redacted]. URL:
[redacted], [Lesedato: 11.05.2009]

[redacted] 5. januar 2004.

[redacted]6. januar 2004.

Schartum, Dag Wiese (2000) *Lov om behandling av personopplysninger*: URL: http://websir.lovdata.no/cgi-lex/wifthy4?LOV-2000-04-14-31-p14#map9 [Lesedato: 15.05.2009]

Schartum, Dag Wiese (2005): ”Krav til sikring av personopplysninger” I: Informasjonssikkerhet – rettslige krav til sikker bruk av IKT. Schartum, Dag Wiese og Jansen, Arild (red.). Oslo: Fagbokforlaget

Schartum, Dag Wiese (2008): *Personvern i sentralforvaltningen* URL: http://www.kunnskapsnettverk.no/C7/C1/Ressursnettverk%20for%20eforvaltni/Document%20Library/Personvern%20i%20sentralforvaltningen.pdf [Lesedato: 16.05.2009]

Schartum, Dag Wiese og Bygrave, Lee A (31. mars 2006): Utredning av behov for endringer i personopplysningsloven. Oslo: Fagbokforlaget

[redacted] 04.06.2008

St.meld. nr. [redacted]
URL:
[redacted] [Lesedato 28.04.2009]

Styring med styrer, Vurdering av styrene for virksomheter under Utdannings- og forskningsdepartementet (2003). URL: www.difi.no/Rapport_**2003-18**_4qNk-.pdf.file [Lesedato 05.05.2009]

[redacted]

Veileder: Bruk av personopplysninger i forskning
DEL II Hvilke regler gjelder for forskning? (2005). URL: http://www.datatilsynet.no/upload/Dokumenter/veiledere/forskningsinfo_del_ii_1_0.pdf [Lesedato 07.05.2009]

Østerud, Øyvind. (2007), Statsvitenskap. Innføring i politisk analyse. Oslo: Universitetsforlaget.

Årsrapport 2002 [redacted]. URL:
[redacted] [Lesedato 28.04.2009]

Årsrapport 2003 [redacted]. URL:
[redacted], [Lesedato 28.04.2009]