Arbeids- og administrasjonsdepartementet

Konsekvensutredning av prosjekt Elektronisk postjournal

Andersen Consulting og
Advokatfirmaet Føyen & Co

20. desember 1999

Innholdsfortegnelse

1. Sammendrag

Rapporten konkluderer med at det **bør etableres en allment tilgjengelig Elektronisk postjournal**. Dagens løsning gir tilgang til Elektronisk postjournal kun til medieredaksjoner. Vårt syn er at med tanke på en varig og regulær ordning må utgangspunktet være at en ikke kan løse personvernproblematikken ved å begrense tilgangen til visse grupper, mens flertallet stenges ute.

Overordnet inntrykk er at teknisk løsning og IT sikkerhet i dagens løsning er relativt bra, dog med unntak. Datakvaliteten er svært viktig for tjenestens troverdigheten. Vi mener derfor at det viktigste er å få innført rutiner og mekanismer for å avdekke eventuelle feil som oppstår før eller under dataoverføring, konvertering eller innlegging av postjournaler fra informasjonsleverandør til operatør.

Det er **sentrale personvernmessige problemstillinger** som oppstår ved å utvide dagens løsning til å bli en allment tilgjengelig Elektronisk postjournal. Både Stortingets justiskomité og Datatilsynet, blant mange flere, har vært opptatt av dette. To forhold har blitt løftet frem som de viktigste:

- risikoen for at følsomme opplysninger skal bli spredd. Opplysninger som er undergitt taushetsplikt eller som kan unntas fra offentlighet, skal etter dagens regelverk sladdes, men feil vil få en større spredning ved en allment tilgjengelig Elektronisk postjournal
- muligheten for å bygge personprofiler ved å søke på journalopplysninger der personopplysninger fremgår. Det er muligheten til å søke på og sammenstille opplysninger som skaper personvernproblemer, ikke først og fremst den enkelte opplysning vurdert isolert.

Vi anbefaler at det første punktet løses gjennom en **innskjerping og justering av de rutinene som finnes i dag**. Det andre punktet løses ved at **søkemuligheten på navn på fysiske personer**, i saker der navnet ikke av andre grunner uansett skal sladdes, **fjernes etter 12 måneder i den allment tilgjengelige elektroniske postjournalen**. Videre anbefaler vi at det vurderes om også **visning av navn på fysisk person skal begrenses etter 12 måneder.**

Vi har gjennomført en inngående drøfting av de juridiske problemstillinger som reises i tilknytning til Elektronisk postjournal. Avveiningen mellom offentlighetsprinsippet og de personvernmessige forholdene står sentralt i drøftingen (kap 4).

Vi har kartlagt og vurdert de tekniske og sikkerhetsmessige aspekter ved løsningen. Trusselbildet og sikkerhetsfaktorer drøftes i forhold til informasjonsleverandører (de statlige virksomhetene), operatør (Posten SDS) og brukerne (i dag redaksjoner), samt i forhold til kommunikasjonen mellom de tre partene. Videre har vi identifisert en rekke tiltak for å bedre sikkerheten, både i forhold til formelt stilte krav og i forhold til hvilke sikkerhetskrav en løsning som Internett-journal etter vår mening bør møte (kap 5). Vi kommenterer også hva som kan gjøres for å komme frem til en teknisk løsning på den skisserte sladdingen av navn på fysisk person (kap 7).

2. Innledning

2.1 Bakgrunn for oppdraget

Siden 1988 har Pressesenteret i Regjeringskvartalet tilbudt pressen tilgang til offentlige postjournaler fra departementene og en god del underliggende etater. I november 1990 foreslo Regjeringens informasjonsutvalg (RIU) at det skulle gjennomføres et mindre antall pilotprosjekter for å gjøre nytt materiale fra forvaltningen eksternt tilgjengelig. Prosjekt Elektronisk postjournal ble lansert i 1993 som ett av disse pilotprosjekter.

I den første fase av prosjektet var fire departementer, ett direktorat og fem redaksjoner fra distriktene med som deltakere. En evaluering av prosjektet[1] påpekte at løsningen var lite brukervennlig og at bruken av løsningen fra redaksjonenes side var meget begrenset.

Likevel ble fase II av prosjektet startet i februar 1996, blant annet med en vesentlig mer brukervennlig teknisk løsning og med 16 redaksjoner med spesiell interesse for journalsøk. En ny evaluering fra januar 1997[2] konkluderte med at Elektronisk postjournal er meget nyttig for media. Samtidig påpekte den at den økte pågangen av dokumentbestillinger ga et visst merarbeid i arkivene.

Pr. desember 1999 deltar 14 departementer og 7 underliggende etater som informasjonsleverandører til Elektronisk postjournal, mens 82 redaksjoner har tilgang til den passordbelagte søketjenesten på Internett. Prosjektet Elektronisk postjournal er stadig et pilotprosjekt.

Arbeids- og administrasjonsdepartementet uttrykker nå ønske om å bringe tjenesten over i permanent drift, og åpne for allmenn tilgang til de elektroniske postjournalene. Før dette blir aktuelt ønsker imidlertid departementet å få gjennomført en konsekvensutredning med hovedfokus på den juridiske og tekniske aspektene knyttet til dette, henholdsvis:

1. De personvernmessige følgene av å åpne for allmenn tilgang til Elektronisk postjournal.
2. De sikkerhetsmessige aspekter ved nåværende løsning, spesielt mht sikkerhet for overføringene, mulighet for oppdatering av journalene og mulighet for sladding av opplysninger unntatt offentlighet.

Disse spørsmål adresseres i foreliggende konsekvensutredning. Arbeidet er gjennomført i samarbeid mellom Andersen Consulting og Advokatfirmaet Føyen & Co.

2.2 Fremgangsmåte

Utgangspunktet for den juridiske vurderingen har vært å drøfte dette relativt uavhengig av de øvrige, dog vil resultatet gi noe input til de øvrige punkter. Arbeidet har vært en utredning av de kryssende hensyn som ligger til grunn for prinsippet om offentlighet i forvaltningen og personvernprinsippene, herunder drøfting med Datatilsynet.

[1] Kluge: Offentlige elektroniske postjournaler i pressen; Norsk Regnesentral, 1994.
[2] Bonne og Henriksen: Vurdering av elektronisk postjournal; Pharos DA, 1997.

Arbeidet med den tekniske vurderingen har i stor grad tatt utgangspunkt i en sikkerhetsmessig vurdering, dvs. sikring av konfidensialitet, integritet, tilgjengelighet av følgende:

- overføring av data fra informasjonsleverandør til operatør, herunder også kompletthet i overføringene
- lagring av data
- søking i data og overføring av data fra operatør til bruker
- mulighet for uvedkommende å sammenstille tappede data

Det er bedt spesielt om en redegjørelse for hvordan dagens løsning møter de sikkerhetsmessige kravene. Vi har derfor lagt vekt på å klargjøre tekniske og sikkerhetsmessige krav i den foreliggende rapporten, og kartlegge og vurdere hvordan dagens løsning tilfredsstiller disse. Dagens løsning og tekniske og sikkerhetsmessige alternativer er videre vurdert opp mot de juridiske vurderinger.

Kartleggingen av mål og andre overordnede krav, samt kartlegging av brukerbehov, kompetansekrav mv er delvis dekket i evalueringen foretatt av Pharos i 1996/97. Tilsvarende gjelder for synliggjøring av verdier. Kartlegging av dette er derfor til en viss grad bygget på tidligere evalueringer av prosjekt Elektronisk postjournal.

Prosjektets arbeidsform har vært basert på intervjuer og gjennomganger med prosjekt Elektronisk postjournal i STATENS INFORMASJONSTJENESTE, operatør for tjenesten (Posten SDS), Statens forvaltningstjeneste, utvalgte informasjonsleverandører, sikkerhetsansvarlige og brukere, samt drøfting med Datatilsynet.

2.3 Avgrensninger

I denne konsekvensutredningen har vi konsentrert oss om å drøfte de mest sentrale problemstillinger knyttet til dagens løsning for Elektronisk postjournal og for en allment tilgjengelig Elektronisk postjournal. Vi har videre utarbeidet forslag til prinsipiell løsning for allment tilgjengelig Elektronisk postjournal; et forslag som balanserer offentlighetsprinsippet mot personvernhensyn. Vi har vurdert hvordan de tekniske utfordringene knyttet til løsningen skal takles på et overordnet nivå, for å sikre at vi unngår å anbefale løsninger som ikke er gjennomførbare. Vi har imidlertid ikke vurdert de tekniske løsningene i detalj, for eksempel de tekniske konsekvensene av en stor økning i antall brukere og informasjonsleverandører.

Det har ikke ligget innenfor rammen av dette oppdraget å vurdere alternative tekniske løsningskonsepter.

Denne konsekvensutredningen gjør ikke en vurdering av kostnader knyttet til drift av løsningen. Kostnadene knyttet til en eventuell oppgradering av eksisterende løsning vurderes heller ikke.

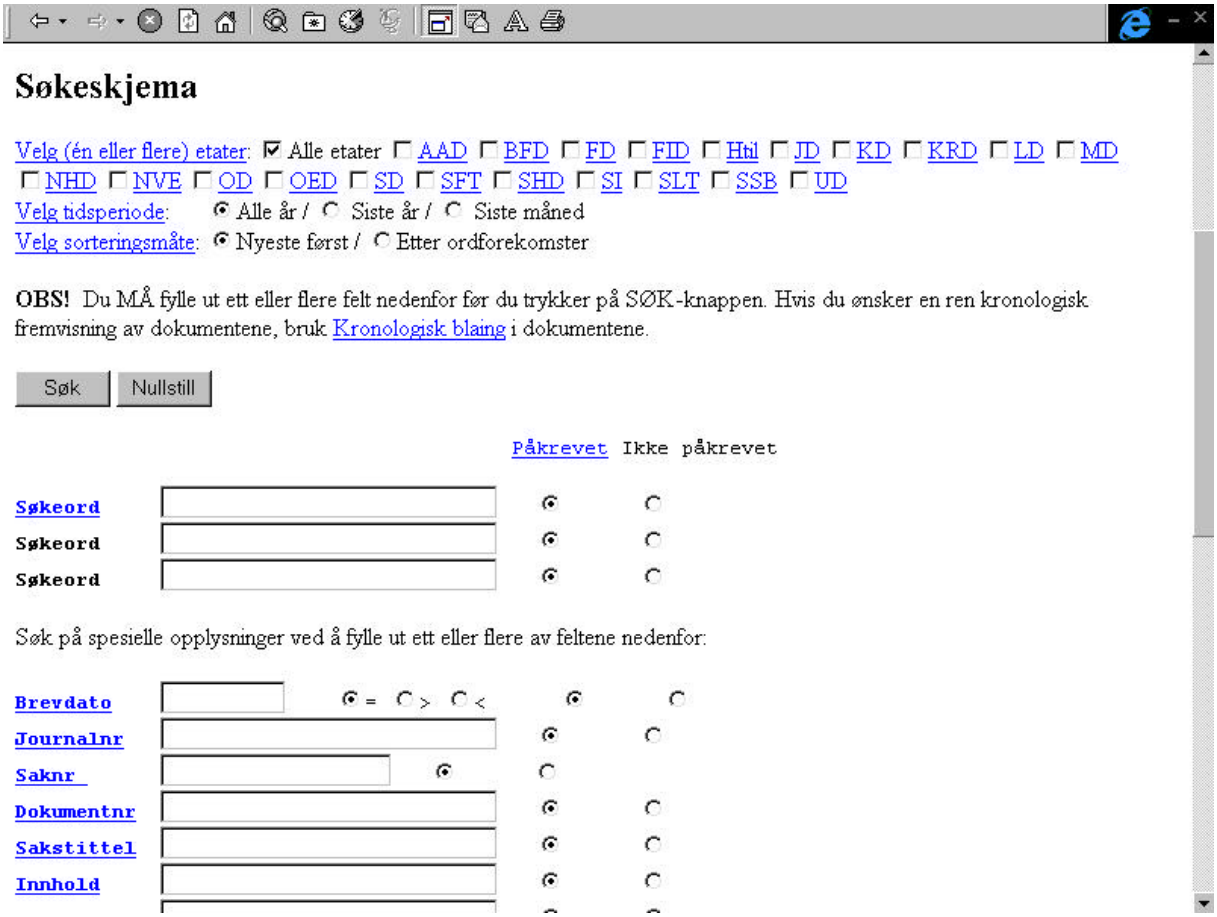
Våre vurderinger baserer seg på de dokumenter som er tilgjengelige om Elektronisk postjournal, samt øvrig relevant dokumentasjon av teknisk, juridisk og politisk karakter. Vi har fått innspill fra og drøftet problemstillingene med utvalgte informasjonsleverandører og storbrukere av tjenesten, Datatilsynet, Statens informasjonstjeneste og Posten SDS.

Ellers må det presiseres at vi ikke vurderer direkte elektronisk tilgang til dokumenter; det er forutsatt at dette skal bestilles i papirformat som i dag. Bestillingsfunksjonen er riktignok meget enkel med Elektronisk postjournal, men selve saksdokumentene er ikke søkbare. Det må antas at det ikke ligger så langt inn i framtiden at de aller fleste offentlige dokumenter blir elektronisk tilgjengelige. Det vil betydelig redusere forvaltningens arbeid knyttet til praktisering av offentlighet. Det vil også forsterke de personvernmessige betenkeligheter, selv om sentrale opplysninger i dokumentet vil framgå i journalen. Prosjektet vurderer ikke dette nærmere.

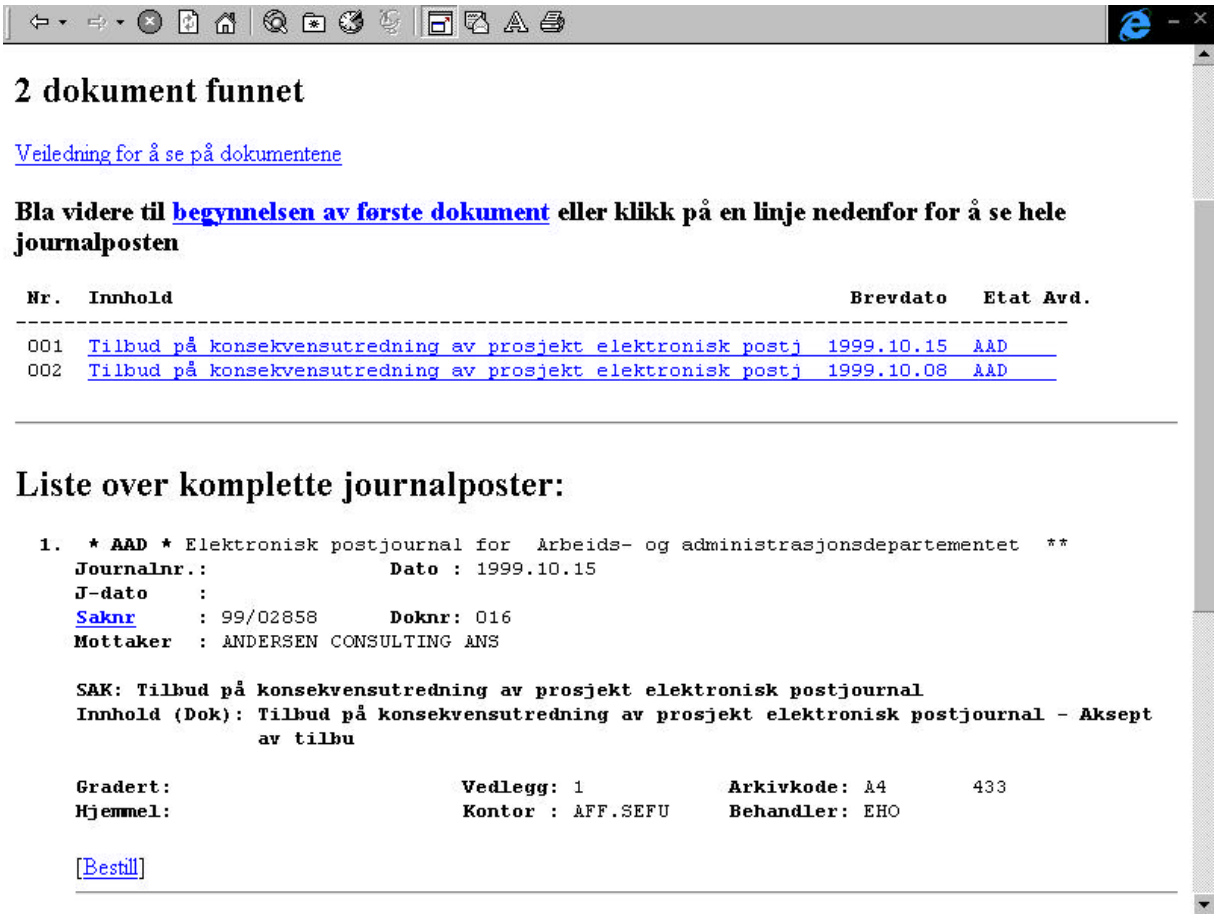
2.4 Om Elektronisk postjournal pr. desember 1999 – roller og begreper

Vi vil her kort redegjøre for de ulike rollene i Elektronisk postjournal og hvem som gjør hva. Vi vil også definere de mest sentrale begrepene i denne sammenhengen. Som en illustrasjon, vil vi først vise et par skjermbilder fra Elektronisk postjournal.

Nedenfor vises bildet som fremkommer ved å klikke på søk i dokumenter i Elektronisk postjournal.



Et eksempel på søkeresultat, ved å søke på Andersen Consulting i mottakerfeltet og krysse av for Arbeids- og administrasjonsdepartementet som informasjonsleverandør og siste år, fremkommer følgende bilde:



2 dokument funnet

Veiledning for å se på dokumentene

Bla videre til begynnelsen av første dokument eller klikk på en linje nedenfor for å se hele journalposten

Nr.	Innhold	Brevdato	Etat	Avd.
001	Tilbud på konsekvensutredning av prosjekt elektronisk postj	1999.10.15	AAD	
002	Tilbud på konsekvensutredning av prosjekt elektronisk postj	1999.10.08	AAD	

Liste over komplette journalposter:

1. * AAD * Elektronisk postjournal for Arbeids- og administrasjonsdepartementet **
   Journalnr.: Dato : 1999.10.15
   J-dato :
   Saknr : 99/02858 Doknr: 016
   Mottaker : ANDERSEN CONSULTING ANS

   SAK: Tilbud på konsekvensutredning av prosjekt elektronisk postjournal
   Innhold (Dok): Tilbud på konsekvensutredning av prosjekt elektronisk postjournal - Aksept av tilbu

   Gradert: Vedlegg: 1 Arkivkode: A4 433
   Hjemmel: Kontor : AFF.SEFU Behandler: EHO

   [Bestill]

2.4.1 Roller og ansvar

Grovt sett er det tre roller knyttet til daglig operasjon av tjenesten Elektronisk postjournal. Dette er den virksomhet som leverer en kopi av sine journaler for elektronisk offentliggjøring (informasjonsleverandør), den virksomhet som samler de elektroniske journalene og gjør dem tilgjengelige over Internett (operatør) samt brukeren av tjenestene. Operatør er i dag Posten SDS.

Statens informasjonstjeneste har i dag en rolle i etableringen av Elektronisk postjournal, men har ingen egen rolle i drift. SIs driftsrolle er heller å være kanal for felles interesser hos informasjonsleverandørene, for eksempel å være rådgiver ved etablering av tjenesten, å forestå valg av operatør og å koordinere publisering av felles informasjon om tjenesten.

Kort sagt kan vi si at dersom vi legger terminologien fra Personopplysningsloven[3] §§ 13 og 15 til grunn, er informasjonsleverandøren *behandlingsansvarlig*, mens operatøren er *databehandler*. Dette er videre diskutert i kap 4.2.2.5.

2.4.2 Begreper

Noen av de sentrale begreper i foreliggende vurdering er definert under. Se forøvrig videre definisjoner i vedlegg 1.

Prosjekt Elektronisk postjournal er prosjektet under Statens informasjonstjeneste som har stått for utvikling av tjenesten Elektronisk postjournal som den fremstår i dag. Prosjektet administrerer pilot-ordningen, dvs hvem som skal ha tilgang til tjenesten i pilot-perioden.

[3] Ot prop nr 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven). I det følgende oftest referert til som persondataloven

Elektronisk postjournal er tjenesten å tilby journalene fra et antall departementer og underliggende etater på elektronisk form, foreløpig til et begrenset antall brukere.

Allment tilgjengelig Elektronisk postjournal, eller kortformen **Internett-journal**, er Elektronisk postjournal lagt ut på Internett uten tilgangsbegrensninger. Dog kan det være begrensning i hvor mye informasjon som er lagt ut (sladding) eller hvor lenge den enkelte journalpost er tilgjengelig.

Informasjonsleverandør er et departement eller annen offentlig etat som leverer sin journal til Elektronisk postjournal.

Operatør er den som driver tjenesten Elektronisk postjournal etter avtale med Statens informasjonstjeneste. I dag er dette Posten SDS.

3. Prosjektet i forhold til offentlighetspolitikken

Vi vil her kort redegjøre for de politiske målsetningene knyttet til prosjekt Elektronisk postjournal, slik disse er nedfelt i offentlige dokumenter.

3.1 Målsetninger

Den tidligste offisielle forankring for prosjekt Elektronisk postjournal er i IT-strategi for Regjeringens informasjonsutvalg (RIU) fra november 1990[4]. Under et punkt 11.2.3 foreslås det at man bør gjennomføre et mindre antall pilotprosjekter som tar sikte på å gjøre nytt materiale fra forvaltningen eksternt tilgjengelig. Et av disse prosjektene går ut på å gjøre offentlige postjournaler fra utvalgte departementer tilgjengelige for pressen (pkt 11.2.3.2).

I juni 1992 orienterer Statens informasjonstjeneste i et brev til Arbeids- og administrasjons-departementet om at RIU-rapporten er bakgrunn for at Statens informasjonstjeneste har startet arbeidet med prosjektet. Begrunnelsen er *geografisk utvidelse av pressens mulighet til å praktisere innsynsretten etter offentlighetslovens prinsipper*. Pressesenteret i regjeringskvartalet hadde på det tidspunktet bedret pressens mulighet til å praktisere innsynsretten for de redaksjoner som har sete i Oslo gjennom utlegg av papirjournaler. Elektronisk postjournal ville gjøre tilgangen lettere for redaksjonene i Oslo og vesentlig lettere for redaksjoner utenfor Oslo. En utvidelse av brukere til også å gjelde forvaltningen løftes frem som en mulig videreutvikling.

Offentlighetsmeldingen[5], gir en bred presentasjon av offentlighetspolitikken generelt, og beskriver også hvordan Elektronisk postjournal og andre teknologiske nyvinninger støtter opp om de politiske målene på området. Bondevik-regjeringen uttaler (kap 5.12.4.1):

> *»Regjeringen er positiv til å bruke informasjonsteknologi for å effektivisere gjennomføringen av offentlighetsprinsippet og vil gå inn for å nytte informasjonsteknologien slik at brukerne av offentlighetsloven får raskere og enklere tilgang til forvaltningens journaler og saksdokumenter. Samtidig er det en forutsetning at informasjonsteknologien nyttes på en måte som tar tilbørlig hensyn til andre verdier, som f eks personverninteresser. Videre er det viktig at tradisjonelle måter å gjennomføre offentlighet på ikke svekkes, fordi store deler av befolkningen fremdeles vil være avhengig av disse.»*

I AADs tildelingsbrev til Statens informasjonstjeneste nevnes hvert år prosjekt Elektronisk postjournal. I tildelingsbrevet for 1999 er formuleringen:

> *»Regjeringen legger stor vekt på større åpenhet og innsyn i forvaltningen. SI bør bidra til dette, og departementet ser positivt på at SI videreutvikler prosjekt Elektronisk postjournal også i 1999 med sikte på å få alle departementer og Statsministerens kontor, samt de 15-20 største direktoratene med. Prosjektet Elektronisk postjournal er et svært viktig ledd i arbeidet med større åpenhet og innsyn i forvaltningen. Dette prosjektet bør nå evalueres/konsekvensutredes. Departementet ønsker å drøfte opplegget for en slik utredning med SI, med sikte på gjennomføring i løpet av første halvår 1999. Prosjektets videre fremtid vil bli basert på resultatene fra denne utredningen.»*

I kapittelet om resultatkrav i tildelingsbrevet er dette konkretisert: *Statens informasjonstjeneste skal medvirke til større åpenhet og innsyn i statsforvaltningen bl a ved å videreutvikle prosjektet Elektronisk*

[4] IT-strategi for Regjeringens informasjonsutvalg (RIU), november 1990
[5] St meld 32 1997-98, Om offentlighetsprinsippet i Forvaltningen

postjournal slik at det omfatter alle departementene og de største direktoratene (AAD vil evaluere prosjektet i 1999).

Også i Regjeringens Forvaltningspolitiske redegjørelse til Stortinget, som ble holdt av statsråd Dåvøy 26. april 1999[6], blir prosjektets positive bidrag til offentlighetsprinsippet fremholdt:

> *» Bruk av ny teknologi fører til store endringer i forvaltningen og samfunnet for øvrig. Lovverket må revideres slik at det tar hensyn til endringene. Ny teknologi og medieutvikling har bidratt til mer åpenhet, men stiller også nye krav til arkivering, gjenfinning og offentliggjøring i forvaltningen. Jeg ser det derfor som svært viktig å ha et bevisst forhold til denne utviklingen. Prosjektet Elektronisk postjournal er et godt eksempel på hvordan ny teknologi kan bidra til større åpenhet i forvaltningen. Samtidig minskes betydningen av geografisk avstand til forvaltningen ved at departementenes journaler gjøres elektronisk tilgjengelige og søkbare på Internett. Regjeringen har som mål å få alle departementer og større etater med på dette prosjektet.»*

3.2 Vurdering av Elektronisk postjournal i henhold til målsetninger i offentlighetspolitikken

Vi har ikke kunnet identifisere personer eller miljøer som er kritiske i forhold til at Elektronisk postjournal støtter opp om de sentrale målsetningene i offentlighetspolitikken. Det er en klar og enkel sammenheng mellom tiltak som gjør tilgjengeligheten til journaler lettere og målene knyttet til åpenhet i forvaltningen. Det er også vanskelig å se for seg alternative tiltak som på en bedre måte kan bidra til måloppnåelse innenfor dette konkrete feltet. Dette er antagelig årsaken til den manglende debatten knyttet til om Elektronisk postjournal er et godt virkemiddel i denne forbindelse. Ut fra offentlighetspolitikken isolert sett, blir altså det mest kritikkverdige at tiltaket ikke er mer omfattende, både på informasjonsleverandør og brukersiden.

De viktige avveiningene i forhold til personvernhensyn må imidlertid ivaretas, jf. diskusjoner i kap 4. Dette blir også understreket av Justiskomitéen i Stortinget. Komitéen har, i sin behandling av offentlighetsmeldingen, enstemmig gitt uttrykk for at forskjellen mellom papirdokumenter og digitalt nett som informasjonsbærer er meget stor, og bør få konsekvenser[7]:

> *«Komiteen viser til at saksdokumenter og journaler i forvaltningen skal være offentlige som hovedregel. En hensiktsmessig måte å gjøre dette på vil være å gjøre dokumentene eller journalen digitalisert og dermed søkbar. Dette reiser etter komiteens oppfatning personvernmessige problemstillinger. Slike søkemuligheter vil gjøre det mulig å sammenholde opplysninger og lage "profiler" og "biografier" av enkeltpersoner. Teknisk anonymisering vil ofte vise seg å være utilstrekkelig, da man kan identifisere personer gjennom andre søkekriterier.*
>
> *Komiteen mener at forskjellen mellom papirdokumenter og digitalt nett som informasjonsbærer er meget stor og bør få konsekvenser. Dagens offentlighetspraksis forutsetter at man vet hva man leter etter, finner det og setter det inn i en sammenheng ut fra en definert interesse. Den sammenstilling av opplysninger som et digitalt nett gir muligheter for, skaper nye utfordringer. Det åpner muligheter for at forvaltningens viten og informasjon fra innbyggerne kan bli misbrukt i en mindre aktverdig retning. Det kan føre til at en del borgere vil unnlate å ta kontakt med forvaltningen. I så fall vil offentlighetsloven motvirke sin intensjon, nemlig å åpne for informert, offentlig ordskifte og meningsbryting om fellesskapets anliggender og borgerens aktive engasjement i samfunnsspørsmål.*
>
> *Komiteen mener at borgere aktivt må informeres om at henvendelser vil bli tilgjengelig elektronisk.*

[6] http://odin.dep.no/aad/publ/publ.html – Offentlig sektor – et spørsmål om tillit
[7] Innst. S. nr. 21 1998-99

Komiteen ber Regjeringen også vurdere mulighetene for anonymisering av enkeltpersoner, og for å fjerne direkte søkemuligheter på personalia.»

4. Vurdering av prosjektet i forhold til de personvernmessige hensyn

4.1 Innledning

Dette kapittelet utgjør den juridiske delen av prosjektet «Konsekvensutredning av Elektronisk postjournal» som Andersen Consulting og Advokatfirmaet Føyen & Co (Føyen) gjennomfører i samarbeid for Arbeids- og administrasjonsdepartementet .

Denne delen av prosjektet er beskrevet under pkt 1 i tilbudsinnbydelsen fra Arbeids- og administrasjonsdepartementet. En del av bakgrunnen er at Datatilsynet har akseptert at Elektronisk postjournal kan fortsette uten sletting av journaler etter en bestemt tid, men kun så lenge adgangen til journalbasen er begrenset slik det er i dag. I regjeringens offentlighetsmelding signaliseres en positiv holdning til å bruke IT til å «effektivisere gjennomføringen av offentlighetsprinsippet». Samtidig, heter det videre, «er det en forutsetning at informasjonsteknologien nyttes på en måte som tar tilbørlig hensyn til andre verdier, som f eks personverninteresser.»[8] I justiskomiteens innstilling om meldingen blir dette ytterligere framhevet, jf avsnitt 3.2.[9]

Arbeids- og administrasjonsdepartementet ønsker derfor at de personvernmessige følgene av å åpne for allmenn tilgang til databasen, som en nå ønsker å vurdere, skal utredes og drøftes nærmere med Datatilsynet.

Utgangspunktet for herværende prosjekt er offentlighetsprinsippet. Elektronisk postjournal begrunnes primært i at dette er en måte å fremme offentlighet i forvaltningen på. Dette hensyn har også en sterk rettslig forankring. På den annen side står i særlig grad personvernhensyn. Det er imidlertid også andre beskyttelseshensyn som gjør seg gjeldende, knyttet til både private og offentlige interesser. Det ligger utenfor prosjektets rammer å belyse dette med noen grundighet.

Herværende utredning belyser derfor de rettslige spørsmål prosjektet reiser i skjæringspunktet mellom offentlighetshensyn og personvernhensyn.

Nedenfor gis først en generell oversikt over rettsstoffet. Relevante regler og annet rettskildemateriale relatert til de to hovedhensyn blir gjennomgått (kap 4.2). Dernest (kap 4.3) beskrives de sentrale trekk ved Elektronisk postjournal sett i forhold til de juridiske problemstillinger (typer opplysninger som gjøres tilgjengelig, søkemuligheter mv). Identifiserte alternative systemer/løsningsmåter beskrives for så vidt dette har relevans for de juridiske spørsmål. I kap 4.4 foretas en konkret drøftelse av de aktuelle løsningsmåter sett i lys av de rettslige utgangspunkter og de kryssende hensyn som konkret gjør seg gjeldende. Det vurderes hvorvidt personvernmessige grunner tilsier at det settes særlige begrensninger eller tiltak.

Det er ikke i prosjektbeskrivelsen sagt noe om at det skal vurderes lov- eller forskriftsendringer. Det anses likevel nødvendig for utredningen å berøre slike spørsmål.

[8] Se St meld nr 32 (1997-98) Om offentlighetsprinsippet i forvaltningen, på s.87

[9] Se Innst S nr 21 (1998-99) på s.2-3. Omtales heretter bare som Innst.

Dette kapittelet utformes slik at det kan stå på «egne bein». Samtidig er den en del av hovedrapporten, der den avsluttende anbefaling reflekterer de vurderinger som kommer fram i herværende delrapport.

4.2 Generell oversikt over rettsstoffet

4.2.1 Offentlighetsprinsippet

4.2.1.1 Overordnete utgangspunkter

I offentlighetsmeldingen er det i kap 2 og 3 gitt en generell framstilling av offentlighetsprinsippets bakgrunn og innhold. Det heter her (s 11) at «Offentlighetsprinsippet regnes i dag som et grunnleggende demokratisk prinsipp i de nordiske land.» Det refereres også flere forslag om å grunnlovsfeste prinsippet om borgernes rett til dokumentinnsyn.

Et slikt forslag er også tatt opp i Ytringsfrihetskommisjonens innstilling[10], hvis forslag til nytt fjerde ledd i grl § 100 lyder:

«Enhver har Ret til Indsyn i Statens og Kommunernes Acter og til at følge Forhandlingerne i Retsmøder og folkevalgte Organer. Loven kan kun sætte slige klarlig definerede Grændser for denne Ret, hvor særligt tungtveiende Hensyn gjøre dette nødvendigt.»

Kommisjonen foreslår dessuten et nytt siste ledd i grl § 100 som også kan ses i lys av offentlighetsprinsippet:

«Det paaligger Statens Myndigheder at lægge Forholdene til Rette for en aaben og oplyst offentlig Samtale.»

Å tilrettelegge for praktisering av innsyn i informasjon som er så viktig for den alminnelige samfunnsdebatt som forvaltningens saksdokumenter, er et betydelig bidrag til en åpen og opplyst offentlig debatt. Det er i dag ingen klar rettslig forankring for dette synspunktet for statsforvaltningens del; derimot inneholder kommunelovens § 4 en bestemmelse som sier:

»Forholdene skal legges best mulig til rette for offentlig innsyn i den kommunale og fylkeskommunale forvaltning.»

Enkeltbestemmelser i lovverket, herunder regelen i fvl § 11 om forvaltningens alminnelige veiledningsplikt, kan imidlertid ses som utslag av et liknende synspunkt også for statsforvaltningens del. Synspunktet har under enhver omstendighet en sterk politisk forankring.[11]

4.2.1.2 Offentlighetslovens hovedregler om dokument- og journaloffentlighet

Den viktigste form for offentlighet i forvaltningen er i praksis dokumentoffentlighet, som har sin rettslige forankring i offentlighetsloven av 19. juni 1970 nr 69. Hovedregelen er som kjent etter § 2 første ledd at forvaltningens saksdokumenter er offentlige. § 2 andre ledd lyder:

[10] NOU 1999:27 Ytringsfrihed bør finde sted

[11] Se NOU 1999:27 på s.89-91 for en drøftelse av offentlig informasjonspolitikk og informasjonsplikt. Se dessuten Administrasjonsdepartementet: *Statlig informasjonspolitik: Hovedprinsipper*. Desember 1994

«Enhver kan hos vedkommende forvaltningsorgan kreve å få gjøre seg kjent med det offentlige innholdet av dokumenter i en bestemt sak. Det samme gjelder journal og lignende register og møtekart til folkevalgte organer i kommuner og fylkeskommuner.»

Det er den siste setningen - som statuerer utgangspunktet og hovedregelen om at journaler er offentlige (unntakene kommer vi til nedenfor) - som utgjør det rettslige utgangspunktet for herværende prosjekt.

Grunnen til regelen om offentlighet for journaler er først og fremst at disse gir en nøkkel til å finne fram til saker og dokumenter som kan ha interesse for et eller annet formål. Av dette følger at journalen som utgangspunkt skal være offentlig i sin helhet; det gjelder ingen avgrensning til en enkelt eller konkret angitt sak, slik det gjør for dokumentoffentlighet (kravet til individualisering). Dette individualiseringskrav vil det, uten journalinnsyn, svært ofte være meget vanskelig å oppfylle. Regelen om offentlige journaler er således helt sentral for at innsynsretten skal ha realitet. Visse unntak gjelder likevel, som det vil framgå nedenfor under pkt 4.2.1.5.

Journalen kan også ha interesse i seg selv. Hvilket formål den som ønsker innsyn har med å se journalen, har ingen betydning for innsynsadgangen.

F eks ba fredsforskningsinstitusjonen PRIO i 1980 om å få bruke journalen bl a i Forsvarsdepartementet for å lage statistikk over antall graderte saker i departementet, noe som i første omgang ble delvis avslått. Etter lovendringen i 1982 er det ikke rom for tvil om at journalinnsyn ikke kan avslås i et slikt tilfelle.

Som det har framgått, er offentlighetsloven § 2 en regel om rett til innsyn på begjæring. Det finnes ingen regel i offentlighetsloven som verken hjemler eller krever mer aktiv publisering. Offentlighetsloven kan imidlertid åpenbart ut fra hele sitt formål og karakter ikke forstås slik at den setter *skranker* for dette

Spørsmålet om bruk av digitale verktøy ved praktisering av offentlighet, er ikke direkte regulert i loven. I § 8 heter det at forvaltningsorganet avgjør spørsmålet om utleveringsform «ut fra hensynet til forsvarlig saksbehandling». § 8 tredje ledd forutsetter at dokument også kan gjøres tilgjengelig «i maskinlesbar form». Direkte er ikke journaler nevnt her. Reelt sett er det imidlertid ikke grunn til å behandle journaler som er undergitt offentlighet annerledes enn saksdokumenter som er det.[12] Etter dette må vi kunne legge til grunn at offentlighetsloven ikke krever elektronisk publisering, men at den heller ikke er til hinder for dette.

4.2.1.3 Hovedregler om unntak fra offentlighet

For det første: Opplysninger som er undergitt taushetsplikt, har forvaltningen *plikt* til å holde hemmelig, jf offentlighetsloven § 5a. Slike opplysninger må dermed heller ikke framgå av det som gjøres tilgjengelig gjennom journal. Det understrekes at dokumentet som sådan ikke - som utgangspunkt - er unntatt offentlighet selv om visse opplysninger i dokumentet er det. Når det gjelder hva som er belagt med taushetsplikt, er det ikke grunn til å gå detaljert inn på det her. Offentlighetsloven inneholder ikke selv regler om taushetsplikt, men viser generelt til bestemmelser om «taushetsplikt i lov eller i medhold av lov». De viktigste regler er å finne i forvaltningsloven[13] § 13 og § 13 a-f, men taushetsplikt er også fastsatt i enkelte andre lover. Det

[12] Hos Arvid Frihagen, Offentlighetsloven, 1994, Bind I, heter det på s. 154: «I og med at loven nå uttrykkelig fastsetter at journalen skal være offentlig, må vi anta at de vanlige regler om krav på kopi etter § 8 gjelder.»

[13] Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967.

understrekes at avtale- eller instruksbasert taushetsplikt ikke er tilstrekkelig til at en opplysning faller inn under § 5 a.

For det andre har offentlighetsloven regler om dokumenter som *kan* unntas fra offentlighet, men hvor det også er adgang til å gi innsyn, meroffentlighet. Slike bestemmelser kalles *kompetansenormer*. I denne kategorien har vi for det første interne dokumenter (§ 5) og for det andre dokumenter som kan unntas offentlighet på grunn av sitt innhold (§ 6). Det vil ikke være i strid med offentlighetsloven dersom det gis innsyn i slike dokumenter, og dermed heller ikke om opplysninger i denne kategorien framgår av offentlig journal.

4.2.1.4 Hovedbestemmelser om plikt til journalføring

Offentlighetsloven inneholder etter sin ordlyd verken et pålegg til forvaltningen om å føre journal eller noen regler om hva journalen skal inneholde og hvordan den skal føres. Men ettersom journalføring, som foran nevnt, er helt vesentlig for å gjennomføre offentlighetsprinsippet, må en kunne si at loven innebærer en plikt til journalføring. Visse minimumskrav til innholdet i journalføringen følger nødvendigvis allerede av selve journalbegrepet.

En klarere uttrykt plikt for offentlige organer til å føre journal, og de generelle krav til hva journal skal inneholde mv, følger av arkivregelverket. Det vises til lov om arkiv av 04.12.92 nr 126 §§ 6 og 12, og til arkivforskriften (forskrift om offentlige arkiv av 11.12.98 nr 1193). § 2-6 flg. Begge trådte i kraft 01.01.99. Før dette tidspunkt var arkiverings- og journalføringsplikten kun forankret i instruks, nemlig arkivinstruksen. Det rettslige grunnlaget for forvaltningens plikt til å føre journal er for så vidt, etter vår vurdering, i dag tilstrekkelig klart (om det kan være grunn til endringer på enkeltpunkter er en annen sak). Justiskomiteen går i innstillingen om offentlighetsmeldingen (avgitt i november 1998) inn for at det i offentlighetsloven lovfestes en plikt til å føre fortløpende journal for hele den offentlige sektor (Innst s. 8).

Etter arkivforskriften § 2-6 første ledd skal alle inngående og utgående dokument som etter offentlighetsloven §§ 2 og 3 må regnes som saksdokumenter for organet, registreres, så fremt de «er gjenstand for saksbehandling og har verdi som dokumentasjon.» Det har i prinsippet ikke betydning om det dreier seg om brev, telefaks eller e-post. Arkivforskriften § 3-2 sier:

»Dokument som blir avsende eller mottekne via telefaks og e-post, og som etter form eller innhald må reknast som saksdokument for organet, skal arkivmessig behandlast som andre saksdokument etter denne forskrifta, jf. særleg §§ 2-6, 3-1 og 3-8.

Organ som nyttar e-post, skal ha eit sentralt e-postmottak for post til organet. E-post til det sentrale postmottaket skal opnast av arkivtenesta.»

Noe annet er at når det gjelder e-post, er det kjent at det slurves nokså mye med overholdelsen av registreringsplikten, hvilket ikke er et ubetydelig problem gitt den store økningen i bruk av denne kommunikasjonsform.

Privat post til tjenestemann eller til politisk ledelse, herunder partipost, er ikke registreringspliktig. Avgjørende er ikke uten videre hvem posten er adressert til, men om innholdet fyller arkivforskriftens og offentlighetslovens kriterier. Grensedragningen er i prinsippet grei, selv om den involverer skjønn. Også her har en, i hvert fall tidligere, sett at praksis ikke alltid har vært helt regelverklojal.[14] I offentlighetsmeldingen anføres det imidlertid at

[14] Se Arvid Frihagen, Offentlighetsloven, 1994, Bind I, s. 178

det på dette området har utviklet seg en hensiktsmessig praksis, en vurdering justiskomiteen i sin innstilling slutter seg til.[15]

Det bør nevnes at journalføring ikke er et vilkår for offentlighet. Er et dokument feilaktig utelatt fra journalføring, vil det derfor likevel kunne være offentlig. I praksis blir imidlertid offentlig innsyn betydelig vanskeliggjort i slike tilfeller.

Organinterne dokumenter kan registreres, «så langt organet finn det tenleg.» (§ 2-6)

I forbindelse med utbredelsen av e-post i forvaltningen, har det vært reist spørsmål om de registre som e-postprogrammene genererer, er «journal eller lignende register» i offentlighetslovens forstand. Det kan ikke sees at det er grunnlag for et slikt syn. Slike registre har karakter av interne arbeidsredskap. De vil typisk inneholde en betydelig mengde uformelle og gjerne personlige henvendelser. Det reelle journalføringsbehov må ivaretas ved overføring av relevante epostmeldinger til det regulære arkivet. Det kunne vurderes å innføre endrete rutiner, herunder særlige krav til funksjonalitet for e-postprogrammer benyttet i forvaltningen, som på en bedre måte sikret og tilrettela for at arkivverdige e-postmeldinger faktisk ble journalført. Det ligger utenfor prosjektets rammer å gå nærmere inn på dette.

Arkivforskriften § 2-6 andre ledd åpner for elektronisk journalføring og sier uttrykkelig at dersom journalen inngår i et elektronisk arkiv- eller saksbehandlingssystem, skal en på en enkel måte kunne hente ut og gjøre tilgjengelig de journalopplysninger som allmennheten har krav å få innsyn i. NOARK-standarden, som dominerer i bruk i statsforvaltningen i dag, jf også forskriften § 2-9, fyller disse krav.

Av § 2-7 framgår hvilke opplysninger journalen skal inneholde, og som dermed allmennheten har krav på innsyn i etter offentlighetsloven. Hovedprinsippet er at journalføring skal skje på en måte som gjør det mulig å identifisere dokumentet, så langt det kan gjøres uten å røpe opplysninger som

- er undergitt taushetsplikt,
- eller som *kan* unntas offentlighet etter §§ 5 og 6 i offentlighetsloven.

Hvis registrering ikke er mulig uten at slike opplysninger blir røpet, kan det benyttes «nøytrale kjenneteikn, utelatingar eller overstryking» på den del av journalen «som allmenta kan krevje innsyn i». I den elektroniske journalen skjer dette i dag rett og slett ved at de aktuelle deler utelates. Det går altså ikke an å se at det er sladdet, slik som man kan hvor dette er gjort på papir. Dermed kan man heller ikke søke på spesielle tegn for å få fram journalinnføringer hvor det er foretatt sladding. Vi kan ikke se at verken ordlyd eller reelle hensyn bak «sladdingsreglene» tilsier at man skal kunne se hvor det er sladdet, slik at dagens praksis er uproblematisk i forhold til reglene, selv om man i praksis får en teknologibetinget forskjell.

Hel utstryking er bare tillatt dersom dette er nødvendig for ikke å røpe opplysninger som er undergitt lovhjemlet taushetsplikt.

Ikke alle deler av journalen er nødvendigvis offentlige. Ifølge § 2-7 første og andre ledd *skal* journalen inneholde:

a) journalføringsdato,
b) saks- og dokumentnummer (journalnummer i papirbaserte journalar),
c) sendar og/eller mottakar,
d) opplysningar om sak, innhald eller emne,
e) dateringa på dokumentet.

[15] Innst s. 12.

I tillegg skal journalen innehalde arkivkode (etter arkivnøkkelen), ekspedisjons- eller avskrivingsdato og avskrivingsmåte.

Som det sees, er det som omfattes av bokstavene a-c og e entydig gitt. Derimot er det nødvendig å utøve et visst skjønn i forhold til bokstav d. Det er arkivet som, etter dagens rutiner, foretar innføringen av journaldata og dermed utøver dette skjønnet. Oftest brukes nok overskriften på brevet, men det er ikke sikkert at denne svarer til kriteriet i bokstav d.

Ifølge § 2-7 fjerde ledd *kan* det registreres opplysninger som bare skal brukes for den interne saksoppfølgingen, slik som navn på saksbehandler, behandlingsfrister og lignende.

4.2.1.5 Særregler om unntak fra offentlighet for visse journaler

Forskrift hjemlet i offentlighetsloven § 11 (forskrift av 14.02. 1998 nr 0351) inneholder i kap V og VI spesielle regler om fullstendig unntak fra offentlighet for visse journaler.

Avsnitt V unntar følgende:
- Journaler for saker vedr Industrifondets engasjementer (nr 4)
- Journaler og registre i fremmedsaker og statsborgersaker, dog ikke saker av generell art (nr 8)
- Journal for visse saker under Statens vegledningskontor for oppfinnere (nr 11)
- Overvåkingstjenestens journaler (nr 14)

Avsnitt VI unntar følgende:
- Journaler for en rekke sakstyper på det familierettslige området og for saker etter visse inngrepslover (barnevernlov, lov om psykisk helsevern m fl) (nr 1)
- UDs journal for saker vedrørende person- og familierett, arv med mer (nr 2)
- Tollvesenets journaler (nr 4)

For øvrig er det særregler for dokumenter gradert etter beskyttelsesinstruksen og sikkerhetsinstruksen, som vi skal se nærmere på.

For sikkerhetsinstruksen[16] viser forskriften til denne instruksens § 7, som unntar fra offentlighet journaler for dokumenter merket STRENGT HEMMELIG, HEMMELIG og KONFIDENSIELT. For dokumenter merket BEGRENSET er det valgfritt om de føres i offentlig eller ikke-offentlig journal. Instruksen har ikke annen hjemmel enn den alminnelige instruksjonsmyndighet og prinsippet om regjeringen som overordnet Forsvaret etter grl § 25. Lov går foran instruks, slik at det ikke er uten videre avgjørende for om et dokument er offentlig, eller kan undergis offentlig innsyn, om det er gradert etter sikkerhetsinstruksen.[17] Det er særlig offentlighetsloven § 6 første ledd nr 1, om adgang til å unnta fra offentlighet dokumenter som inneholder visse typer opplysninger om utenriks- og sikkerhetspolitiske forhold, som er av betydning i denne sammenheng. Hvis vilkårene her ikke er oppfylt, vil det ikke være adgang til å unnta dokumentet fra offentlighet, uansett gradering. Og selv om disse vilkårene er oppfylt, vil det være adgang til å praktisere meroffentlighet. Dette harmonerer dårlig med at det er anledning til å føre alle graderte dokumenter i ikke-offentlig journal.

Denne, og andre, rettslige konfliktspørsmål knyttet til sikkerhetsinstruksen vil imidlertid bortfalle. Sikkerhetsinstruksen vil bli avløst av lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) av 20.03. 1998 nr 10, som i § 13 angir kriteriene for de ovennevnte sikkerhetsgraderingene. Loven er pr dags dato ikke satt i kraft. Sikkerhetsloven fastsetter i § 12 taushetsplikt i forbindelse med

[16] Instruks for behandling av dokumenter som av sikkerhetsmessige grunner må beskyttes (sikkerhetsinstruksen) Gitt 17.03.1972.
[17] Se nærmere Frihagen, Bind II s. 354 flg.

sikkerhetsgradert informasjon. Man vil derfor, når sikkerhetsloven trer i kraft, komme innenfor offentlighetslovens automatiske unntak for opplysninger undergitt lovbestemt taushetsplikt (§ 5 a).

Beskyttelsesinstruksen[18], som ikke har annet hjemmelsgrunnlag enn sikkerhetsinstruksen, blir imidlertid ikke opphevet ved sikkerhetsloven. Instruksen kommer til anvendelse ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsinstruksen. Betingelsene for gradering framgår av §§ 3 og 4, og er for det første at dokumentet *kan* unntas fra offentlighet og dernest at offentlighet kan medføre nærmere beskrevne skadevirkninger for offentlige eller private interesser (juridiske eller fysiske personer). Her vil en fortsatt kunne komme i den situasjon at graderte dokumenter er offentlige etter offentlighetsloven, ettersom gradering ikke i seg selv er avgjørende for om organet har adgang til å unnta dokumentet fra offentlighet. At et dokument er gradert, skal heller ikke være avgjørende for praktisering av meroffentlighet, i det instruksens § 5 sier at en revurdering av graderingen skal skje når det kommer henvendelse om innsyn i dokumentet.

For dokumenter gradert etter beskyttelsesinstruksen viser forskriften til offentlighetsloven (nr 6) til denne instruksens § 8. Etter denne er journaler for dokumenter merket STRENGT FORTROLIG unntatt fra offentlighet. For dokumenter merket FORTROLIG er det valgfritt om de føres i offentlig eller ikke-offentlig journal.

Disse bestemmelsene som åpner for at alle graderte dokumenter, også de som er gradert etter laveste grad, føres i ikke-offentlig journal, kan innebære en nokså uheldig konsekvens sett fra offentlighetsprinsippets ståsted. Dokumenter som enten er uriktig gradert, eller der opprinnelig gradering på et senere tidspunkt burde vært opphevet, slik at dokumentet etter loven skulle vært offentlig, vil i praksis ikke kunne bli gjenstand for innsyn, fordi det ikke figurerer i offentlig journal.

Eksempelet gir en generell illustrasjon av journalreglenes viktighet for praktiseringen av offentlighetsprinsippet, og er for så vidt et argument for justiskomiteens ønske om å få disse reglene nedfelt i offentlighetsloven.

4.2.2 Hensynet til personvernet

4.2.2.1 Innledning. Grunnleggende bestemmelser

Også hensynet til personvernet er et grunnleggende prinsipp i vårt samfunn. Vi finner et spor av dette i bestemmelsen i Grunnloven § 102 om at »Hus-inkvisitioner» kun kan finne sted i kriminalsaker. En adskillig mer generell formulering gis i den europeiske menneske-rettighetskonvensjon (EMK) art 8, der det i første avsnitt heter »Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.» Ved menneskerettsloven av 21.05.1999 nr. 30 er EMK gjort til en del av norsk lov med forrang framfor annen lovgivning i tilfelle konflikt.

Personvernhensynet har gitt seg utslag bl a i bestemmelsen i straffeloven § 390 a som setter straff av bøter eller fengsel inntil 3 måneder for «den som krenker privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold.»

Hensynet til personvernet har også på ulovfestet grunnlag blitt anvendt i rettspraksis.

[18] Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsinstruksen (Beskyttelsesinstruksen) Gitt 17.03.1972.

Omfanget av behandling av personopplysninger har økt drastisk over de siste 20-30 år. Utviklingen har særlig skutt fart med nye sprang i utviklingen av de teknologiske muligheter til å håndtere og distribuere informasjon. Den sentrale lovgivning på personvernområdet knytter seg derfor (i hvert fall i praksis) først og fremst til elektronisk behandling av personopplysninger, og håndhevingsorganet er Datatilsynet.

4.2.2.2 Personregisterloven og personopplysningsloven

Den någjeldende lov om personregistre m.m. fra 09.06 1978 (pregl) gjør i liten grad elektronisk lagring til et direkte avgjørende rettslig kriterium. Her er derimot registerbegrepet sentralt, og dette forutsetter at opplysningene er «lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.» (§ 1 andre ledd) Helt fra denne lov ble innført kan en si at den har ligget etter utviklingen, for så vidt som utbredelsen av elektronisk databehandling, og utviklingen av mer avansert databaseteknologi, gjør at gjenfinnbarheten ikke beror på hvordan opplysningene i utgangspunktet er lagret (om dette er gjort «systematisk» eller ikke). I praksis har en imidlertid tolket loven slik at hovedvekten er lagt på gjenfinnbarhet, ikke på om opprinnelig lagring er gjort systematisk. Det betyr at databaserte systemer som inneholder personopplysninger, anses som personregistre i lovens forstand.

Etter forslaget til ny lov om behandling av personopplysninger (persondataloven) er det primære kriterium for hva som omfattes av loven «behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler» (§ 3 første ledd bokstav a). Kriteriet «personopplysning» er identisk etter pregl og persondataloven med en viktig forskjell, nemlig at etter den nye lov omfattes ikke juridiske personer.

Lovforslaget er framsatt i Ot prop nr 92 (1998-99). Loven vil implementere EU-direktiv nr 95/46/EF av 24.10.95,[19] jf EØS-avtalen og EØS-loven.[20] Selv om proposisjonen ikke har vært behandlet av Stortinget, og den antagelig ikke vil kunne settes i kraft før mot slutten av år 2000 (bl a fordi det er nødvendig først å utarbeide forskrifter til loven), er det denne som har størst interesse.

Elektronisk postjournal vil inneholde opplysninger om fysiske personer allerede ved at journalen skal angi dato, avsender og mottaker av dokumentet. Innholdsangivelsen vil dessuten gi ytterligere opplysninger (jf over under pkt 4.2.1.4). At journalen også vil inneholde en mengde opplysninger som ikke har karakter av personopplysninger, gjør ingen forskjell. Behandlingen av opplysningene skjer (pr definisjon) ved elektroniske hjelpemidler. Følgelig vil journalen i utgangspunktet falle inn under persondatalovens virkeområde.

Vi ser i det følgende først kort på forholdet til personregisterloven, og deretter går vi nærmere inn på forholdet til persondataloven.

Slik personregisterloven har blitt tolket, vil Elektronisk postjournal i utgangspunktet omfattes av loven. Fordi den inneholder personopplysninger, og det gjøres bruk av elektroniske hjelpemidler, faller den også i utgangspunktet inn under konsesjonsplikten etter § 9. I § 41 første punktum gjøres det unntak for personregistre i organ for stat eller kommune som er opprettet ved egen lov.

---

[19] Direktivet er i dansk versjon trykt som vedlegg til Ot prop nr 92. (1998-99)

[20] Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) mv (EØS-loven) av 27.11. 1992 nr 109. Se spesielt § 2, som lyder: »Bestemmelser i lov som tjener til å oppfylle Norges forpliktelser etter avtalen, skal i tilfelle konflikt gå foran andre bestemmelser som regulerer samme forhold. Tilsvarende gjelder dersom en forskrift som tjener til å oppfylle Norges forpliktelser etter avtalen, er i konflikt med en annen forskrift, eller kommer i konflikt med en senere lov.»

Forvaltningens journaler er registre som er opprettet ved egen lov, nemlig arkivloven (jf foran). I § 41 heter det imidlertid videre:

«Også for slike registre skal det likevel fastsettes regler som nevnt i § 11, i den utstrekning det ikke er fastsatt noe annet i eller i medhold av heimelsloven. Også de andre bestemmelsene i loven gjelder for slike registre i den utstrekning ikke annet følger av hjemmelsloven.»

Etter § 9 andre ledd er det hjemmel til ved forskrift å unnta «visse typer personregistre» fra konsesjonsplikten, hvilket er gjort for en rekke registre, bl a domstolenes registre (forskrift av 21.12. 1979, sist endret 02.12. 1996). Forskriften fastsetter regler om slike forhold som er nevnt i pregl § 11 om hva som skal reguleres ved konsesjonsvilkår. Imidlertid er ikke forvaltningens postjournaler forskriftsregulert.

I praksis har en sett det slik at offentlig journal ikke har vært omfattet av pregl, men har vært regulert av særlov (strengt tatt var det likevel kun *instruks* – nemlig arkivinstruksen – som hjemlet registrene inntil 01.01.99, da arkiv*loven* trådte i kraft). Det er ikke derfor heller ikke krevd konsesjon etter pregl for journalen. Så lenge den elektroniske postjournalen har vært et begrenset prøveprosjekt, har Datatilsynet heller ikke sett grunn til å kreve konsesjons-behandling av denne. Med en vesentlig utvidelse av tilgjengelighet for, og dessuten innhold i, journalen i forhold til dagens prøveordning, vil imidlertid personvernaspektene bli av en kvalitativt annen karakter, og en kan ikke si at dette er ivaretatt ved reguleringen i arkiv- og offentlighetslovverket, da dette lovverk – som vi har sett – ikke forutsetter slik form for offentliggjøring. Det bør også bemerkes at prøveprosjektet har hatt en varighet og et omfang, som tilsier at det under enhver omstendighet er på høy tid at det gjøres til gjenstand for regulering ut fra personvernhensyn, selv om det ikke var tale om å utvide prosjektet.

Det følger av § 5 i persondataloven at den ikke gjelder «om…annet følger av en særskilt lov som regulerer behandlingsmåten». Hva som nærmere ligger i dette, er ikke åpenbart. Spesialkommentaren i proposisjonen utdyper innholdet i paragrafen ved å si at «de enkelte bestemmelsene i persondataloven (får) anvendelse i den utstrekning ikke annet følger av den særskilte loven som regulerer behandlingsmåten.»[21] Innholdsmessig er dette, i forhold til vår problemstilling, det samme som følger av personregisterloven § 41. Det innebærer altså at offentlighetsloven / arkivloven er særlover som går foran persondataloven så langt det gjelder slik behandling av personopplysninger som er regulert av disse lovene.

En annen bestemmelse om forholdet mellom lovene er persondataloven § 6, der det uttrykkelig er sagt at loven ikke begrenser innsynsrett etter offentlighetsloven. Heller ikke uttrykker noe annet enn det man i dag legger til grunn ved tolkningen av de to lovverkene.
Men når det gjelder Elektronisk postjournal, innebærer dette en form for innsyn som går adskillig *utover* det som følger av offentlighetsloven. Persondataloven § 6 har derfor kun relevans for slik innsynsrett som dagens offentlighetslov regulerer, ikke for det som går utover dette, i.e. Elektronisk postjournal.

4.2.2.3 Konklusjon vedrørende forholdet mellom offentlighetsloven og persondataloven

Vår konklusjon ut fra ovenstående er at «tradisjonell» praktisering av offentlighetsloven / arkivloven faller utenfor persondataloven. Så langt det praktiseres offentlighet innenfor de rammer disse lover trekker opp, vil dette måtte bedømmes som spesielle lover, som går foran persondataloven. Men ved Elektronisk postjournal, og i særlig grad dersom dette gjøres til en åpent tilgjengelig Internett-journal, dreier det seg om en form for tilgjengeliggjøring av

[21] Ot prop nr 92 på s. 106

opplysninger som i vesentlig grad går utover det som er regulert i arkiv- og offentlighetsloven, og som har betydelige personvernmessige implikasjoner.

Regulatorisk er det to hovedmåter å løse dette på. Den ene vil være å endre offentlighetsloven (evt også arkivloven) slik at disse lover hjemler Elektronisk postjournal, derunder slik at de inneholder nærmere regler som personvernmessige hensyn tilsier. Den andre måten vil være å gi persondataloven anvendelse på Elektronisk postjournal.

Det bør tilføyes at dette spørsmålet ikke er avgjørende for hvilket personvernmessig beskyttelsesnivå man legger seg på. Og under enhver omstendighet vil EU-direktivets minimumskrav måtte ivaretas.

Etter vår vurdering vil den første framgangsmåten klart være å anbefale. Elektronisk postjournal springer ut av offentlighetsprinsippet, og det er mest hensiktsmessig og «brukervennlig» at man har samlet bestemmelsene som skal realisere dette prinsippet så langt som mulig i én lov. I nødvendig utstrekning må persondatalovens bestemmelser innarbeides. I neste avsnitt foretar vi en analyse av persondataloven med henblikk på spørsmålet om i hvilken utstrekning lovens bestemmelser bør gis anvendelse på Internett-journal.

4.2.2.4 I hvilken utstrekning bør persondatalovens bestemmelser gis anvendelse på Internett-journal? Forholdet til EU-direktivet

4.2.2.4.1 Innledning

Hva enten Internett-journal reguleres i offentlighetsloven eller i persondataloven, oppstår spørsmålet om i hvilken utstrekning relevante bestemmelser i persondataloven er tilfredsstilt eller bør gis tilsvarende anvendelse. Hvordan dette lovteknisk bør skje, går vi ikke grundig inn på. Dersom en kommer til at noen bestemmelser i persondataloven ikke er tilfredsstilt og ikke egner seg i denne sammenheng – ut fra hensynet til offentlighetsprinsippet og arkivhensyn - blir det spørsmål om en slik løsning er forenlig med EF-direktivet av 24.10.95 om behandling av personopplysninger mm (direktiv 95/46/EF, heretter kalt EU-direktivet eller bare direktivet). Drøftelsen vil derfor fortløpende drøfte forholdet til EU-direktivet i den utstrekning våre anbefalinger om fravik fra persondataloven gjør dette nødvendig.

Spørsmålet om «tradisjonell» praktisering av offentlighetsprinsippet er forenlig med EU-direktivet, er en problemstilling som, for svensk retts del, er drøftet i den offentlige utredning som gikk forut for Lag om personuppgifter (PUL).[22] Konklusjonen er at så er tilfelle.[23] Svensk offentlighets-lovgivning er i vesentlige drag sammenfallende med den norske, og vi trekker veksler på den svenske utredningen i det følgende.

Et generelt holdepunkt i denne sammenheng, er art 72 i fortalen til direktivet, som sier at det ved gjennomførelsen av direktivet kan tas hensyn til prinsippet om aktinnsyn i offentlige dokumenter. Dette gir grunnlag for en viss fleksibilitet ved tolkningen av direktivets enkeltbestemmelser, der dette er begrunnet i offentlighetsprinsippet.

4.2.2.4.2 Persondataloven kap II Alminnelige regler for behandling av personopplysninger

Grunnvilkårene i §§ 8 og 9 forutsettes oppfylt i formell forstand gjennom at behandlingen har forankring i lov. Dette er imidlertid ikke uten videre tilstrekkelig i forhold til EU-direktivet. Den lov det gjelder må i seg selv være forenlig med direktivets krav.

[22] Loven ble endelig vedtatt 29. april 1998 og trådte i kraft 24. oktober samme år.
[23] Se SOU 1997:39, særlig kap 9.

Samtykke fra den registrerte er tilstrekkelig i begge tilfelle. I utgangspunktet kan en imidlertid ikke la praktisering av offentlighet være avhengig av samtykke. At dette kan komme inn i forhold til spredning av personopplysninger gjennom Internett, er en annen sak.

De materielle vilkårene som oppstilles i §§8 og 9, bygger på EU-direktivet art 7 og 8. Etter art 7 nr 3 (jf loven § 8 bokstav d) er behandlingen av ikke-sensitive personopplysninger tillatt dersom det er nødvendig for å utføre en oppgave av allmenn interesse. Praktisering av offentlighetsprinsippet er en slik oppgave.

Etter direktivet art 8 (jf loven § 9) er det sterke begrensninger for adgangen til å behandle sensitive personopplysninger, slik dette begrepet er definert i loven § 2 nr 8 jf direktivet art 8 nr 1. Alternativene i § 9 bokstav c-h vil ha begrenset rekkevidde for vårt formål. Direktivet art 8 nr 4, jf loven § 9 tredje ledd, tillater imidlertid slik behandling når det er fastsatt i lov og det skjer av hensyn til viktige samfunnsmessige interesser. At innsamling, oppbevaring og utlevering av personopplysninger kan skje i overensstemmelse med offentlighetsprinsippet og arkivhensyn, er en viktig samfunnsmessig interesse. Det norske lovutkast er utformet litt annerledes enn EU-direktivet, i det § 9 tredje ledd forutsetter Datatilsynets godkjennelse i slike tilfeller. Det er imidlertid rimelig å tolke § 9 slik at dette ikke gjelder dersom behandlingen er hjemlet i lov, jf § 9 første let i lov og det skjer av hensyn til viktige samfunnsmessige interesser. At innsamling, oppbevaring og utlevering av personopplysninger kan skje i overensstemmelse med offentlighetsprinsippet og arkivhensyn, er en viktig samfunnsmessig interesse. Det norske lovutkast er utformet litt annerledes enn EU-direktivet, i det § 9 tredje ledd forutsetter Datatilsynets godkjennelse i slike tilfeller. Det er imidlertid rimelig å tolke § 9 slik at dette ikke gjelder dersom behandlingen er hjemlet i lov, jf § 9 første ledd og det skjer av hensyn til viktige samfu*utlevering* av slike opplysninger med mindre det er gitt samtykke. Dette må anses som et adekvat beskyttelsestiltak. I forhold til Internett-offentlighet, vil det være aktuelt med begrensninger utover hva som følger av offentlighetsloven i dag, jf nedenfor under kap 4.3.

Den behandling, herunder eventuelt utlevering, av sensitive personopplysninger som skjer i henhold til offentlighetsprinsippet og arkivhensyn, er etter direktivet art 8 nr 6 en ordning som skal meddeles EU-kommisjonen.

Etter persondataloven § 11, jf direktivet art 6, er det bl a krav om at opplysningene bare skal nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, og ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker. Opplysningene skal dessuten ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen. Praktisering av offentlighet, også etter at en sak er ferdigbehandlet, må anses som en del av formålet med forvaltningens virksomhet i vid forstand. Det samme gjelder arkivering av forvaltningens dokumenter, som er en meget viktig kilde til historisk forskning og må ses som en del av den nasjonale kulturarven. Dette dekkes også av § 11 siste ledd om senere behandling for historiske, statistiske eller vitenskapelige formål, jf direktivet art 6 nr 2. De «nødvendige garantier» som direktivet i disse tilfeller krever, må anses ivaretatt gjennom de nærmere bestemmelser i arkivregelverket og offentlighetsloven.

At opplysningene vil være tilstrekkelige og relevante for formålet med behandlingen (§ 11 første ledd d), vil ivaretas gjennom forvaltningslovens bestemmelser om krav til saksbehandlingen. Det samme gjelder kravet om at opplysningene er korrekte og oppdatert (bokstav e). Rene feilføringer i journalen, skal selvsagt rettes opp om det oppdages. Her er det full harmoni mellom persondataloven og offentlighetshensyn / god forvaltningsskikk. Et annet spørsmål er det hvis uriktige eller ufullstendige opplysninger inngår i forvaltningens saksdokumenter og f eks har blitt benyttet i saksbehandlingen. Disse opplysningene vil ikke kunne oppdateres, i betydningen korrigeres, uten at dette strider mot arkivlovgivningen. Også feilaktige opplysninger innkommet til eller sendt fra et offentlig organ, skal bevares i autentisk form. Senere dokumenter kan beriktige

opplysningene, men de feilaktige skal ikke fjernes. Dette følger av grunnleggende offentlighets- og arkivhensyn. Slike dokumenter / opplysninger kan f eks tjene som dokumentasjon ved et etterfølgende spørsmål om erstatning, men det har under enhver omstendighet historisk betydning at også feilaktige registreringer som forvaltningen faktisk har basert seg på, ikke elimineres. Bestemmelsen i persondataloven § 27 andre til fjerde ledd, som omhandles nærmere nedenfor, regulerer denne situasjonen.

Persondataloven § 12 setter begrensninger på bruk av fødselsnummer. Fødselsnummer er etter forvaltningsloven § 13 andre ledd ikke et «personlig forhold», og er en opplysning som kan finnes i journalen. Fødselsnummer bør neppe legges ut på Internett-journalen, og innholdet i § 12 kan for såvidt uten større problemer gis tilsvarende anvendelse. Det synes likevel mer hensiktsmessig at offentlig- / arkivregelverket regulerer dette fullt ut. EU-direktivet art 8 nr 7 forutsetter at det gis regler om fødselsnummer, men setter ikke krav til reglenes innhold.

Reglene i §§13-15, om informasjonssikkerhet, internkontroll og databehandlerens rådighet over personopplysninger bør gis tilsvarende anvendelse.

Lovens § 16 om frist for å svare på henvendelser og § 17 om betaling bør vel gis tilsvarende anvendelse. På disse punkter kan det hevdes at det offentlige bør behandles som andre behandlingsansvarlige etter persondataloven. Langt på vei må innholdet anses ivaretatt gjennom bestemmelsene i offentlighetsloven § 9 og forvaltningsloven § 11 a og offentlighetsloven § 8, og det kan skape uklarhet dersom disse reglene skal gjelde ved siden av persondatalovens regler.

Konklusjonen er at grunnvilkårene i persondataloven §§ 8 og 9 må anses ivaretatt, men det at vi har en offentlighets- og arkivlovgivning som innebærer behandling av sensitive personopplysninger utover de tilfellene som er uttrykkelig tillatt etter direktivet, skal etter direktivet art 8 nr 6 meddeles EU-kommisjonen.

De øvrige relevante bestemmelser - §§ 11-17 – *kan* alle gis tilsvarende anvendelse. Når det gjelder §§ 12, 16 og 17, mener vi det er mer hensiktsmessig at disse spørsmål reguleres i offentlighets- / arkivregelverket.

4.2.2.4.3 Persondataloven kap III Informasjon om behandling av personopplysninger

Tilsvarende bør utgangspunktet være at bestemmelsene i lovens kap III om den behandlingsansvarliges informasjonsplikter gis tilsvarende anvendelse så langt de har relevans. Det skal diskuteres hvorvidt det bør gjøres tilpasninger, og om direktivet gir adgang til det. For å foregripe en konklusjon, er det hensiktsmessig å ta som forutsetning at den informasjon som skal gis i stor utstrekning skjer via journalens hjemmeside på Internett.

§ 18 første ledd skaper ikke spesielle problemer, hvis en tolker bokstav f) slik at det er tilstrekkelig å informere generelt om den form for utlevering av personopplysninger som offentlighetsloven hjemler, herunder eventuelt over Internett. Dette anser vi forenlig med EU-direktivet art 12 nr 1, som krever at informasjon skal gis om mottakerne eller *kategoriene* av mottakere av opplysninger. Oppfyllelse av kravene i bokstav c) og d) må skje i meget generell form.

Oppfyllelse av første ledd bokstav c) og andre ledd bokstav a) må skje ved henvisning til den offentlige journalen, der de konkrete opplysninger og hvor de er hentet fra, vil være tilgjengelige.

Lovens §§19 og 20 jf § 23, jf direktivet art 10 og 11, regulerer informasjonsplikten ved henholdsvis innsamling av opplysninger fra den registrerte og fra andre enn den registrerte

Direktivet gir hjemmel for å tilpasse informasjonen til «de særlige omstændigheter hvorunder oplysningerne indsamles».[24] Ved kravene til informasjonen må en derfor kunne ta i betraktning at det forhold at forvaltningens dokumenter er offentlige, er et grunnfestet og velkjent prinsipp i Norge. I stor grad vil derfor varsling kunne unnlates i medhold av § 19 andre ledd. Det er praktisk sett lite hensiktsmessig, og det synes ikke påkrevd av hensyn til den registrerte selv, å gi individuell informasjon i hvert enkelt tilfelle. For § 19 første ledd c) gjelder tilsvarende som for § 18 første ledd f), jf foran. I en del tilfeller vil innsamlingen av opplysninger være fastsatt ved lov, og unntak fra informasjonsplikten følger da direkte av § 20 andre ledd a). I andre tilfeller vil informasjon som kommer til forvaltningen ikke være et resultat av en aktiv innsamling, men komme inn ved at noen henvender seg på eget initiativ. Dersom det gjennom en slik henvendelse framkommer personopplysninger om en annen person, vil det i mange tilfeller følge av forvaltningsloven § 17 andre ledd at forvaltningen har en plikt til å forelegge vedkommende disse opplysninger til uttalelse.

I § 23 er det fastsatt en rekke unntak fra retten til informasjon som langt på vei samsvarer med hva som kan unntas fra offentlighet etter offentlighetslovens bestemmelser. Det er således ikke problematisk å gi § 23 tilsvarende anvendelse på Elektronisk postjournal. I den grad retten til innsyn etter offentlighetsloven går lenger enn informasjonsplikten etter persondataloven, følger det av persondataloven § 6 at innsynsretten etter offentlighetsloven går foran.

Bestemmelsen i § 24 om at informasjon kan kreves skriftlig, kan en uten særlige problemer gi anvendelse, også om en tolker dette til et krav om papirform. Det kan oppfylles ved at den samme informasjon som ligger på web-sidene, sendes i papirformat til den som krever det.

Bestemmelsene om informasjonsplikt ved bruk av personprofiler (§ 21) og rett til informasjon om automatiserte avgjørelser (§ 22) har ikke relevans for Elektronisk postjournal.

Konklusjon: Ut fra den tolkning av bestemmelsene som her er lagt til grunn, vil kap III i persondataloven – med unntak for §§ 21 og 22 som ikke har relevans - kunne gis anvendelse i sin helhet, hvilket kan skje gjennom en henvisningsbestemmelse i offentlighetsloven. For praktiske formål vil informasjonsplikten etter kap III kunne ivaretas gjennom at relevant informasjon er tilgjengelig på web-sidene. Herunder må det informeres om at opplysninger som kommer inn til forvaltningen blir journalført og gjort offentlig, også via Internett. Det bør informeres om Internett-publisering også via andre kanaler, særlig i en første fase. Dette ivaretas best gjennom generell statlig informasjonsvirksomhet.

4.2.2.4.4 Persondataloven kap IV Andre rettigheter for den registrerte

§§ 25 og 26 har ikke relevans.

Reglene i § 27 om retting av mangelfulle opplysninger, er gitt en slik utforming at de – i hvert fall må man anta at det vil gjelde i de aller fleste tilfeller - er forenlige med offentlighets- og arkivhensyn, jf § 11 e) som er omtalt under pkt 4.2.2.4.2 foran. Det kan på rettspolitisk grunnlag reises spørsmål ved om Datatilsynet bør ha adgang til å beslutte at retting skal skje ved sletting, på tvers av arkivlovens bestemmelser og Riksarkivarens syn i den konkrete sak, jf § 27 tredje ledd.[25] Dette er det ikke grunn til å gå nærmere inn på her. I vår sammenheng er det tilstrekkelig å konstatere at lovutkastet har vurdert arkiv-/offentlighetshensyn opp mot personvernhensynene og harmonisert regelverket.

Forbudet mot å lagre unødvendige personopplysninger i § 28 henger sammen med § 11 e) jf foran. I første ledd er det uttrykkelig vist til at oppbevaring kan skje hvis det følger av

[24] Dansk oversettelse, gjengitt som vedlegg 1 i Ot prop nr 92 1998-99, på s. 148 flg

[25] Ytringsfrihetskommisjonen er kritisk til dette, se NOU 1999:27 på s.110.

«arkivloven eller annen lovgivning». Også § 28 har en bestemmelse som i siste instans gir Datatilsynet kompetanse til å beslutte sletting, etter krav fra den registrerte og på tvers av arkivlovens bestemmelser og Riksarkivarens uttalelse. Vi begrenser oss også her til å konstatere at lovutkastet har vurdert arkiv-/offentlighetshensyn opp mot personvernhensynene og harmonisert regelverket.

Konklusjonen er at kap IV bør gis tilsvarende anvendelse, med unntak for §§ 25 og 26, som ikke har relevans.

4.2.2.4.5 Persondataloven kap V Overføring av personopplysninger til utlandet

Internett-offentlighet innebærer at opplysninger blir tilgjengelig globalt, og er således å regne for en overføring til utlandet. Lovens utgangspunkt er, i tråd med EU-direktivet, at overføring av personopplysninger bare kan skje til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført EU-direktivet oppfyller dette krav.

Internett-publisering innebærer at opplysningene blir tilgjengelig i stater som har et svært mangelfullt regime for persondatasikkerhet. I § 29 andre ledd heter det imidlertid at det ved vurderingen skal legges vekt på bl a opplysningenes art og behandlingens formål. I dette tilfellet dreier det seg om opplysninger som skal være offentlige, og uhindret av hovedregelen vil kunne gjøres tilgjengelig i et hvert fall i hele EU/EØS-området. I denne situasjonen er det ikke noen betenkeligheter knyttet til at opplysningene er tilgjengelige også utenfor dette området. Denne tolkningen må anses forenlig med direktivet.

For øvrig har utkastet § 30 første ledd h) en særregel for tilfeller der det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register. Dette vil ha anvendelse på foreliggende tilfelle.

Konklusjonen er at kap V vil være tilfredsstilt. Noe behov for å gi disse bestemmelsene anvendelse ved henvisning eller innarbeiding, foreligger ikke.

4.2.2.4.6 Persondataloven kap VI Melde- og konsesjonsplikt

Etter persondataloven § 31 vil den elektroniske journalen i utgangspunktet være undergitt *meldeplikt* til Datatilsynet. Etter EU-direktivet art 18 nr 3 er det imidlertid adgang til å unnta fra meldeplikten et register «der ifølge lover eller administrative bestemmelser er beregnet til at informere offentligheten, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.»[26] Dette vil omfatte foreliggende tilfelle, og det er derfor en nærliggende mulighet at regjeringen benytter sin forskriftskompetanse etter persondataloven § 31 fjerde ledd til å gjøre unntak fra meldeplikten for journaler som omfattes av offentlighetsloven og arkivloven.

En reell begrunnelse for å la meldeplikten få anvendelse her, kan være at den ivaretar det hensyn at man da på ett sentralt sted, dvs hos Datatilsynet, kan få en fullstendig oversikt over hvem som behandler personopplysninger og de andre opplysninger som melding skal inneholde, jf persondataloven § 32. Det følger av § 42 tredje ledd nr 1 at tilsynet skal føre «en systematisk og offentlig fortegnelse» over innmeldte behandlinger. Det kan dog ikke sees at dette moment er særlig tungtveiende i forhold til offentlig journal etter offentlighetsloven, og det er vel også begrunnelsen for unntaksmuligheten etter EU-direktivet.

Konsesjonsplikt vil, uansett eventuelt innhold av sensitive personopplysninger, ikke gjelde hvis registeret opprettes ved egen lov, jf persondataloven § 33 nest siste ledd. EU-direktivet er ikke til hinder for denne ordning.

[26] Se noten foran.

Konklusjonen er at det bør gjøres unntak fra meldeplikten ved forskrift etter § 31 fjerde ledd. For øvrig har bestemmelsene i kapitlet ikke betydning, forutsatt at Internett-offentlighet gjøres til gjenstand for regulering i egen lov.

4.2.2.4.7 Persondataloven kap VII Fjernsynsovervåking

Kapittelet har ikke relevans her.

4.2.2.4.8 Persondataloven kap VIII Tilsyn og sanksjoner

De generelle bestemmelser om Datatilsynets og Personvernnemndas organisering og oppgaver i §§ 42 og 43 gjelder naturligvis. Det samme er tilfelle for bestemmelsene om tilgang til opplysninger og om taushetsplikt i §§ 44 og 45. Det er intet behov for å henvise til eller innarbeide disse bestemmelsene i annen lov.

Det er imidlertid i noen grad grunn til å problematisere reglene vedrørende tilsyn og sanksjoner.

Datatilsynet er gitt en generell påleggskompetanse i persondataloven § 46. I den utstrekning bestemmelser i persondataloven gis anvendelse for Elektronisk postjournal, antar vi det i utgangspunktet vil følge at Datatilsynet også kan gi pålegg til den ansvarlige om endring eller opphør av ulovlige behandlinger, herunder at det settes vilkår for behandlingen.

Ot prop'en (s. 134) forutsetter at pålegg også kan rettes mot offentlige organer «i den utstrekning ikke konstitusjonelle grunner er til hinder for dette.» Pålegg kan ikke gå ut på strengere regulering enn det som følger av loven, men i den grad lovens bestemmelser er skjønnsmessige forutsettes det i proposisjonen (samme sted) at pålegg i praksis vil kunne innebære en presisering av lovtekstens nærmere innhold «innenfor rammen av ordlyden i de ulike bestemmelsene.»

Etter vårt syn er det motforestillinger forbundet med å gi Datatilsynet en slik påleggskompetanse på offentlighets-/arkivlovgivningens område, utover det som er uttrykkelig fastsatt i lovutkastet §§ 27 og 28. Det kan heller ikke sees å være behov for det.
I motsetning til det aller meste av den behandling av personopplysninger som persondataloven omfatter, er det her tale om et regelverk med en sterk og prinsipiell rettslig forankring. Hvis vi forutsetter at det gis gjennomarbeidete særregler i lovs form, basert på avveining mellom offentlighets-/arkivhensyn mot personvernhensyn, bør det behandlingsansvarlige forvaltningsorgan selv kunne håndtere de avveiningsproblemer som likevel kan tenkes å oppstå. Regimet for overprøving og kontroll bør her være det samme som gjelder etter offentlighetsloven i dag. I den forbindelse bør det framheves at Sivilombudsmannen på dette området har en viktig rolle som rettssikkerhetsgaranti.

Datatilsynet har også, etter § 47, kompetanse til å fastsette tvangsmulkt ved pålegg etter §§ 12, 27, 28 og 46. Vi har ovenfor foreslått at § 12 (om fødselsnummer) ikke gis anvendelse i herværende sammenheng. Dersom heller ikke § 46 gis anvendelse, blir en stående igjen med §§ 27 og 28, der lovutkastet, som foran påpekt, uttrykkelig gir tilsynet kompetanse på arkivlovgivningens område. En må kunne forutsette at det i disse tilfeller i praksis uansett ikke vil oppstå spørsmål om å ilegge tvangsmulkt overfor forvaltningsorganet. Etter dette er det vanskelig å se at det er grunn til å gi § 47 anvendelse i vår sammenheng.

Når det gjelder bestemmelsene om straff, persondataloven § 48, vil en stå igjen med at kun et fåtall av alternativene er aktuelle. Det gjelder ingen av alternativene i bokstav a – d. Det gjelder i § 48 e) henvisningen til §§ 13 og 15 (regler om informasjonssikkerhet og om databehandlers rådighet over personopplysninger). I § 48 f) gjelder det manglende overholdelse av

informasjonsplikten ved innsamling av opplysninger (§§ 19 og 20) og nektelse av å gi Datatilsynet tilgang til opplysninger (§ 44).

I og med at persondatalovens og EU-direktivets utgangspunkt er at loven gjelder på like linje for offentlige og private personopplysningsbehandlere, antar vi at straffebestemmelsene bør gis tilsvarende anvendelse. Som det framgår av ovenstående, må dette antas å ha meget begrenset praktisk betydning.

Når det gjelder bestemmelsene om erstatning, § 49, er det ingen grunn til at ikke denne skulle ha tilsvarende anvendelse. Det bør framheves at bestemmelsen på to relevante punkter innebærer en klar skjerpelse i forhold til det alminnelige (offentligrettslige så vel som privatrettslige) erstatningsansvaret. For det første innføres det et skyldansvar med omvendt bevisbyrde, så fremt personopplysninger er behandlet i strid med loven. For det andre omfatter ansvaret, foruten økonomisk tap, også «slik erstatning for skade av ikke-økonomisk art (oppreisning) som synes rimelig.»

Konklusjonen er at §§ 47-49 bør gis tilsvarende anvendelse. §§ 42-45 vil gjelde uten innarbeidelse / henvisning. § 46 bør ikke gis anvendelse.

4.2.2.5 Hvem bør være pliktsubjekter?

Persondataloven definerer to kategorier pliktsubjekter. Den klart viktigste er *behandlingsansvarlig*, som er tillagt ansvar for å følge opp så å si alle de plikter som er gjennomgått ovenfor. I § 2 nr 4 er behandlingsansvarlig definert som: «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.» Dette tilsvarer i hovedsak registeransvarlig etter dagens lov.

Det andre pliktsubjekt er databehandler, definert i § 2 nr 5 som «den som behandler personopplysninger på vegne av den behandlingsansvarlige». Dette tilsvarer i hovedsak databehandlingsforetak etter dagens lov. Databehandlerens plikter etter loven er begrenset til å behandle personopplysninger i samsvar med det som er skriftlig avtalt med den behandlingsansvarlige og å ivareta krav til informasjonssikkerhet (persondataloven §§ 15 og 13).

Etter dette vil behandlingsansvarlig, så langt det gjelder tradisjonell offentlighet og arkivføring, være den samme som har ansvaret etter offentlighetsloven og arkivloven, nemlig det enkelte forvaltningsorgan. I sammenheng med Elektronisk postjournal betegnes dette organ som informasjonsleverandør, i tråd med terminologien i det avtaleverk som i dag regulerer forholdet mellom aktørene, jf kap 5.4 foran. Rollen som tilsvarer persondatalovens begrep databehandler har Posten SDS, som har en avtale (standardavtale) med den enkelte informasjonsleverandør. Statens informasjonstjeneste (SI) har på statens vegne prosjektansvar for Elektronisk postjournal og framstår på Internett-sidene som ansvarlig. Statens informasjonstjeneste har også inngått avtale med Posten SDS med nærmere regulering av de gjensidige plikter og rettigheter disse i mellom. Aktørenes status er ikke vurdert med henblikk på ansvar i forhold til personvernlovgivningen, hvilket er en naturlig følge av at Elektronisk postjournal hittil rent faktisk ikke har blitt trukket inn under denne.

I forbindelse med en regulær ordning med Internett-journal må selvsagt en slik vurdering og klargjøring foretas. Vi ser det slik at det enkelte forvaltningsorgan bør stå som behandlingsansvarlig for all behandling av organets «egne» data også på Internett, herunder for at pliktene til å gi informasjon, foreta retting osv ivaretas. Det betyr også at f eks erstatningsansvar for spredning av uriktig informasjon eller informasjon som ikke skulle vært publisert, påhviler forvaltningsorganet (informasjonsleverandør). Det synes klart at det fortsatt er hensiktsmessig at Statens informasjonstjeneste har en sentral rolle i gjennomføringen av Internett-publisering, men

dette vil da i prinsippet være noe Statens informasjonstjeneste gjør på vegne av det enkelte forvaltningsorgan, enten regulert ved avtale eller gjennom instruksjon fra overordnet forvaltningsorgan, dvs gjennom tildelingsbrev fra Arbeids- og administrasjonsdepartementet.

Alternativet er å gjøre Statens informasjonstjeneste til behandlingsansvarlig for hele Internett-journalen og la hver informasjonsleverandør kun ha behandlingsansvar for sin egen journal, papirbasert så vel som elektronisk, fram til et eller annet punkt i overføringen.

Vi antar dette ikke er hensiktsmessig. Ut fra persondatalovens ståsted, bør behandlingsansvaret i størst mulig grad plasseres i samme organ, jf Ot prop nr 92 på s. 103. Ut fra offentlighetsprinsippet er Internett-offentlighet bare en utvidelse av den tradisjonelle form for offentlighet. Det synes ikke naturlig at ansvarslinjen brytes ved at en bestemt form for praktisering av offentlighet innføres. Endelig synes dette også best i samsvar med prinsippene for statlig informasjonspolitikk, f eks linjeprinsippet om at hver etat er ansvarlig for informasjonsvirksomheten innen sitt fagområde.

Det bør nevnes at hva enten eventuelle feil skyldes Statens informasjonstjeneste eller informasjonsleverandør, er det tale om samme juridiske person, så lenge vi snakker om statlige organer. For den som krever erstatning, vil det for så vidt være av liten betydning om Statens informasjonstjeneste eller informasjonsleverandør har gjort feilen.

Posten SDS, eller en annen aktør som fyller den rollen Posten SDS i dag gjør, vil være databehandler, med sine oppgaver og plikter definert dels ved kontrakt med hver enkelt informasjonsleverandør, dels direkte i persondataloven.

Det kan være litt uklart om Statens informasjonstjeneste gjennom sitt avtalebaserte samarbeid med Postens SDS også måtte defineres som databehandler etter persondataloven. Det er i så fall neppe hensiktsmessig. Alternativet vil være at behovene for avtaleregulering fullt ut ivaretas ved avtaler direkte med informasjonsleverandør, som så engasjerer Statens informasjonstjeneste til å gjennomføre noen av sine plikter (eller at dette reguleres ved instruks, jf over). En del av behovet for avtaleregulering vil falle bort når det gis allmenn tilgang, da gjeldende avtaleverk (kalt Hovedavtalen) også regulerer særlige problemer som springer ut av at tilgangen er begrenset. Det er ikke rom for å gå nøyere inn på dette innenfor det foreliggende prosjektets rammer.

4.3 Drøftelse av de kryssende hensyn. Behovet for, og mulige former for, begrensning av tilgangen til Elektronisk postjournal

4.3.1 Hva er utfordringen. Justiskomiteens synspunkter

Tirsdag 12.10 1999 ble en 41 år gammel mann skutt ned og drept av nynazister utenfor sin bolig sør for Stockholm. Aftenposten skriver (16.10.):

«Drapsmennene har etter alt å dømme kartlagt sitt offer grundig. I forrige måned ble den dreptes passbilde samt personopplysninger bestilt politiets register. Og slik offentlighetsprinsippet praktiseres i Sverige, ble bildet og opplysninger på anmodning sendt til en bedrifts postboks i Stockholm.»

Det kan legges til at postboksen er sporet til nynazistiske miljøet. De aktuelle hendelser i vårt naboland er en sterk påminnelse om hva offentlighetsprinsippet kan misbrukes til, og hva personvernhensyn i ytterste fall kan handle om.

Vi nevner at i Norge innførte man i offentlighetsloven § 6 nr 8 i 1993 en adgang til å unnta «personbilde unntatt i et personregister» fra offentlighet. Regelen kom etter uheldig avisbruk av denne retten i et par drapssaker. Elektronisk postjournal på Internett vil ikke gi noen utvidet mulighet til å innhente fotoer, eller i og for seg noen andre enkeltopplysninger enn de det fra før er adgang til å utlevere. Det vil likevel gi vesentlig utvidet faktisk mulighet for å skaffe seg slike opplysninger.

Basert på innhold, grensesnitt og funksjonalitet som en har for Elektronisk postjournal under forsøksordningen i dag, kan de prinsipielt viktigste forskjellene mellom den form for journalinnsyn som offentlighetsloven forutsetter og en allment tilgjengelig Elektronisk postjournal på Internett, punktvis oppsummeres som følger:

- Internett-publisering betyr en dramatisk økt mulighet for raskt og enkelt å finne fram til informasjon fra journaler, og derigjennom også sammenstille informasjonsbiter fra ulike journalinnføringer, slik at journalene i seg selv gir økt informasjon.
- Uansett om selve saksdokumentene ikke er tilgjengelige på Internett, vil systemets brukergrensesnitt sammen med offentlighetslovens alminnelige bestemmelser om praktisering av innsynsreglene, gi dramatisk økt mulighet for å finne dokumenter en har interesse for, identifisere dem på en slik måte at offentlighetslovens individualiseringskrav er oppfylt, og å få dokumentene tilsendt.
- Offentlighetsloven forutsetter at det kommer en konkret henvendelse om innsyn som avgjøres av forvaltningsorganet i hvert enkelt tilfelle. Selv om retten til innsyn i offentlige journaler (nødvendigvis) gjelder journalen i sin helhet, og ikke er betinget av individualisering av saken slik som ved dokumentinnsyn, ligger det en betydelig reell forskjell i at journalen ligger åpen for alle med tilgang til Internett, uten at en behøver å henvende seg til forvaltningen.
- Internett-publisering betyr at det blir mulig å nedlaste opplysninger til annet elektronisk medium og krysskjøre opplysninger i journalen med elektronisk lagrede opplysninger fra andre kilder.
- Internett-publisering betyr at opplysninger blir tilgjengelig over hele verden, og altså at de også blir overført til utlandet uten at det blir noen særskilt mulighet til å ha kontroll med dette.

I hvert fall de tre første punktene må sees som klart positive om en utelukkende ser det ut fra et offentlighets- og informasjonssynspunkt. Det har entydig framkommet ut fra de intervjuer og den kartlegging som er gjort under prosjektarbeidet, at Elektronisk postjournal er et meget nyttig verktøy for pressen i dag, og at det er et svært verdifullt bidrag til å realisere offentlighetsprinsippet. Det gir en unik mulighet bl a til å følge utviklingen av en sak over tid, til å kartlegge vesentlige spørsmål vedrørende offentlig politikk og forvaltning som behandles på tvers av forvaltningsorganer. Det forhold at den elektroniske journal gjør innhenting av informasjon så mye raskere enn det papirbaserte alternativet har også en kvalitativ side, både ved at det gjør det lettere å omtale saker når de er aktuelle og ved at det totalt sett gjør det mulig å skaffe et mye bedre informasjonsgrunnlag innenfor gitte ressursrammer. Dette er det fundamentalt å ha med seg i den videre diskusjon.

Det er også andre brukere eller potensielle brukere som kan framheves. Advokater som opptrer på vegne av klienter overfor forvaltningen, vil kunne orientere seg både om forløpet av den enkelte sak og om behandlingen av tilsvarende saker i forvaltningen, noe som kan være relevant som rettskilde f eks i forhold til spørsmål om prinsippet om likebehandling er ivaretatt, og under enhver omstendighet vil det kunne ha informasjonsverdi. Forskere på ulike felter vil kunne ha stor nytte av journalen, ikke bare de som forsker på forvaltningen som sådan, men også forskere på saksområder som det offentlige innehar informasjon om. Frivillige organisasjoner som forsøker å påvirke offentlig politikk, er en viktig potensiell brukergruppe. Det samme gjelder foretak som har kontakt med forvaltningen i enkeltsaker og som også har interesse i å orientere seg generelt om forvaltningens virksomhet på det område en holder på med. Også enkeltpersoner kan ha

samme type interesse. Disse siste eksemplene illustrerer hvordan offentlighetshensynene, og Internett-journal spesielt, kan ligge nært opp til partsoffentlighetshensynene og ses som en måte å sikre gjennomføringen av disse reglene.

Endelig vil vi nevne det offentliges egne saksbehandlere. I hvert fall potensielt synes det klart at en Internett-journal kan være et nyttig hjelpemiddel også innad i forvaltningen. Man kunne tenke seg å ivareta dette ved en Elektronisk postjournal som kun var tilgjengelig for forvaltningen selv, uten at dette kunne anses å være i strid med offentlighetsprinsippet, jf pkt 4.3.2.4 foran, men dette er neppe praktisk å tenke seg. Det er derfor mest realistisk å se hensynet til det offentliges egen bruk som et tilleggsmoment i favør av Internett-offentlighet.

Personvernmessig er det imidlertid betenkeligheter. Utfordringen er naturligvis å finne den riktige balansen mellom offentlighetshensyn og personvernhensyn. Vi viser i denne sammenheng til sitatet fra en enstemmig Justiskomité i denne rapportens punkt 3.2. Dette er tungtveiende synspunkter både i kraft av sitt saklige innhold og hvem de kommer fra.

Man kan si at vår personvernlovgivning, bygger på det syn at enhver spredning av personopplysninger – i hvert fall om det ikke bygger på samtykke - innebærer en aktuell eller potensiell skadevirkning for personen, og at det derfor krever en positiv begrunnelse å tillate det. I det minste vil det for den enkelte være knyttet et ubehag til det forhold at «noen vet noe om deg».[27] Grensen mellom bruk og misbruk er i det perspektiv flytende. Dette videreføres i forslaget til ny persondatalov, som i valget mellom regulering basert på en «misbruksmodell» og «behandlingsmodell» velger den sistnevnte.[28] Dette kan virke overdrevet og «paranoid», i hvert fall om en ser hver enkelt opplysning isolert. Men det er den *totale* spredning av personopplysninger i samfunnet, sammen med de stadig bedrete muligheter til å søke seg fram til, sammenstille og lagre opplysningene, som er hovedbekymringen og som kan føre til at det vi kan kalle «personlighetens rettsvern» blir overtrådt. Problemet må en imidlertid forholde seg til individuelt for hver gang spørsmålet om nye former for behandling / spredning av personopplysninger dukker opp. Det er således ikke noe vektig argument mot en restriktiv holdning å vise til at det allerede er så mange opplysninger tilgjengelig.

Forvaltningens offentlige journaler representerer til sammen en enorm informasjonsbase. I dag er det fortsatt bare en brøkdel av etatene som er omfattet av offentlighetsloven, som er med i Elektronisk postjournal. Riktignok er de fleste departementer med, men bare et mindre antall av de underliggende organer hørende til sentralforvaltningen. Statlig forvaltning på lokalt nivå – så som trygde- og ligningskontorene – er ikke representert, og heller ikke kommuneforvaltningen. Selv om vi her begrenser perspektivet til statsforvaltningen, ligger det an til en betydelig økning i tilfanget til informasjonsbasen. Det må legges til grunn at om en først etablerer dette som en permanent ordning, er siktemålet at den etter hvert skal omfatte alle statsorganer på like linje.

Denne informasjonsbasen vil vokse år for år ikke bare i «bredden», men også i «lengden». I dagens Elektronisk postjournal blir informasjon ikke slettet. Hvis denne ordning skal videreføres på samme måte, vil journalen med tiden bli et omfattende historisk arkiv. Dette anses i personvernsammenheng å være særlig betenkelig. Det er slike historiske arkiv som i særlig grad gir mulighet til å skape personprofiler, og dessuten til å hente fram opplysninger som ellers den enkelte kunne ha regnet med ville «gått i glemmeboken.»

---

[27] Jf The Economist's lederartikkel May 1st –7th 1999 s. 14: «In the future, nobody will know for certain who knows what about them. That will be uncomfortable.» Vi må nesten ta med neste setning i sitatet, selv om dette får stå for Economists egen regning: «But the best advice may be: get used to it.»

[28] Se Ot prop nr 92 (1998-99) på s. 20-21. Det framgår her at departementet ser saklige motforestillinger mot behandlingsmodellen. Imidlertid gjør hensynet til EU-direktivet at man ikke egentlig har noe valg.

Alle mulige former for bruk eller misbruk av personopplysninger kan vanskelig overskues på forhånd. Vi har for det første pressen. Den har selvsagt en legitim rolle i omtale av det som har en allmenn interesse, men så vel journalistiske hensyn som rene salgshensyn kan lett friste til oppslag med bruk av personopplysninger som er belastende for den det gjelder, og kanskje utover det saklige mothensyn berettiger. Videre har vi markedsaktører som benytter personopplysninger for å legge grunnlag for mest mulig effektiv markedsføring av sine produkter eller tjenester. Dette har selvsagt en nyttefunksjon, men kan gå lenger enn vi ønsker. Videre kan vi tenke oss profesjonelle rekrutteringsbyråer som systematisk samler inn personopplysninger fra alle slags kilder og bruker dette. Vi kan tenke oss arbeidsgivere som før en intervjurunde tar en «sveip» gjennom Internett-journalen og finner opplysninger som viser at en søker har hatt en personalsak med sin tidligere statlige arbeidsgiver, kanskje mange år tilbake, eller har engasjert seg overfor forvaltningen i et politisk anliggende som arbeidsgiver er lite begeistret for. Vi kan tenke oss mer eller mindre ubalanserte personer, opphisset av sjalusi eller annen sinnsbevegelse, som systematisk vil forsøke å finne og benytte ufordelaktige opplysninger om sin utvalgte fiende. Vi kan – jf eksempelet fra Sverige – tenke oss opplysninger brukt for å kartlegge eller skade politiske motstandere.

Vi har også hensynet til de ansatte i forvaltningen. Vi kan tenke oss at en part i en forvaltningssak finner ut hvem som er saksbehandler (initialene blir i stor utstrekning ført i journalen, selv om dette ikke er en plikt etter arkivforskriften) og så forsøker f eks å presse vedkommende. En misfornøyd og hevngjerrig part, eller andre for den del, kan dessuten ved å søke på tvers av journalen på initialene til saksbehandler få en samlet oversikt over hvilke saker vedkommende har hatt / har befatning med, en kunnskap som kan tenkes misbrukt på ulike måter.

Man kan også tenke seg misbruk i den form at det sendes inn brev til forvaltningen med opplysninger – riktige eller uriktige – om en person kun i skadeøyemed, nettopp for at de via offentlighetsreglene skal bli tilgjengelige på Internett.

Det er i denne sammenheng viktig å framheve den særlige karakter som det offentliges journaler har. I stor utstrekning kan en ikke selv velge å ikke bli registrert, fordi forvaltningen i kraft av sine lovbestemte oppgaver behandler opplysninger om borgerne og fordi en selv må ta kontakt med forvaltningen i en lang rekke helt nødvendige forbindelser, for å få tillatelser, informasjon, inngi pliktige opplysninger osv osv. Dernest er det *ønskelig* å oppmuntre til kontakt med forvaltningen utover dette, jf det som justiskomiteen er inne på om verdien av borgernes aktive engasjement i samfunnsspørsmål – også ved direkte kontakt med forvaltningen. Hvis Internett-offentlighet fører til at en del borgere unnlater å ta kontakt med forvaltningen, fordi de ikke ønsker å få opplysninger om seg selv spredt på nettet, er dette i så fall en annen form for skadevirkning. Det bør kanskje ikke betegnes som et personvernproblem, men er i hvert fall et demokratiproblem *forårsaket* av mangler ved personvernet. Det er selvsagt ikke mulig å gjøre noen kvalifiserte antagelser om hvilket omfang dette problemet vil kunne få, men det er i hvert fall et moment som hører med i den samlede avveining.

4.3.2 Løsningsforslag

4.3.2.1 Innledning

Til syvende og sist blir det her tale om et valg på et verdibasert grunnlag, der oppfatningene alltid vil variere. Men en kan komme et godt stykke på vei i retning av å klarlegge premissene for valget og redusere området for det verdibaserte valg. Vi begynner med det som synes minst problematisk.

4.3.2.2 Økt behov for kvalitetssikring og informasjonssikkerhet

Det er åpenbart at Internett-publisering gjør det mer alvorlig dersom det forekommer feilføringer i journalen. Det er ikke tvil om at dette forekommer i en viss utstrekning. Feilføring kan for det første bestå i at det journalføres opplysninger som ikke skal journalføres. I vår sammenheng er det her særlig grunn til å peke på faren for at taushetsbelagte personopplysninger uriktig føres i journalen, hvilket selvsagt er i strid med arkivforskriften. Men det vil også være meget uheldig dersom journalen inneholder opplysninger som er taushetsbelagt som forretningshemmeligheter, eller som kan unntas offentlighet etter bestemmelsene i offentlighetsloven §§ 5 og 6, og som derfor heller ikke skal med i journalen etter arkivforskriften § 2-7. Det vil her riktignok sjelden dreie seg om personopplysninger, men det er under enhver omstendighet uheldig at lovens forutsetninger ikke følges, og skadevirkningene ved dette vil generelt være større dersom opplysningene ligger i en Internett-journal.

Feilføringer kan dernest bestå i at det kommer inn direkte uriktige opplysninger i journalen. I den grad dette skyldes feil i «input», dvs i de saksdokumenter som arkivføres, så må det håndteres etter reglene om retting og sletting i etterhånd, jf foran. Arkivets oppgave vil være å føre inn opplysninger på grunnlag av det dokumentet viser. Men feilføringer kan også oppstå i arkivet.

På dette punkt vil det ikke være snakk om endring av de materielle bestemmelser, men om å lage rutiner og eventuelt regler som bedre sikrer mot at feilføringer skjer, herunder at det skjer feil ved den tekniske overføring av informasjonen fram til Internett-publisering, og som sikrer rask korreksjon dersom dette oppdages.

4.3.2.3 Journalen skal ikke gi tilgang til opplysninger som etter arkivreglene forutsettes ikke å være offentlige

Det bør videre være enighet om at det ikke er ønskelig at Internett-journalen, via de søke- og koblingsmuligheter denne gir, skal gi tilgang til opplysninger som etter gjeldende regler kan unntas fra offentlighet, og i særdeleshet skal det ikke innebære at taushetsbelagte opplysninger kommer ut.

Muligheten til enkelt å sammenstille opplysninger på tvers av etatene er et forhold som kan gi slike konsekvenser. Inntil nylig har Justisdepartementet i saker om billighetserstatning ført inn navnet på søker i innholdsfeltet, sammen med stikkordet billighetserstatning. Statens helsetilsyn har derimot lenge hatt den praksis at det i journalen kun føres inn stikkordet billighetserstatning. Når Helsetilsynet skriver til JD om en sak om billighetserstatning, vil saken journalføres hos både avsender og mottaker, og på Internett-journalen vil en lett kunne søke seg fram til journalinnføringen hos mottaker dersom man først har funnet avsenders brev.

Vi tar ikke her opp en diskusjon om det (alltid) er slik at en opplysning om at en person har søkt billighetserstatning er taushetsbelagt. Poenget er at mer innskrenket praksis hos en etat ofte vil ha liten betydning hvis andre etater har en annen praksis. En annen side ved varierende journal-praksis er at summen av opplysninger i journalen blir større enn hver enkelt etats innføring. Ved sammenkobling av innføringer hos avsender og mottaker, kan resultatet bli at det kommer ut opplysninger som ikke skulle vært offentliggjort etter arkivforskriften, selv om hver enkelt innføring i seg selv ikke innebærer noe brudd på forskriften.

Internett-journal gjør det altså vesentlig med en mer enhetlig journalføringspraksis også innenfor rammen av arkivforskriftens bestemmelser.

Dette poenget er særlig viktig å ha for øye dersom man lager et regime med sterkere begrensninger for hvilke opplysninger som skal inngå i en Internett-journal, se nedenfor under pkt 4.3.2.5 og 4.3.2.6.

Det er også påpekt for prosjektgruppen i dets møte med representanter for Finansdepartementet at ved kobling av journalopplysninger om ulike dokumenter kan det framkomme opplysninger om innholdet i regjeringsnotater (r-notater) som ikke skal gjøres offentlig. På dette punkt gir nok arkivforskriften rom for noe ulik praksis. Utgangspunktet er at et r-notat er et internt dokument som kan unntas fra offentlighet i sin helhet, og opplysninger om dets innhold skal derfor ifølge arkivforskriften ikke føres i journalen. På den annen side krever forskriften at registreringen skal fylle kravet om identifikasjon av dokumentet, og at opplysning om «sak, innhold eller emne» skal fylles ut (§ 2-7 d). Det er dessuten uttrykkelig fastsatt at det kun er dersom det er nødvendig av hensyn til lovbestemt taushetsplikt, at dette feltet kan gjøres helt blankt. Det vil sjelden være tilfellet for et r-notat. Utover det minimum at det dreier seg om et (utkast til) r-notat, kan det være rom for å føre også visse opplysninger om temaet. Så vidt det kan sees, er imidlertid de fleste departementenes praksis gjennomgående den at det i innholdsfeltet kun føres inn «Utkast til r-notat».

Et annet forhold er at man via saksnummeret i journalen i en del tilfeller kan finne tidligere dokumenter i samme sak, der det i journalen framkommer flere opplysninger om hva saken gjelder. På denne måten kan en finne ut hva som er temaet for r-notatet. R-notater fra enkelte departementer gis nytt saksnummer, slik at denne koblingen ikke kan finne sted.

Tilsvarende vil kunne gjelde for taushetsbelagte personopplysninger. En sak kan forandre karakter underveis, slik at det på et tidspunkt blir en sak omfattet av taushetsplikt, som en kan ivareta ved anonymisering av journalen. Men på grunn av den «link» som saksnummeret utgjør, vil en kunne lete seg tilbake i dokumentkjeden og slik få fram informasjon som forteller hvem opplysningen gjelder. Summen av tilgjengelige opplysninger vil dermed kunne utgjøre brudd på taushetsplikten, selv om dette ikke er en følge av noen enkelt innføring.

Løsningen på disse spesifikke problemer synes å måtte være at man oppretter en ny sak, og dermed et nytt saksnummer, når en sak endrer karakter på den måten som er beskrevet. Dette er uheldig sett ut fra hensynet til at arkivsystemet skal være et hjelpemiddel til intern saksbehandling, men det vil neppe gjelde et stort antall tilfeller.

4.3.2.4 Likebehandling

Dagens prøveordning innebærer en særbehandling av en begrenset gruppe medlemmer av offentligheten, nemlig massemediene (og heller ikke alle mediene). De som har tilgang til Elektronisk postjournal via passord, må sies å ha fått et informasjonsprivilegium. Slike informasjonsprivilegier for mediene eller andre enkeltgrupper kan vanskelig forsvares med bakgrunn i offentlighetsprinsippet. Dette prinsipp forutsetter tvert i mot at rett til innsyn i den offentlige forvaltnings saksdokumenter[29] tilkommer enhver i egenskap av samfunnsborger. Mye taler for å se dette prinsipp som så fundamentalt at det kan betegnes som en grunnleggende menneskerettighet eller en grunnrettighet, jf forslaget om å ta dette inn i grl § 100 om ytringsfriheten. Slike grunnrettigheter kan ikke noen ha i større grad enn andre. De må nødvendigvis tilligge alle borgere på like linje.

Det er derfor i høy grad et spørsmål om den prøveordning som nå har eksistert i flere år, bryter grunnleggende med offentlighetsprinsippet. Dette hører det ikke hit å ta stilling til, men vårt syn er i hvert fall at med tanke på en varig og regulær ordning må utgangspunktet være at en ikke kan løse personvernproblematikken ved å begrense tilgangen til visse grupper, mens flertallet stenges ute.

[29] I JDs høringsnotat av august 1999 om endring av offentlighetsloven med forskrifter foreslås dokumentbegrepet utvidet til å omfatte ethvert informasjonsbærende medium.

4.3.2.5 Mulige former for begrensning i innhold mv i Internett-journal. Utgangspunkter

Dette prosjekt skal ikke vurdere endringer i offentlighets-/arkivlovgivningen utover det som måtte være begrunnet i forhold til Internett-publisering. Vi legger derfor til grunn at retten til innsyn i papirbasert journal, og reglene for føring av journal mv, ikke skal innskrenkes eller endres. Det som framstår som et behov, er å utforme et sett av særregler for publisering i Internett-journal. Det vil i så fall innebære at en i prinsippet har to journaler: En som kun offentliggjøres i papirform (at den vil *føres* og *lagres* elektronisk er en helt annen sak) og en som publiseres på Internett.

Et naturlig utgangspunkt er å reise spørsmål om Internett-journalen overhodet ikke bør inneholde personopplysninger i persondatalovens forstand, dvs opplysninger som direkte eller indirekte kan knyttes til en (fysisk) enkeltperson. (Vi holder foreløpig saksbehandlers navn utenfor i denne sammenheng.) En konsekvens av dette ville være at mottaker/ avsender av brev ikke kunne føres i Internett-journalen dersom dette var en fysisk person. (At person A har sendt et brev til Y-departementet er i seg selv en personopplysning.) En annen konsekvens ville være at navn eller andre identifiserende kjennetegn måtte utelates fra innholdsfeltet i journalen, også utover de tilfeller der taushetsplikten kommer inn. Det minnes om at begrepet «personlige forhold» i forvaltningsloven § 13 er adskillig snevrere enn begrepet personopplysning i personregisterloven og persondataloven.

Dette synes å gå for langt. For det første kan det for personer som opptrer på vegne av andre overfor forvaltningen, typisk advokater, ikke være personvernmessige grunner av nevneverdig vekt som taler for at det ikke skal framkomme at disse er avsender eller mottaker av brev om saken. For det andre vil det være tilfeller der personens navn er avgjørende for dokumentets alminnelige interesse, slik som der offentlig kjente personer eller personer som representerer viktige institusjoner skriver til forvaltningen. For det tredje vil det rent generelt være et poeng at forvaltningen ikke framstår som «ansiktsløs», heller ikke i Internett-journalen. Offentlig forvaltning handler i stor grad om saker knyttet til personer, og det er en realitet som bør framkomme. Anonymisering vil også redusere muligheten til å gjenfinne relevante dokumenter. Det ville således innebære et betydelig tap i forhold til offentlighetshensynene om personopplysninger forsvant helt, selv om navn fortsatt er tilgjengelige i papirjournalen.

Når det gjelder initialene til saksbehandler, taler mye for at dette i utgangspunktet ikke er en opplysning som personvernmessige hensyn tilsier ikke skal offentliggjøres. (Og uansett vil en ved henvendelse til arkivet vedrørende en bestemt sak alltid kunne få saksbehandlers navn oppgitt.) Å delta i utøvelse av offentlig myndighet er en offentlig handling, som ikke gir krav på anonymitet, selv om saksbehandler ikke står formelt ansvarlig for forvaltningens beslutninger. Det kan likevel være unntak på visse områder der følelsene og interessene knyttet til forvaltningens avgjørelser er særlig sterke. Men dette lar seg håndtere på en fleksibel måte innenfor rammen av dagens regelverk, da dette en opplysning som etter arkivforskriften ikke er obligatorisk å føre inn i offentlig journal. Med Internett-offentlighet vil det for enkelte forvaltningsorganer, eller avdelinger innen disse, kunne være grunn til å vurdere en annen praksis med hensyn til å føre inn saksbehandlers initialer i journalen. Men av hensyn til journalens verdi som internt arbeidsverktøy for forvaltningen, bør initialene alltid figurere i den journalen som benyttes internt på arkivet.

En annen type begrensning som kan gjøres, er i tråd med det som Datatilsynets konsesjon til Fylkesmennene er basert på, nemlig at det settes en grense i tid for hvor lenge journalinnføringer skal ligge på Internett. Datatilsynet har for Fylkesmennene satt grensen ved 3 måneder. Et argument for en slik begrensning er at en da unngår å gjøre tilgjengelig et historisk arkiv,

samtidig som offentlighetens interesse for innsyn primært vil gjelde de aktuelle saker. Det er muligens et poeng at den alminnelige høringsfrist etter utredningsinstruksen er på 3 måneder.

Vi ser likevel en 3-månedersgrense som et for sterkt inngrep i forhold til offentlighetshensynene. Det har klar verdi, både for mediene og for andre brukere at journalen går lenger tilbake i tid, selv om det er riktig at verdien vil reduseres jo lenger tid som går. Det er et motargument mot enhver form for tidsbegrensning at det meget enkelt vil kunne omgås ved systematisk nedlasting av det som publiseres. Det lar seg gjøre å legge inn tekniske hindre som vanskeliggjør slik nedlasting, men slike hindre vil alltid kunne overkommes. Vi ser imidlertid ikke dette som et avgjørende argument. Ved at en samtidig innfører et forbud mot slik nedlasting, vil en i hvert fall avskjære de seriøse aktørene. Opplysning om dette forbudet bør kunngjøres på hjemmesidene. Pressen vil kunne få særskilt tillatelse til å nedlaste data og bygge opp sitt eget register, i tråd med de begrensede regulatoriske krav som stilles ved behandling av personopplysninger for journalistiske formål, jf persondataloven § 7.

Samlende tror vi en oppnår det beste kompromiss ved en kombinasjon av tidsbegrensning og innholdsbegrensning i Internett-journalen. Dersom journalen ikke inneholder personopplysninger, er det ikke personvernmessige betenkeligheter ved et historisk Internett-arkiv.

4.3.2.6 Forslag: Kombinasjon av begrensninger i tid og innhold

Avsender / mottakerfeltene:

- Alle navn på fysiske personer i disse feltene gjøres utilgjengelig på Internett etter 12 måneder. Det kan skje ved sletting av navn i basen eller ved et filter som hindrer søking på og visning av navn. Man fjerner da samtidig navn på advokater som representerer parter, hvilket personvernmessige hensyn i og for seg neppe kan sies å begrunne. På den annen side er det neppe særlig tungtveiende offentlighetshensyn som tilsier at advokaters navn ligger på Internett-journalen uten tidsbegrensning. Rent teknisk vil det være vanskelig ikke å ha en konsekvent linje på personnavn i dette feltet.

- Det innføres og publiseres på Internett-sidene forbud mot nedlasting av eldre (ikke-anonymiserte) innføringer.

Det ville i og for seg være ønskelig at den enkelte kunne gi samtykke til at ens navn kunne ligge lenger, eventuelt overhodet *ikke* slettes. Det vil imidlertid være vanskelig å forene med en «filter-løsning». Det vil uansett løsning innebære et teknisk-administrativt merarbeid og dessuten en kilde til feil. Konklusjonen er at fordelen er for liten til at det oppveier ulempene.

4.3.2.7 Sak-/innholdfeltene

Arkivforskriften krever ikke entydig at både sak- og innholdsfelt skal fylles ut. Noen etater praktiserer likevel dette. I så fall er det innholdsfeltet som kan inneholde personopplysninger.

Hvis vi forutsetter:

- at det skjer en innskjerping i forhold til overholdelse av allerede gjeldende regelverk vedrørende sladding av opplysninger som ikke skal offentliggjøres, særlig opplysninger om «noens personlige forhold»,
- at avsender / mottakerfeltet anonymiseres som beskrevet foran,

vil det i svært liten grad forekomme opplysninger i dette feltet som kan knyttes til person.

Det bemerkes her at kriteriet «noens personlige forhold» er så vidt skjønnsmessig at det i grensetilfeller kan være grunn til å legge vekt på at opplysningen blir publisert på Internett, og ikke bare på papir. Det kan altså bli tale om en viss justering også i tolkningen av gjeldende regler, ikke bare i praktiseringen av dem.

Å gjennomføre full anonymisering av dette feltet kun med tanke på Internett-journalen vil innebære en ny rutine som må gjennomføres manuelt. Det antas at nytten ved dette ikke står i forhold til kostnaden. Det minnes om at i forhold til foreliggende problemstilling er ikke spredning av en og annen personopplysning problemet, men at det gjøres tilgjengelig en ny base med en stor mengde personopplysninger. Dette vil en unngå med foreslåtte ordning.

Konklusjonen er at det ikke innføres særregler for anonymisering av dette feltet utover det som allerede gjelder. Det er i så fall grunn til å evaluere dette etter noen tid.

4.3.2.8 Feltet med saksbehandlers initialer

Her krever ikke arkivforskriften at disse tas med i offentlig journal, men dette praktiseres i stor utstrekning i dag. Dette er en praksis som etter vår vurdering i all hovedsak bør fortsette, ut fra det synspunkt at det her gjelder vedkommende persons rolle som deltaker i offentlig myndighetsutøvelse, slik at personvernhensyn må stå tilbake. Det kan likevel i enkelte tilfeller eller for enkelte saksområder være grunn til å legge større vekt på hensynet til å beskytte vedkommende person. Denne vurdering kan den enkelte etat foreta innenfor rammen av gjeldende regelverk, og det er da relevant å legge vekt på at initialene vil bli publisert i Internett-journal, og ikke bare imidlertid papirformat.

5. Vurdering av prosjektet i forhold til de sikkerhetsmessige og tekniske krav

5.1 Hensikt og disponering

Hensikten med dette kapittelet er å gi en teknisk og sikkerhetsmessig vurdering av dagens løsning, med fokus på sikkerhet ved overføringene og mulighetene for sladding av opplysninger. Det er hensiktsmessig å gjøre en slik vurdering inndelt i områdene konfidensialitet, integritet og tilgjengelighet.

Konfidensialitet
Med vekt på at sensitiv eller gradert informasjon kun skal være tilgjengelig for autoriserte personer og det må være foretatt en gyldig identifisering og autentisering mot systemet.

Informasjonskvalitet og integritet
Med vekt på at informasjonen må være fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter.

Tilgjengelighet
Med vekt på at tjenesten skal oppfylle brukernes krav til stabilitet slik at aktuell informasjon er tilgjengelig ved behov.

Vi vil i neste kapittel definere hvordan vi måler trusler. I kapittel 5.2. vil vi identifisere trusler og sårbarheter dagens system står overfor. Videre vil vi i kap 5.3.2.1 identifisere og beskrive hvilke krav til sikring som er stilt, både ut fra gjeldende regelverk og ut fra systemets kravspesifikasjon. Vi vil så i kap 5.5 beskrive og vurdere systemet slik det er i drift i dagens pilotprosjekt. Vurderingen tar utgangspunkt i dagens definerte brukergruppe og informasjonsleverandører. I kap 5.6 vurderes så de tekniske og sikkerhetsmessige konsekvensene av at dagens løsning åpnes for allmenn tilgang på brukersiden og at antall informasjonsleverandører økes.

5.2 Målemetoder

5.2.1 Angivelse av trusselens størrelse (skadeomfang)

Her graderes skadeomfang *dersom* en skade inntreffer ved hjelp av adjektiver innen 3 nivåer:

Skadens Omfang	Betydning	Eksempler
A	Alvorlig skade	Uriktige krenkende personopplysninger blir "plantet" i Internett-journalen, tjenesten blir utilgjengelig i flere uker, tjenesten betraktes som upålitelig som presse-kilde
B	Middels skade	Alle postjournaler er tilgjengelig på Internett først 1 uke etter, 20% av journalpostene "forsvinner" uten at det oppdages samme dag, sensitive personopplysninger offentliggjøres hver uke
C	Liten skade	Postjournal for tre arkiver forsinkes i en uke, tjenesten nede én time i løpet av en arbeidsdag, 5% av journalpostene "forsvinner" uten at det oppdages samme dag

5.2.2 Angivelse av sårbarhet

I tabellen under graderes *sårbarhet* ved hjelp av beskrivende adjektiver innen tre nivåer. Sårbarhet defineres som sannsynligheten eller muligheten for at en skade inntreffer *tatt i betraktning* a) den iboende sannsynlighet for at et slik brudd vil inntreffe; b) spesielle omgivelser; c) sterke og svake sider ved virksomhetens sikkerhet og kontrollmiljø.

Sårbarhet	**Betydning**	**Eksempel på sannsynlighet (antall ganger)**
A	Vil trolig inntreffe (sannsynligvis)	2 ganger pr mnd
B	Kan inntreffe (mulig)	4 ganger pr år
C	Lite trolig (usannsynlig)	1 gang hvert 5 år

(Disse brukes for å ha ens sammenlikningsgrunnlag for forskjellige analyser)

Ved skadeomfang eller sårbarhet **A** anses risikoen for høy **(H)**
Ved skadeomfang eller sårbarhet **B** anses risikoen for middels **(M)**
Ved skadeomfang eller sårbarhet **C** anses risikoen for lav **(L)**

Sikkerhetstiltak som foreslås i kapittel 5.7 vil være basert på en analyse av skadeomfang og sårbarhet og gis prioritet Høy, Middels eller Lav.

5.3 Trusselbildet og sikkerhetsfaktorer

5.3.1 Trusselbildet

Vi vil her identifiseres og beskrive ulike trusselfaktorer i forbindelse med elektronisk offentlig postjournal. En trussel definerer vi i denne sammenhengen som «*en hendelse, påvirkning eller fenomen som kan redusere tilgjengelighet, pålitelighet eller evnen til å beskytte data mot urettmessig innsyn i et IT-system eller et nettverk*». En trussel kan defineres ved dens kilde, intensjon, metode og mål.

Et trusselmål er et system, en person, en virksomhet, en prosess eller lignende som kan bli påført en eller annen form for skade. I Elektronisk postjournal er det primært tre trusselmål:

- Omtalte personer: Trusselen mot enhver virksomhet eller individ som omtales i journalen
- Brukere og saksbehandlere : Den spesifikke trusselen mot saksbehandlere og brukere
- Tjenesten Elektronisk postjournal: Trusselen mot den offentlige journalen og funksjonene rundt systemet

I dagens Elektronisk postjournal er det snakk om trussel mot at

- journalinformasjon tilsiktet eller utilsiktet endres, degraderes eller slettes
- følsom informasjon utilsiktet blir tilgjengelig og brukt til utenforliggende formål, herunder sammenstilling av enkeltopplysninger til å bli følsomme personopplysninger
- informasjon helt eller delvis blir utilgjengelig i kortere eller lengere perioder.
- utilsiktet tilgang til andre systemer som følge av åpning av Elektronisk postjournal

Bakgrunnen for truslene kan være bevisste eller ubevisste menneskelige handlinger, manglende handlinger, uforutsette hendelser som feil i maskin- eller programvare og lignende. Erfaringsmessig utgjør imidlertid mennesket det største og viktigste elementet i ethvert trusselbilde. Dette gjelder både mennesker med og uten tilgang til systemet.

Mulige metoder for å påføre trusselmålene skade kan være elektronisk avlytting, tyvkopiering av

data, sletting eller endring av data, sending av falske data, snoking, uautorisert pålogging, spionering, tyveri, hærverk, bevisst påføre systemet overbelastning etc.

Vi vil ikke gå inn på intensjonene bak evt. skadeverk, men det kan tenkes å være økonomisk vinning, skjule handlinger, skaffe konkurransefortrinn, nysgjerrighet, hevn, sabotasje, hærverk, ære, eventyrlyst, etc.

5.3.2 Sikkerhetsfaktorer

Forebyggende sikringstiltak reduserer sannsynligheten for at en realisert trussel gir negative konsekvenser. Sikringstiltak vil bestå av administrative tiltak (prosedyrer, retningslinjer, forskrifter osv), fysiske tiltak (dørlåser, alarmsystemer osv) og tekniske tiltak. Vi skal her beskrive de viktigste administrative og tekniske sikkerhetsfunksjonene som er relevant å diskutere i Elektronisk postjournal. Disse vil inngå i varierende grad i ulike deler av systemet, både i elektroniske og manuelle prosedyrer. Diskusjon rundt de enkelte funksjonene kommer i kapittel 5.6.

Det er hensiktsmessig å gjøre en vurdering inndelt i hovedområdene konfidensialitet, integritet og tilgjengelighet.

5.3.2.1 Integritet

Forklaring relatert til denne sammenhengen
De offentlige elektroniske postjournalene må ikke uautorisert endres etter at de er sendt fra informasjonsleverandøren. Dette gjelder sletting, endring, degenerering eller ødeleggelse av journalene under overføring eller lagring. Noen ganger kan utilsiktede hendelser føre til dette, f eks ved tekniske feil. Det man fokuserer på i denne sammenhengen, er tilsiktede hendelser. De vanligste teknikkene for å sikre informasjonens integritet er autentisering ved bruk av digitale signaturer og kryptering.

Eksempel: Autentisering
Autentisering er validering av påstått identitet. Passord er en svak brukerautentisering, men som likevel er velegnet i mange sammenhenger. Det finnes også sterkere teknikker for dette. Ved autentisering av avsender eller dataopphav benyttes ofte digital signatur.

5.3.2.2 Konfidensialitet

Forklaring relatert til denne sammenhengen
I noen tilfeller kan det være behov for å sikre offentlige postjournaler mot uønsket innsyn, både ved lagring hos informasjonsleverandøren og ved overføring til og lagring hos operatøren. Ved overføring er kryptering er den vanligste teknikken å sikre mot dette på. Ved lagring benyttes ofte aksesskontroll, f eks ved bruk av adgangskontroll, passord og filkryptering.

Eksempel: Ikke-fornektelse
Ikke-fornektelsestjenester er aktuell i forbindelse med elektronisk post og skal sikre at den som utfører en handling, ikke senere skal kunne benekte at handlingen fant sted. De vanligste tjenestene er ikke-fornektelse av opphav, -sending og -mottak.
Ikke-fornektelse av opphav er ikke aktuell i Elektronisk postjournal, da alle brukere av systemet er definert og kjent. Ikke-fornekting av sending og -mottak er imidlertid aktuelle, både i forbindelse med overføring av Elektronisk postjournal fra informasjonsleverandør til operatør. Dette er også aktuelt i forbindelse med overføring av saksdokumenter fra informasjonsleverandør til sluttbruker, men dette blir ikke omtalt nærmere her. Kvitteringsmekanismer og digitale signaturer er velegnede teknikker for å implementere slike tjenester.

5.3.2.3 Tilgjengelighet

Forklaring relatert til denne sammenhengen
Å sikre tilgjengelighet betyr i denne sammenhengen at tjenestene Elektronisk postjournal er mulig å benytte for brukerne. Tilgang til informasjon skal gis etter behov. Både angrep og overbelastning kan medføre lav tilgjengelighet. De viktigste tiltakene mot dette er robuste løsninger som er designet og implementert på en måte som gjør den motstandsdyktig mot overbelastning og angrep. Brannmur er f eks et sentralt tiltak mot angrep. I tillegg er det viktig med gode rutiner og kvalitetssikring i form av driftsovervåkning.

Eksempel: Tilgangskontroll
Tilgangskontroll er å regulere muligheten for å lese, skrive og slette informasjon, samt muligheten for å benytte tjenester. Tilgangen kan bestemmes eksplisitt ved tildeling av rettigheter til enkeltpersoner (autorisasjon), eller ved gruppetilhørighet. Tilgangskontroll kan sikre at kun personer med tjenstlig behov får tilgang til informasjon, programmer og andre tjenester, i det lokale nettverket og Departementsnettet (Depnett), samt at kun registrerte brukere av tjenesten får tilgang til Elektronisk postjournal.
På operatør- og informasjonsleverandørsiden i Elektronisk postjournal brukes brukerbestemt tilgangskontroll, der eieren bestemmer hvilke andre brukere eller grupper av andre brukere som kan få tilgang til dataene, og hvilke rettigheter de får.

Eksempel: Driftsovervåkning
Å foreta en uavhengig gjennomgang og kontroll (revisjon) av systemlogger og -aktiviteter. En auditlogg er et sett med logger som sammenstilt gir dokumentert bevis på aktiviteter. Brukes for å spore originaltransaksjoner til relaterte logger og rapporter. Logger kan benyttes for å spore innbrudd og «haste-rettelser» fra operatøren.

5.4 Sikkerhetsmessige krav til løsningen

5.4.1 Generelt om gradering på informasjon som behandles i Elektronisk postjournal

Departementsnettet (Depnett) er en sammenkobling av departementenes lokalnett. I tilknytning til Depnett har Statens forvaltningstjeneste ansvar for enkelte fellestjenester som blant annet e-post og tilknytninger til eksterne nettverk.

Depnett er beskyttet med tekniske sikringsmekanismer (brannmur og filtrerende rutere), slik at det ikke skal være mulig for brukere tilknyttet andre nett å koble seg direkte opp mot ressurser i Depnett.

Sikkerhetsnivået i Depnett tillater kun behandling av såkalt normalsikret informasjon, dvs. offentlig informasjon, informasjon som er unntatt offentlighet men ikke gradert i henhold til Sikkerhetsinstruksen eller Beskyttelsesinstruksen, og personregistre som ikke inneholder sensitive personopplysninger, jfr.Lov om personregistre mm.

Informasjon som er gradert iht Sikkerhetsinstruksen og Beskyttelsesinstruksen kan altså ikke behandles på systemer tilknyttet Depnett. Heller ikke sensitive personregistre kan behandles med mindre tillatelse er innhentet fra Datatilsynet. Verken Depnett eller Elektronisk postjournal skal derfor behandle informasjon gradert i henhold til Sikkerhetsinstruksen eller Beskyttelsesinstruksen.

5.4.2 Vurdering av eksterne sikkerhetskrav til Elektronisk postjournal

Vedrørende datasikkerhet og tekniske løsninger, må prosjektet forholde seg til en rekke ytre krav, bestemmelser og anerkjente anbefalinger. Vi vil i det følgende belyse de som har eller kan ha betydning for prosjektet.

Overordnede krav, f eks krav til opplæring i IT-sikkerhet, fysisk sikring, adgangskontroll, spørsmål knyttet til etikk og moral, overordnet sikkerhetsorganisasjon, taushetsplikt, bevisstgjøring, krav ved ansettelser og fratredelse, internkontroll etc, forutsettes ivaretatt utenfor Elektronisk postjournal og behandles derfor ikke i denne rapporten.

Vi har vurdert Elektronisk postjournal i forhold til Datasikkerhetsdirektivet[30] / Sikkerhetsloven[31], Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger[32] (Datatilsynet), Overordnet sikkerhetsstrategi for Depnett[33], IT-sikkerhetshåndbok for virksomheter i Depnett[34], Arbeids- og administrasjonsdepartementets veiledning i bruk av elektronisk post[35], Kravspesifikasjon for Noark-4[36] og kommet til at verken dagens løsning eller en løsning basert på allmenn tilgang kommer i konflikt med disse bestemmelsene. Imidlertid er det knyttet usikkerhet til hvorvidt enkelte av disse er tilstrekkelig oppfylt. Disse kravene er listet i vedlegg 6 og er gjenstand for videre diskusjon i kapittel 5.5.

5.4.3 Elektronisk postjournal-spesifikke sikkerhetskrav

Hovedavtalen[37], Leverandøravtalen[38] og Brukeravtalen[39] regulerer krav og betingelser for henholdsvis informasjonsleverandør, operatør og bruker. Avtalene er styrende også for systemtekniske og sikkerhetsmessige krav til Elektronisk postjournal. I vedlegg 5 er alle sikkerhetsrelaterte krav som er identifiserte i Elektronisk postjournal-avtalene listet.

I tillegg forefinnes ulike dokumenter og rapporter som danner bakgrunnsdokumentasjon for prosjektet og løsningen. Disse er listet i vedlegg 8.

5.5 Beskrivelse og vurdering av sikkerhet i dagens løsning

5.5.1 Forutsetninger

I dette kapitlet beskrives tekniske og sikkerhetsmessige sider ved dagens Elektronisk postjournal-løsning, hvordan sikkerhetskravene er oppfylt og hvilke tiltak som ikke er oppfylt.

Innenfor tidsrammene har det ikke vært anledning til å etterprøve den framlagte informasjonen. Det er derfor de enkelte aktørene selv, ved kontaktpersoner, som innestår for at de fremlagte opplysningene om sikkerhetsløsningene er korrekte.

Noen av punktene er omfattende, og kan ikke behandles detaljert innenfor gitte ressursrammer. I

[30] Datasikkerhetsdirektivet, Forsvarets overkommando / Sikkerhetsstaben 1.mars 1998
[31] Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) av 20.03. 1998 nr 10 (ikke i kraft)
[32] Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger (Datatilsynet)
[33] Overordnet sikkerhetsstrategi for Depnett, Statens forvaltningstjeneste 5.mai 1999
[34] IT-sikkerhetshåndbok for virksomheter i Depnett, Statens forvaltningstjeneste 5.mai 1999
[35] Arbeids- og administrasjonsdepartementets veiledning i bruk av elektronisk post, 1995
[36] NOARK-4 Norsk arkivsystem, Funksjonsrettet beskrivelse og kravspesifikasjon, Riksarkivet 1999
[37] Hovedavtale om elektronisk lagring og spredning av mottatt EPJ-informasjon mellom SI og Posten SDS, 1.12.97
[38] Leverandøravtale om elektronisk leveranse og overføring av EPJ-informasjon melloam IL og SDS som tjenesteyter og distributør, 1.12.97
[39] Brukeravtale for Elektronisk postjournal (EPJ), bilag til Hovedavtalen

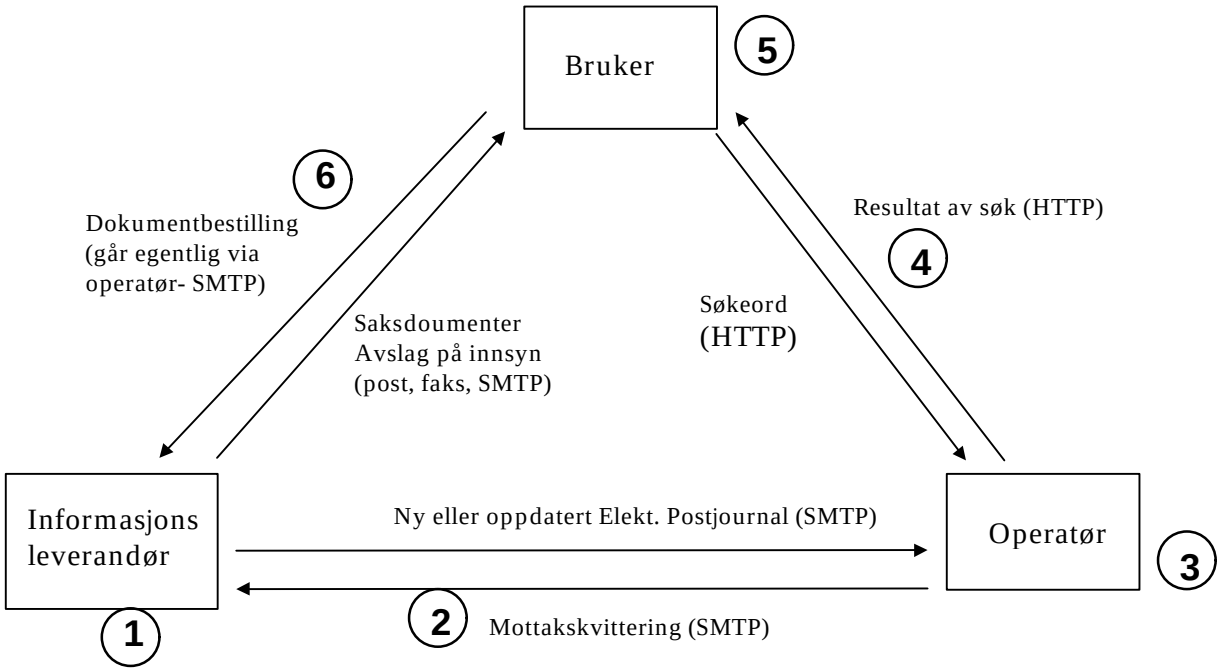
gjennomgangen som er utført, er forhold rundt selve Elektronisk postjournal-løsningen prioritert. Flere områder ivaretas av andre deler av virksomheten, f eks Depnett.

Det er heller ikke gjennomført aktiviteter for å kontrollere samsvar mellom foreliggende retningslinjer og praksis på de ulike punktene.

I vurderingen av hvilke sikkerhetsmekanismer som skal implementeres, må risikoen alltid vurderes opp mot kostnadene.

5.5.2 Informasjonsflyt i Elektronisk postjournal

Ved å ta utgangspunkt i figuren under, vil vi gå gjennom hvert enkelt område for å beskrive hvilke tekniske og prosedyremessige sikringstiltak som er implementert i Elektronisk postjournal. Tekniske detaljer legges i vedlegg. Eventuelt manglende sikkerhetstiltak listes til slutt.



Figur 1: Beskrivelse av informasjonsflyt i Elektronisk postjournal

5.5.3 Systemarkitektur

Elektronisk postjournal ble først realisert som en tradisjonell databaseløsning der kommunikasjon mellom de enkelte aktørene var basert på X.400 og X.25. Senere ble det realisert et Web-grensesnitt, som har gjort databasens innhold søkbart via Internett ved hjelp av en nettleser. Applikasjonen bruker SIFT programmeringsgrensesnitt (API) for lagring og gjenfinning av journalposter.

Posten SDS er operatør for Elektronisk postjournal og ansvarlig for den daglige driften. De har utviklet system for mottak av postjournaler fra informasjonsleverandørene, SIFT-database, ulike konverteringsprogrammer, Web-grensesnitt og rutiner for mottak og håndtering av postjournaler og bestillinger.

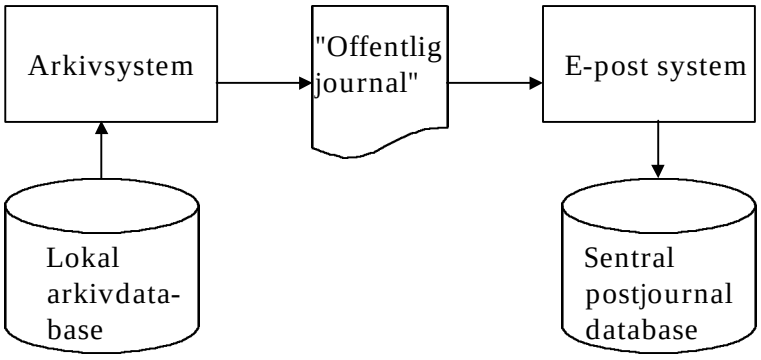
Vurdering:
Overordnet systemarkitektur i dagens løsning er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav. Det synes fornuftig å ha en tjenesteleverandør som

felles operatør for alle departementer og etater. Rollefordelingen med informasjonsleverandør, operatør og bruker synes fleksibel og hensiktsmessig.

Det største potensialet for å forbedre tjenesten, ligger i overgangen til elektroniske saksdokumenter. Dette åpner for elektronisk tilgang til saksdokumenter gjennom hyperkoblinger. Dette krever imidlertid større endringer i dagens systemarkitektur som ikke omtales i denne rapporten.

5.5.4 Sikkerhet hos informasjonsleverandør (1)

Informasjonsleverandørene har rutiner for utsending av den offentlige journalen hver dag. Fra arkivsystemet genereres rapporten "Offentlig journal" til en tekstfil som følger NOARK-standarden. Se figuren under. Sladding/anonymisering av taushetsbelagte personopplysninger gjøres delvis automatisk i arkivsystemet ved påføring av gradering og delvis manuelt i tittelfeltet og avsender- og mottakerfeltet. Filen sendes som vedlegg til e-post til operatøren. Etter at operatøren har mottatt filen med e-posten, konvertert innholdet og lagt postjournalen inn i SIFT-databasen, sendes en mottaksrapport tilbake til informasjonsleverandøren. Mottaksrapporten viser blant annet hvor mange journalposter som ble lagt inn i databasen. Eksempel på mottaksrapport finnes i vedlegg 3.



Rapporten "Offentlig journal" genereres fra informasjonsleverandørens lokale arkivsystem og sendes med e-post til den sentrale elektronisk postjournal-databasen

Den systemtekniske delen av Elektronisk postjournal hos informasjonsleverandørene består utelukkende av felles teknisk infrastruktur og støtteapplikasjoner i virksomhetens lokale datanettverk. Disse er sikret iht «IT-sikkerhetshåndbok for virksomheter i Depnett», uavhengig av Elektronisk postjournal. Dette omfatter all IT-infrastruktur, virksomhetens arkivsystem, tekstbehandlingssystem og elektronisk postsystem. Ingen applikasjoner er utviklet spesielt for Elektronisk postjournal.

Den ikke-tekniske delen består av manuelle rutiner, prosedyrer og organisasjon. Disse er dekket av Elektronisk postjournal-uavhengige retningslinjer for f eks kontorsikkerhet, adgangskontroll, autorisering, opplæring, vedlikehold, kvalitetssikring.

Vurdering:
Funksjonalitet vedrørende sikring av konfidensialitet hos informasjonsleverandøren og tilgangskontroll til informasjonsleverandørens lokalnettverk, arkivsystemet, postsystemet i dagens løsning er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav.

Med utgangspunkt i de sikkerhetsmekanismene som ble definert i kapittel 5.3.2, vil vi likevel vise

til områder som bør ha et høyere sikringsnivå. Områdene er gruppert etter sårbarhet og skadeomfang definert i kapittel 5.2:

Risiko H:

- Tilgang til Elektronisk postjournal vil øke offentlighetens interesse for forvaltningens dokumenter. Journalføringens datakvalitet er derfor av stor interesse. Brukerne karakteriserer den foreliggende datakvaliteten som svært varierende. Det finnes tilfeller der journalposter har "forsvunnet" under oversendelse til operatør. Hos en av informasjonsleverandørene inneholdt ikke arkivsystemet funksjonalitet for å telle antall journalposter som ble generert i postjournalen. Antallet ble heller ikke telt opp før sending. Når mottaksrapporten kom, sjekket mottakeren kun postjournalens dato og ikke antall poster mottatt av operatøren. Informasjonsleverandøren må innføre daglige rutiner og systemer for å kontrollere at det som blir lagt inn i Elektronisk postjournal-databasen, er i overensstemmelse med det som ble sendt og var ment sendt til operatøren.

Risiko M:

- Journalpostene som ved en feil ikke skulle ha blitt sendt en dato, må identifiseres en og en og så manuelt fjernes fra databasen. Dette er en uheldig og tidkrevende prosess som kan unngås ved å innføre journaldato (som beskrevet i NOARK-4) som et eget felt i databasen.
- For å sikre mot at operatøren skal kunne nekte for å ha mottatt en postjournal, bør sendte mottaksrapporter lagres systematisk hos informasjonsleverandøren.
- Det skjer ingen automatisk logging av postjournal-overføringene. For å holde kontroll på hvilke journaler som er sendt og hvilke mottaksrapporter som er mottatt, bør det etableres et system for loggføring. Det bør fremgå av loggen om det gjelder ordinær overføring, re-sending ved feil, oversendelse av rettelse eller nedgraderingsrapport.

Risiko L:

- For å sikre at journalene offentliggjøres så snart som mulig, bør flere personer være autorisert og opplært til å generere, kontrollere og oversende den offentlige journalen.
- Hos informasjonsleverandøren bør standardrapporten "Offentlig journal" genereres iht NOARK-4 definisjonen, slik at alle journaler som sendes til operatøren er like. Dette reduserer risikoen for introduksjon av feil og behovet for manuelle inngrep både hos operatøren og informasjonsleverandøren (f eks sletting av overskytende antall tegn i tittelfelt)
- Elektronisk postjournal bør støtte re-sending av journaler med avgraderte dokumenter (som rapporten «Avgraderingsliste» iht NOARK-4), slik at Elektronisk postjournal-databasen gjenspeiler de endringer som den offentlige postjournalen i vedkommende arkiv påføres etter en avgradering
- For å få en felles standard løsning, Justisdepartementet over fra dagens FTP til e-post
- Informasjonsleverandøren skal alltid ha en separat sikkerhetskopi av den informasjon som leveres til operatøren, og bevare denne i syv dager. Det er usikkert om dette praktiseres hos alle.

Følgende sikkerhetsfunksjoner er vurdert men ikke ansett som nødvendig:
- Sikker måte å validere avsenders påståtte identitet ved mottak av mottaksrapport.
- Konfidensialitetssikring under overføring av journalene til operatøren (det sendes kun offentlig informasjon).
- Sikring av tilgjengelighet under kommunikasjon. (det er umulig å garantere tilgjengelighet på Internett).

5.5.5 Kommunikasjonssikkerhet mellom informasjonsleverandør og operatør (2)

Det er ikke implementert Elektronisk postjournal-spesifikke sikkerhetsfunksjoner ved overføring av data mellom informasjonsleverandøren og operatøren. Kommunikasjonstjenester mellom informasjonsleverandøren og operatøren er dekket av Depnetts elektroniske postsystem og underliggende felles kommunikasjonstjenester i den tekniske IT-infrastrukturen, samt Internett.

Eventuelle sikkerhetstiltak utover dette vil implementeres som ende-til-ende sikkerhetstjenester hos operatør/informasjonsleverandør.

5.5.6 Sikkerhet hos operatør (3)

Operatøren mottar daglig e-post til Elektronisk postjournal-postkassen hvor de elektroniske postjournalene følger med som vedlegg.

Når en e-post kommer inn starter en prosess automatisk der den vedlagte postjournal-filen dekodes, konverteres, legges inn i rette SIFT-database og indekseres. Antall mottatte journalposter telles opp. Det er etablert en databaser per informasjonsleverandør. Det sendes så en rapport til informasjonsleverandøren med e-post med oversikt over hvor mange journalposter SIFT har lest, hvor mange som er importert og hvor mange som evt er forkastet. Formatet på denne rapporten er beskrevet i vedlegg 3.

I denne prosessen sjekkes det for det første at avsender er riktig (at adressen finnes i listen over registrerte informasjonsleverandører) og at postjournal-dato er riktig.

Løsningen ivaretar problemet som kan oppstå i tilfelle samme journal sendes to ganger ved at den forrige sendte journalen overskrives. For at informasjonsleverandørens og operatørens journaldatabase skal være konsistent, skal oppdateringer bare skje ved at ny journal genereres fra arkivsystemet for aktuelle dato og oversendes operatøren, som legger journalpostene inn på nytt.

Sikkerhet i infrastrukturen:
Hos operatøren er sikkerheten i infrastrukturen ivaretatt gjennom sikkerhetskomponenter i det lokale nettverket og i grensesnittet til Internett. Posten SDS har etablert en felles infrastruktur bestående av servere, nettverk, sikre operativsystem, brannmurer, rutere mm som er dimensjonert for Web-tjenesten. Sikkerheten er implementert uavhengig av Elektronisk postjournal og skal hindre hacking av server fra Internett og evt. beskyttelse mot in-sidere.

Det er etablert en brannmur hos operatøren som implementerer aksesskontroll mot tjenesten ved bruk av passord-innlogging.

Autorisering og autentisering av brukeren i operatørens lokale nettverk gjøres ved hjelp av standard sikkerhetsrutiner, som administreres lokalt på serverens operativsystem og på databasenivå.

Sikring av oppetid på web- og databaseserver:
Sikring mot maskinvarefeil i på Web- og databaseserver er løst ved at flere maskiner speiler hverandre (clustering). Hvis en disk eller maskin går ned, vil en annen automatisk ta over. I tilfelle strømbrudd er avbruddsfri strømforsyning (UPS) tilkoblet maskinene.

Operatøren sitter på kompetanse på den teknisk løsning. Supportavtale på maskinvare med oppetidsgaranti finnes. Det er i avtaler mellom driftsleverandør og systemeier avklart hvem som gjør hva i de enkelte feilsituasjonene.

Sikkerhet ved sending og mottak av Elektronisk postjournal -relaterte e-post:
Ved mottak av e-post i Elektronisk postjournal-postkassen sjekkes det for det første at avsender er

riktig, at postjournalen er kommet fram og at riktig postjournal er mottatt. Mottakeradressen og ruting-informasjon i headeren i en e-post fra et arkiv er som regel tilstrekkelig bevis på at e-posten virkelig kommer fra den som står anført som avsender. Helt sikker kan man imidlertid ikke være uten å bruke sterkere autentiseringsmekanismer.

Tilgangskontroll til tjenester og forretningsdata på Web- og databaseserver:
Funksjonell logikk i tjenestene på Web-serveren ivaretar at en bruker ikke skal kunne operere (kun lese) på andre data på Web- og databaseserveren enn de han er autorisert for (offentlige postjournaler). Det ivaretar også at han ikke skal kunne utføre operasjoner han ikke har lov til.

Alle kolonnefeltene i Elektronisk postjournal-databasen har et flagg som angir om i hvilken grad et felt er søkbart. Det opereres med de tre gradene «ikke søkbart» (kun for databaseansvarlig), «kun søkbart i dette feltet» og «søkbar i fulltekst (dvs søkes i hvis et felt ikke er angitt)».

Feltene avsender, mottaker, sakstittel og innhold er fullt søkbare fra Internett. Dette må vurderes nærmere i forbindelse med begrensning av muligheten for å søke på opplysninger om enkeltpersoner.

Vurdering:
Funksjonalitet og komponenter vedrørende sikring av infrastrukturen, oppetid på tjenesten, sending og mottak av postjournaler med e-post, backup og recovery, tilgangskontroll til tjenester og forretningsdata på Web- og databaseserver i dagens løsning er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav.

Med utgangspunkt i de sikkerhetsmekanismene som ble definert i kapittel 5.3.2, vil vi likevel vise til områder som bør ha et høyere sikringsnivå. Områdene er gruppert etter sårbarhet og skadeomfang definert i kapittel 5.2:

Risiko H:

- Database og Web-applikasjon kjører på samme maskin. Dette er uheldig ut fra et sikkerhetsmessig synspunkt. Databasen bør kjøre på en egen server og Web-applikasjonen på en annen med brannmur i mellom.

Risiko M:

- I dagens Elektronisk postjournal har operatøren få muligheter for å verifisere og autentisere avsendere av e-post. I realiteten kan noen utgi seg for å være en informasjonsleverandør og sende falske postjournaler. Rutiner og mekanismer for å verifisere og autentisere avsender bør derfor implementeres
- Operatørens systemer for kvalitetssikring og feilhåndtering av innkommende postjournaler er også tiltak som bør iverksettes. Det bør innføres rutiner og systemer for automatisert sammenstilling og kontroll av innkommende elektronisk post til Elektronisk postjournal.
- Ubevisst eller bevisst endring av data kan føre til omfattende inkonsistens i databasen. Ved å sette opp logger hvor endring av data spores, vil man ha mulighet for å finne ut hvem som utførte endringen og når. Både operativsystemet og ruter bør konfigureres slik at bare navngitte personer fra navngitte maskiner skal ha tilgang til databaseserveren. Ekstern innlogging via Telnet må slås av.
- All e-post og vedlagte filer som mottas i Elektronisk postjournal postkassen må virussjekkes før de behandles.
- Mislykkede påloggingger (på Unix -, DB- og applikasjons nivå) må logges. Loggene må gjennomgås på fastsatte tidspunkter slik at forsøk på innbrudd kan oppdages.

Risiko L:

- Det er ingen sikre mekanismer hos operatøren for å hindre at en avsender skal kunne nekte for å ha sendt en journal. Hvis det skulle bli uenighet om hvorvidt en journal er sendt eller ikke, kan den mottatte e-posten brukes som "dokumentasjon". Denne dokumentasjon er imidlertid ikke sikkert "bevis", det kan være at journalen har en falsk avsender. "Sikkert bevis" får man bare ved at forsendelsen inneholder en digital signatur.
- Backup-rutinene hos operatøren må dokumenteres i drifts- eller brukerdokumentasjon. Vedlegg 7 gir en oversikt over filer som må være med i backupsystemet.
- Databaseserveren bør overvåkes av et overvåkingssystem ved at logger fra maskinen leses. På databasesiden bør tablespace, tabeller, extents osv overvåkes kontinuerlig. Dette for å sikre stabil oppetid på tjenesten.
- Dokumentasjon av rutiner knyttet til Elektronisk postjournal er ikke tilstrekkelig dokumentert i drifts- og produksjonshåndbøker. Operatørens ordinære kvalitetssikringsrutiner skal gjelde.
- Depnett-dokumentene «Geografisk lokalisering og fysisk plassering», «Systemteknisk sikringstiltak» og «Autorisasjonsliste» må forefinnes i Depnett-systemer og bør i noen grad gjelde for operatøren av Elektronisk postjournal. Slik dokumentasjon finnes imidlertid ikke.

5.5.7 Kommunikasjonssikkerhet mellom bruker og operatør (4)

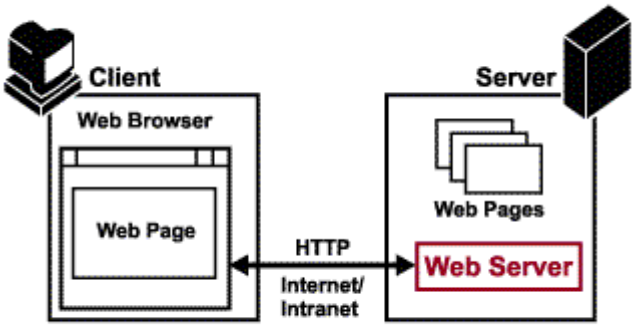
Kommunikasjon mellom brukeren og operatøren skjer via brukerens nettleser og operatørens Web-server ved bruk av protokollene HTTP og TCP/IP. Brukeren angir søkeord og kriterier og sender disse til Web-serveren. Tilbake får brukeren resultat av søket i form av en liste journalposter. Ingen av disse protokollene implementerer spesifikke sikkerhetsmekanismer. Alle HTTP-transaksjonene sendes i realiteten i klar tekst over Internett og de som ønsker å lese, endre eller slette informasjonen, kan i teorien gjøre det. Sannsynligheten for at dette skjer er imidlertid lav.

Kryptering mellom brukerens nettleser og operatørens Web-server (SSL) er ikke implementert i dagens løsning. Det har heller ikke fremkommet krav eller behov for verken autentisering eller konfidensialitetssikring av data som sendes mellom nettleseren og Web-serveren (søkekriterier, resultat av søk, brukernavn, adresser ol).

Vurdering:
Den tekniske og sikkerhetsmessige løsningen på brukersiden er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav.

5.5.8 Sikkerhet hos bruker (5)

I den Web-baserte Elektronisk postjournal-løsning aksesserer brukeren tjenesten på operatørens Web-server fra sin nettleser som vist i figuren under.



Brukeren aksesserer Elektronisk postjournal-databasen på operatørens Web-server fra sin nettleser

Dagens Elektronisk postjournal-løsning er basert på at brukeren er registrert og har fått tildelt brukernavn og passord for at tjenesten skal kunne brukes.

Fra søkeresultatet skal brukerne ha mulighet til å sende bestilling på dokumentkopier til den enkelte informasjonsleverandørs arkiv. Slike bestillinger skal oversendes via e-post til informasjonsleverandørs elektroniske postkasse.

Med den Web-baserte løsningen som pilotprosjektet benytter, ligger nesten all forretningslogikk og grunnlagsdata på operatøres Web-server. På sluttbrukerens lokale maskin vil Elektronisk postjournal-relatert data kun være kode for visning av Web-siden (HTML-kode) og programkode (Javascripts) for logikk knyttet til validering av inndata.

Elektronisk postjournal har en forhåndsdefinert brukergruppe, der hver enkelt bruker er tildelt brukernavn og passord av operatøren. Hvis en sluttbruker røper brukernavn og passord til en annen person, og denne personen benytter dette til å skaffe seg tilgang til Elektronisk postjournal, er ikke brukeren autentisk. Det er vanskelig å sikre autentisitet i slike tilfeller og neppe relevant i dette prosjektet. Ved åpning for allmenn tilgang vil aksesskontroll ved bruk av brukernavn og passord for å få tilgang til nettsiden med Elektronisk postjournal-tjenesten fjernes.

Riktig håndtering av brukernavn og passord, samt avlogging av systemet etter bruk, vil i stor grad sikre mot uautorisert tilgang på sluttbruker-siden. Man ser ikke behovet for sterkere autentisering enn passord.

Det har imidlertid ikke framkommet ønsker om sterkere brukerautentisering på sluttbruker-siden, og det vil derfor i det følgende ikke vurderes alternativer til dette.

Dokumentbestillinger sendes per elektronisk post fra brukeren og til informasjonsleverandøren. Denne e- posten sendes i realiteten i klar tekst over Internett og det er i teorien mulig for andre å lese, endre eller slette informasjonen. Dette krever imidlertid ekspert-kunnskaper og det er vanskelig å se hvilken motivasjon en person skulle ha for å gjøre dette. Informasjonsleverandøren sender tilbake saksdokumenter til person og adresse angitt i dokumentbestillingen. I dag sendes disse med ordinær postgang, eventuelt telefaks. Avslag på innsynsbegjæring sendes med e-post, telefaks eller ordinær post.

Vurdering:
Funksjonalitet vedrørende sikkerhet hos brukeren, er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav.

Med utgangspunkt i de sikkerhetsmekanismene som ble definert i kapittel 5.3.2, anbefales følgende tiltak som vil bedre sikkerheten ytterligere:

- Passordbeskyttelse kan lett skape falsk trygghet dersom ikke disse behandles på en forsvarlig måte. I dag tildeler operatøren brukeren passord første gang og passordet byttes ikke senere. Det bør innføres rutiner for å bytte passord med jevne mellomrom og utarbeides en kort veiledning i valg og håndtering av disse i Brukeravtalen.

Følgende sikkerhetsfunksjoner vært vurdert, men anbefales ikke:

- I forbindelse med klientsikkerhet er det aktuelt å beskytte mot programmer (applets) som kommer f eks sammen med dokumenter, eller virus, kan foreta seg uønskede operasjoner. HTML-filen inneholder Javascripts som inneholder eksekverbar kode. Dette er en sikkerhetsrisiko fordi disse skriptene kan foreta uønskede operasjoner. Imidlertid anses risikoen for dette som lav. Videre vil det være vanskelig å få dette til uten at dette oppdages.

- For å hindre trojanske hester, og for at klienten skal vite hvem som har lagd appleten og at ingen har endret på koden i appleten, kan signerte applets benyttes (JAR-filer i Netscape og CAB-filer i Internett Explorer). Det er ikke stilt krav til slik sikkerhet i Elektronisk postjournal og risikoen og konsekvensene ved denne trusselen anses så lav at det heller kan ikke anbefales å sikre mot dette.

- Java inkluderer mekanismer for å autentiserte (signerte) "applets" kontrollert adgang til ressurser på lokal maskin. Det er imidlertid praktiske problemer knyttet til å ta dette i bruk, blant annet på grunn av kompatibilitetsproblemer, manglende sertifiseringsautoriteter og lokale administrasjon av adgangsrettigheter.

5.5.9 Kommunikasjonssikkerhet mellom bruker og informasjonsleverandør (6)

Brukeren sender sine saksdokumentbestillinger til vedkommende arkiv ved bruk av elektronisk post. E-posten sendes i realiteten via operatøren. All kommunikasjon mellom brukeren og informasjonsleverandør benytter e-poststandarden SMTP og MIME-standarden for inkludering av vedlegg. TCP/IP benyttes som standard transportprotokoll. Ingen av disse standardene implementerer spesifikke sikkerhetsmekanismer.

Vurdering:
Kommunikasjonssikkerhet er i hovedsak i overensstemmelse med kravspesifikasjonen og andre relevante krav.

Likevel kan følgende bemerkes:

- Elektronisk post basert på SMTP mangler tilfredsstillende kvitteringsmekanismer. F eks kan man ikke være sikker på å få tilbakemelding fra nettverket i tilfelle feil oppstår under under overføring. Det finnes tilfeller der bestillinger har "forsvunnet" oversendelse til informasjonsleverandør. Dette fordrer at det innføres rutiner hos avsender og mottaker som oppdager og håndterer slike feilsituasjoner.

5.5.10 Spesifikt vedrørende håndtering av feil i Elektronisk postjournal-databasen

Det har framkommet en viss bekymring for at feil eller mangler i de offentlige journalene som allerede er lagt inn i operatørens database, ikke lar seg rette opp i ettertid.

Årsakene til feilene eller manglene det vises til kan, være følgende:

- Et saksdokument (og dermed også journalen) inneholder gale opplysninger
- Et saksdokument som ikke skulle ha vært ført i offentlig journal, blir det
- Arkivet glemmer å sladde personopplysninger i den elektroniske offentlige journalen
- Arkivet sender feil journal til operatøren (dette har faktisk skjedd)
- Datofeltet i en journal inneholder amerikansk datoformat
- Det oppstår filfeil under dataoverføring fra arkivet

Dagens rutiner for å oppdatere informasjon i SIFT-databasen, er å sende oppdatert postjournal for den aktuelle datoen. Et program (cron-jobb) hos operatøren leser alle innkommende e-poster fra informasjonsleverandørene. Hvis en tidligere oversendt journalpost sendes på nytt, vil den gamle bli slettet fra databasen og den nye legges inn.

Saksnr og Doknr danner nøkkelen til en journalpost i dag. Et vesentlig problem med dette er at det ikke er mulig å identifisere alle de postene som er lagt inn en spesifikk dato. Dette gjør at de journalpostene som ved en feil ikke skulle ha blitt sendt en dato, først må identifiseres og så manuelt fjernes fra databasen. Dette er en tidkrevende prosess som kan unngås ved å innføre journaldato (som beskrevet i NOARK-4) som et felt i journalposten. Da kan alle journalposter for en spesifikk dato på en enkel og sikker måte fjernes fra databasen og den nye postjournalen legges inn på nytt.

At annet problem med dagens løsning for oppdatering av tidligere sendte journalposter, er at de endrede journalpostene legges inn i begynnelsen av databasen isteden for på samme plass som opprinnelig ble lagt inn på. Dette medfører feil i den kronologiske rekkefølgen i databasen, slik at brukeren ved kronologisk blaing vil få de "gamle" oppdaterte journalposter listet blant nye.

Vurdering:
Metoden med å overføre postjournalen for en hel dag hver gang en journalpost skal oppdateres, er i utgangspunktet en ryddig måte å oppdatere databasen på.

Imidlertid kan følgende bemerkes:

- Feltet Journaldato (som beskrevet i NOARK-4) må inn som et felt i journalposten og databasedefinisjonen, slik at man ved oppdatering/korrigering av en postjournal for en dag, entydig kan identifisere alle journalposter for denne dagen.
- Oppdaterte journalposter må vises på samme kronologiske plass også etter en eventuell oppdatering.
- Rutinene rundt oppdatering/korrigering av tidligere innlagte journalposter må dokumenteres bedre i driftsdokumentasjonen.
- Det må tas stilling til hvordan avgraderinger (jfr. Avgraderingsliste i NOARK 4) skal behandles hos informasjonsleverandørene.

5.6 Vurdering av fremtidig løsning for Internett-journal

I en fremtidig løsning ser man for seg tre funksjonelle utvidelser av Elektronisk postjournal; utvidelse av antall informasjonsleverandører, utvidelse av brukergruppen og elektronisk tilgang til saksdokumenter.

Dagens tekniske løsning må utvides på en rekke områder for å støtte slike utvidelser og kommer i tillegg til de tiltak som allerede er foreslått implementert i dagens løsning.

5.6.1 Utvidelse av brukergruppen

En utvidelse av brukertilgangen (fra dagens 82 redaksjoner til åpne tilgang) kan enten gjøres ved at tjenesten gjøres allmenn tilgjengelig uten kontroll på hvem som aksesserer tjenesten, eller at dagens brukerbestemte tilgangskontroll beholdes og antall brukere økes. I det følgende vurderes den første utvidelsen; Elektronisk postjournal som en åpen tjeneste på Internett.

Elektronisk postjournal er i dag tilgjengelig på en Web-server og en åpning for allmen tilgang er i utgangspunktet teknisk enkel oppgave. Imidlertid vil det være behov for å øke kapasiteten på Web- og databaseserver for å kunne håndtere en økning i antall samtidige brukere som aksesserer tjenesten. Dagens SIFT-database kan håndtere et ubegrenset antall samtidige transaksjoner i lesemodus fra Web. Begrensningen ligger derimot i antall samtidige prosesser som kan kjøres samtidig på Web-serveren, slik serveren må dimensjoneres etter hvor stor pågang det blir til tjenesten.

Vurdering:
Dagens Elektronisk postjournal-løsning er mulig å utvide til en åpen løsning. Utvidelsen vil få betydning for både operatøren og informasjonsleverandørene.

Følgende forhold må tas i betraktning:

- En åpen løsning gjør at det generelt sett stilles langt strengere krav til sikkerhet hos operatøren enn det som er foreslått implementert for å bedre sikkerheten i dagens løsning.
- Selve Web-serveren må ha et høyere sikringsnivå enn i dag og bør etableres på en egen maskin. Operativsystemet bør konfigureres slik at kun helt nødvendige funksjoner er tilgjengelige. For eksempel bør funksjoner som Telnet, FTP, RPC, PING gjøres utilgjengelige.
- Elektronisk postjournal-databasen bør etableres på en egen maskin som er separert fra Web-serveren med en brannmur.
- Web-, database- og Mailserveren må dimensjoneres for den økte trafikken en åpen løsning medfører.
- Brukeren av Elektronisk postjournal må i dag undertegne Brukeravtalen hvor de blant annet godtar at de ikke skal videreselge informasjonen de får tilgang til i databasen. I en åpen løsning kan en slik undertegning implementeres gjennom at brukeren leser og godtar vilkårene for tjenesten ved å trykker en "OK" knapp før det gis aksess til nettsiden. Alternativt kan man innføre en løsning der brukeren ved første gangs bruk må registrere seg og få tildelt en brukeridentitet og passord.
- Antall dokumentbestillinger og henvendelser til arkivene må ventes å stige ved en åpen tilgang. Dette kan potensielt medføre nye utfordringer som det ikke har vært tatt høyde for i denne rapporten og må vurderes nærmere.

5.6.2 Utvidelse av antall informasjonsleverandører

Det ligger i kortene at antall informasjonsleverandører ønskes økt. I dag er de fleste departementer og et antall underliggende etater med og det ligger ingen hindringer i veien for at dette antallet kan økes på relativt kort tid.

Vurdering:
En utvidelse av antall informasjonsleverandører (fra dagens 21 til langt flere) vil måtte skje gradvis over tid. Dagens Internett-baserte løsning er i utgangspunktet egnet for en slik utvidelse, men en rekke endringer er nødvendig.

Følgende tekniske forhold må tas i betraktning:

- De sikringstiltak som er foreslått i forhold til dagens løsning og antall

informasjonsleverandører blir enda viktigere ved en økning i antall informasjonsleverandører
- Man må foreta en oppskalering av den tekniske løsningen hos operatøren. Mail-server må kunne håndtere økt trafikk, flere konverteringsprosesser og databaseoppdateringer må kunne kjøre samtidig
- Antall personer som drifter mottakssystemet hos operatøren økes for å kunne håndtere feilsituasjoner og henvendelser fra informasjonsleverandørene
- Kravet til automatiserte rutiner for feilhåndtering vil øker på operatørsiden

5.6.3 Elektronisk tilgang til saksdokumenter

Elektronisk tilgang til saksdokumentene kan implementeres ved at brukeren gis tilgang til ønsket saksdokument via hyperkobling tilgjengelig i den elektroniske postjournalen.

En slik utvidelse er imidlertid utenfor omfanget av denne vurderingen og vil ikke bli behandlet nærmere i denne rapporten.

5.6.4 Vedrørende hvordan personnavn gjøres utilgjengelig i Elektronisk postjournal

Dagens praksis legger opp til at den offentlige journalen i medhold av Offentlighetsloven sladdes før den offentliggjøres. Moderne arkivsystemer innehar funksjonalitet for å gjøre noe av sladdingen på en hensiktsmessig måte. En slik sladding er sikker, da sladdete opplysninger blir elektronisk fjernet fra den offentlige journalen.

Frykten for at elektroniske offentlige journaler kan brukes til å samle inn, sammenstille og bearbeide personlig opplysninger (personnavn, adresse etc) gjør det aktuelt å vurdere begrensning i søkbarhet og visning. Teknisk sett kan dette gjøres på to måter:

- Arkivet sladder personlige opplysninger (også i de saksdokumentene som ikke er unntatt offentligheten)
- Operatøren begrenser søkbarhet og aksess til personlige opplysninger i Elektronisk postjournal-databasen

Eventuell sladding av personlige opplysninger i arkivet kan gjøres på to måter. De kan sladdes før den offentlige postjournalen sendes over fra informasjonsleverandøren til operatøren første gang. Da det kun er personnavn som ligger i databasen over tid som er problemet, er dette ikke ønskelig. "Nye" personnavn bør ligge i databasen en viss tid. Alternativt kan arkivene etter en viss tid, for eksempel tolv måneder, sende en oppdatert postjournal der alle personnavn er fjernet. Operatørens database replikeres dermed og personnavn fjernes. Dette medfører imidlertid vesentlig merarbeid for arkivene og vil være uheldig ut fra et sikkerhetsmessig synspunkt, da risikoen for feilbehandling øker når antall overføringer øker.

Ved en løsning der begrensning i søkbarhet og aksess til personlige opplysninger i Elektronisk postjournal-databasen begrenses sentralt hos operatøren, unngår man at informasjonsleverandøren må initiere sletting av personopplysninger fra den sentrale databasen. Selv om en slik løsning stiller strengere krav til autorisasjon og aksesskontroll til Elektronisk postjournal-databasen, synes en slik løsningen mer hensiktsmessig. Hvis man ønsker en løsning der det er valgfritt om personlige opplysninger i en journalpost skal være søkbare og lesbare etter en viss tid, kan et flagg som angir dette innføres i den offentlige postjournalen.

Den mest hensiktsmessige løsning vil fra et teknisk og sikkerhetsmessig synspunkt være at operatøren begrenser søkbarhet og aksess til personlige opplysninger etter en angitt tid, hvis ikke annet er angitt. Se forøvrig kapittel 7 for en nærmere diskusjon omkring hvordan operatøren kan implementere denne begrensningen.

5.7 Konklusjon på teknisk løsning og sikkerhet

Generell vurdering er at teknisk løsning og IT sikkerhet i dagens Elektronisk postjournal er rimelig bra. Imidlertid anbefaler vi et antall tiltak som klart vil bedre sikkerheten i dagens løsning. I tillegg foreslår vi nødvendige tiltak for en utvidelse av løsningen på både informasjonsleverandørsiden og brukersiden.

Områdene i det følgende er gruppert etter sårbarhet og skadeomfang definert i kapittel 5.2; Høy (H), Middels (M) og Lav (L) risiko.

5.7.1 Forslag til tekniske og sikkerhetsmessige tiltak som bedrer situasjonen i dagens løsning

Dette er tiltak for å bedre sikkerheten i løsningen som den framstår i dag. Disse er nødvendige - men ikke nødvendigvis tilstrekkelige for Internett-journal.

Risiko H:

Etablere Web-serveren på dedikert maskin

I dagens løsning kjører SIFT-databasen og Web-serveren på samme maskin. Ut fra et sikkerhetsmessig synspunkt er dette uheldig og Web-serveren bør derfor etableres på en egen maskin.

Verifisering av informasjonsleverandører ved mottak av elektronisk postjournal

I dagens Elektronisk postjournal har operatøren få automatiserte muligheter for å verifisere avsendere av e-post. Rutiner og mekanismer for å verifisere avsender bør derfor implementeres gjennom kontroll av avsenders adresse. Mekanismer for å autentisere disse er ønskelig, men foreslås først ved en større utvidelse av antall informasjonsleverandører.

Lagre og kontrollere mottaksrapporter

Informasjonsleverandørene bør innføre rutiner for systematisk lagring og kontroll av mottaksrapportene fra operatøren. Dette først og fremst for å sikre at feil under konvertering og innlegging i databasen oppdages. I tillegg sikrer dette bedre sporbarhet med hensyn til hvilke journaler som er mottatt hos operatøren. Informasjonsleverandøren må sjekke mottaksrapporten manuelt mot postjournalen.

Risiko M:

Innføre journaldato som felt i offentlig journal og i databasen

Saksnr og Doknr danner nøkkelen til en journalpost i dag. Et vesentlig problem med dette er at det ikke er mulig å identifisere alle de postene som er lagt inn en spesifikk dato. Dette gjør at de journalpostene som ved en feil ikke skulle ha blitt sendt en dato, først må identifiseres og så manuelt fjernes fra databasen. Dette er en tidkrevende prosess som kan unngås ved å innføre journaldato (som beskrevet i NOARK-4) som et felt i journalposten. Da kan alle journalposter for en spesifikk dato på en enkel og sikker måte fjernes fra databasen og den nye postjournalen legges inn på nytt.

Innføre system for elektronisk autorisasjon av elektroniske postjournaler

Elektronisk postjournal bør innføre system for å elektronisk autorisere postjournalens innhold til erstatning for håndskrevet signatur. Dette som et ledd i å forbedre kvalitetssikringen av postjournalenes innhold og klargjøre ansvarsforhold. Digitale signaturer kan benyttes til dette.

Kontrollere at innholdet på Web-siden er korrekt

For å kunne oppdage at journalposter "forsvinner" eller endres under overføring fra et arkiv til databasen, bør informasjonsleverandørene som fast daglig rutine sjekke at den postjournalen som ble sendt til operatøren stemmer overens med det som faktisk vises når man aksesserer Elektronisk postjournal Web-siden på Internett. Sjekkpunkter med "vanlige" feil bør dokumenteres.

Dokumentere backuprutiner hos operatøren og informasjonsleverandør

Rutiner for backup databasefiler, journalfiler og programmer hos operatøren må beskrives i driftsdokumentasjon. Dette for raskt å kunne gjenopprette databasen i tilfelle feil oppstår. Det er også viktig at disse er testet slik at man sikrer at gjenoppretting av databasen blir vellykket. Rutiner for backup av sendte journalposter fra den enkelte informasjonsleverandøren må også beskrives i brukerdokumentasjon. I brukerdokumentasjonen må det framgå hvilke kataloger filene skal lagres på og med hvilket navn og hvem som skal ha tilgang til disse. Dette for å raskt kunne re-sende identiske filer i tilfelle feil oppstår.

Dokumentere rutiner - brukerdokumentasjon

Rutiner ved ulike arbeidsoppgaver hos operatøren og informasjonsleverandøren (spesielt oppdatering av tidligere sendte journaler, backup og recovery av data og programmer, oppfølging av logger, sjekkpunkter ved kontroll av mottaksrapport o.l.) må være skriftlige og bør etableres i et miljø slik at de er lett tilgjengelige.

Kvalitetskontroll og feilhåndtering

Operatørens systemer for kvalitetssikring og feilhåndtering av innkommende postjournaler er også tiltak som kan forbedres, herunder rutiner og systemer for automatisert sammenstilling og kontroll.

Risiko L:

Standardisere formatet på Offentlig journal

Hos alle informasjonsleverandører bør standardrapporten "Offentlig journal" genereres iht NOARK-4 definisjonen, slik at alle journaler som sendes til operatøren er like. Dette reduserer risikoen for introduksjon av feil og reduserer behovet for manuelle inngrep både hos operatøren og informasjonsleverandøren. Utvidelser må vurderes.

5.7.2 Forslag til tekniske og sikkerhetsmessige tiltak ved utvidelse av antall informasjonsleverandører

I tillegg til tiltakene nevnt i 5.7.1, foreslås følgende tiltak i forbindelse med en eventuell utvidelse av antall informasjonsleverandører:

Risiko H:

Innføre systemer for autentisering og integritetssikring

Den elektroniske postjournalen må ikke uautorisert endres etter at de er sendt fra informasjonsleverandøren. Operatøren må også være sikker på at den elektroniske postjournalen virkelig kommer fra en informasjonsleverandør. I realiteten kan noen utgi seg for å være en informasjonsleverandør og sende falske postjournaler. På grunn av det store antallet informasjonsleverandører, anbefales det å innføre digitale signaturer. Digitale signaturer sikrer integritet og autentisitet ved bruk av krypto. Feil under overføringen av en postjournal fra et arkiv til operatøren kan oppdages raskt og sikkert.

Verisign Class 1 Digital ID er et eksempel på et digitalt sertifikat som kan brukes på e-postadresser. Sertifikatet utstedes av Verisign som er en såkalt tiltrodd tredjepart (TTP) som

verifiserer identiteten på en adresse.

Posten SDS har utviklet sikkerhetssystemet SecApp som benyttes mellom Kommunal- og regionaldepartementet og Husbanken (EDNA-prosjektet).

Filforsegling og sjekksum-funksjoner er andre mekanismer kan brukes til sikring av integritet. POSTSEC, SIGLL og PGP er produkter som tilbyr slike mekanismer.

Risiko M:

Innføre system for autorisere postjournalens innhold

Elektronisk postjournal bør benytte system for å autorisere postjournalens innhold til erstatning for håndskrevet signatur / parafering. Dette vil gi en mer formalisert utsending og kvalitetssikring av den elektroniske offentlige journalen.

5.7.3 Forslag til tekniske og sikkerhetsmessige tiltak ved åpen brukertilgang

I tillegg til tiltakene nevnt i 5.7.1 og 5.7.2, foreslås følgende tiltak i forbindelse med en eventuell åpen brukertilgang:

Risiko H:

Legge om dagens brannmur-løsning

Ved en åpen Internett-tilgang anbefales det å etablere en brannmur mellom Web-serveren og databaseserveren. Denne brannmuren bør være satt opp slik at den kun slipper igjennom nødvendig trafikk til databaseserveren - og ikke mer. I brannmuren settes det opp hvilke IP adresser som skal ha ekstern tilgang til lokalt nettverk. Den må også ha funksjoner som kan avdekke unormale hendelser gjennom logging og alarmfunksjoner. Den må også tilby funksjoner for autentisering, aksesskontroll og virus-deteksjon. Driftspersonellet må gis kompetanse til å gjennomføre analyse av loggene, og det må etableres rutiner som personellet skal arbeide etter. Driftspersonellet må gis myndighet til å treffe umiddelbare tiltak dersom regelverket nevnt over blir brutt. Checkpoint Firewall-1 er en av flere egnede brannmurløsninger. Av sikkerhetshensyn bør en screening ruter plasseres på utsiden av Webserveren. Operativsystemet på Web-serveren bør konfigureres slik at kun helt nødvendige funksjoner er tilgjengelige. For eksempel bør funksjoner som Telnet, FTP, RPC, PING gjøres utilgjengelige.

Oppgradere eller bytte ut SIFT-database for å kunne håndtere flere informasjonsleverandører

Med dagens databasedesign vil antall SIFT-databaser øke etterhvert som antall informasjonsleverandører øker. Det er i dag definert én database per informasjonsleverandører. Spesialversjon av SIFT tillater opp til 50 parallelle databaser. Når antall informasjonsleverandører blir større enn dette, må databasestrukturen enten re-designes, eventuelt byttes ut med et nytt databasesystem.

Risiko M:

Etablere regelverk

Det må etableres et regelverk som er relativt enkelt og lett å forstå. Dette regelverket skal være kjent for alle brukere (informasjonsleverandører) av systemet, samt konsekvensen av eventuelle brudd.

Innskjerpe rutiner ved sladding av sensitive personopplysninger

Det er tildels nødvendig med strengere rutiner for sladding av sensitive personopplysninger ved en løsning basert på åpen brukertilgang. Hvis f eks sladding av sensitive

personopplysninger ikke blir utført ved en feil, vil dette kunne medføre store konsekvenser i Internett-journalen på grunn av den vide spredningen. Det er her snakk om innskjerping av ordinære arkiv-rutiner både i forhold til forebyggende tiltak og tiltak som skal iverksettes når feil oppdages.

6. Vurdering av prosjektet i forhold til brukerkrav

Elektronisk postjournal har eksistert som prøveprosjekt siden 1992-93. I løpet av perioden frem til i dag, har systemet blitt videreutviklet, bl a som følge av innspill fra både informasjonsleverandører og redaksjoner.

Innhenting av synspunkter fra brukerne var en sentral del av det arbeidet Pharos gjorde i forbindelse med evalueringen av Elektronisk postjournal i 1996[40]. Vi har derfor ikke gjort dette til et sentralt område i denne gjennomgangen, jf forøvrig mandatet for konsekvensvurderingen.

6.1 Brukerønsker ift dagens løsning

6.1.1 Redaksjonene

Oppsummeringen av journalistenes syn i Pharosrapporten konkluderte med at de vurderte Elektronisk postjournal som et meget nyttig og godt verktøy med få svakheter. For journalister som har tilgang til Internett og er vant til å bruke dette krever Elektronisk postjournal:

- *«ingen anskaffelse av programvare eller utstyr»*
- *«ingen spesielle installasjoner eller datatekniske inngrep»*
- *«ingen spesielle besvergelser for å kople seg til databasen»*
- *«tilnærmet ingen opplæring, søkefunksjonen er tilnærmet selvforklarende (bare et par av brukerne fant det vanskelig å søke i journalene »*

De viktigste svakhetene som ble fremhevet i systemet var:

- *«for dårlig håndtering av svarene når databasesøket gir flere enn 100 treff. Dette gjelder også for kronologiske søk med flere enn 100 dokumenter»*
- *«tungvint bare å kunne be om 10 dokumenter pr bestilling»*
- *«krever repeterende inntasting av data pga lite bruk av samme data fra et bilde til et annet»*
- *«behov for enkelt å kunne be om utvidet offentlighet ved begrenset innsyn til et dokument, f eks ved hjelp av e-post»*
- *«mangler lenke til internettside som gir veiledning i bruk av offentlighetsloven»*

Fra journalistenes side ble det understreket at den største begrensningen knyttet til Elektronisk postjournal ikke ligger i systemet selv, men i den begrensede deltagelsen i antall arkiver, i manglende kunnskap om og ferdighet i å bruke de offentlige postjournalene, og i den varierende kvaliteten i dataregistreringene. Innenfor dagens løsning, er dette hovedinntrykket fortsatt gjeldende.

Som nevnt har det siden prøveprosjektet ble etablert, blitt gjennomført flere utviklingstiltak. Flere tiltak er gjennomført for å bedre kommunikasjonen, blant annet overgang fra modem til Internett, fra telefaks til e-post (bestillinger) og fra SIFT til web-brukergrensesnitt. Det er også gjennomført funksjonelle endringer for å gjøre tjenesten lettere å bruke, blant annet hyppigere oppdatering, tjenesten vis alle dokumenter i en sak og bla bakover / fremover i journalen (50 og 50 poster).

[40] Vurdering av Elektronisk postjournal, Pharos 1997

De vesentligste ønskene vi har registrert, som denne brukergruppen ikke har fått oppfylt er:

- Mulighet for å få samlet oversikt over hvilke dokumenter egen redaksjon har bestilt.
- Å få inn et kommentarfelt i bestillingsskjemaet

I tillegg til dette, har redaksjonene ønsker i forhold til å kunne bestille dokumenter, f eks å kunne bestille alle dokumenter i en sak. Dette ønsket vil kunne få stor betydning for arbeidsmengden i arkivene, og har derfor blitt balansert mot denne gruppens ønsker på samme område, jf om bestillingsfunksjonen i avsnitt 6.1.2. Pressekilder vi har intervjuet, gir imidlertid uttrykk for at dette balansespørsmålet ikke er relevant. Forvaltningen bør etter dette synet stille de nødvendige ressurser til disposisjon, slik at innsyn kan gis.

6.1.2 Informasjonsleverandørene

Arkivene pekte i Pharosrapporten på overføringsrutinene mellom departementene og SDS som den største svakheten ved systemet. Forbedringer av systemet burde ha følgende mål:

- *«færre manuelle operasjoner»*
- *«sterkt redusert tid fra et dokument er registrert i et arkiv til det er tilgjengelig i databasen for Elektronisk postjournal»*
- *«oppdatering av databasen for Elektronisk postjournal når den tilhørende registreringen i et arkiv er endret»*
- *«kvittering for at hver overføring er vellykket mottatt og innlest i databasen hos SDS»*
- *«standardisering av overføringsformatet, f eks som en NOARK standard, slik at overføringer fra alle arkivsystemer kan behandles av et felles mottaksprogram»*

Informasjonsleverandørene har hatt Forum for Elektronisk postjournal (Forum-epj) som en viktig kanal for å formidle brukerønsker. Her har representanter fra informasjonsleverandørene kunnet møte prosjektledelsen. Også ift denne brukergruppen har det blitt gjennomført utviklingsarbeid, men i den seneste tiden har utviklingsarbeidet stått noe tilbake for utvidelsesarbeidet (1999).

En beskrivelse av de viktigste endringene:

- Bestillingsfunksjonen - det ble i samråd med alle leverandørene bestemt at tjenesten "bestill alle dokumenter i saken " ble fjernet. Dette for å begrense antallet bestillinger noe. Overfor pressen ble dette begrunnet med at de likevel kunne få "se" alle dokumentene (postene) i en sak ved å søke på linken "saksnummer". Denne skal gi treff på alle poster av en sak (som er lagt inn i databasen).
- Kvitteringer - informasjon om e-postkvitteringens (mottakerrapport) funksjon og betydning for innlegging av offentlig journal har blitt tatt opp ved en rekke anledninger, og flere ganger i Forum-epj. Kvitteringen har gjennomgått forbedringer slik at også siste innlegging av data i shift-databasen ble talt opp.
- Bestillingsmail - utformingen av denne ble gjort i samråd med leverandørene (arkivene) - både i forum, men også i brevs form sendt på høring.
- Rutiner - ulike rutiner for oversendelse av offentlig journal - mottak av kvitteringer - mottak og behandling av bestillinger - har vært diskutert og tatt opp i Forum-epj.

Informasjonsleverandørene drar også nytte av tiltakene som er gjennomført for å bedre kommunikasjonen for redaksjonene.

Mange av de mer konkrete svakheter som ble påpekt i Pharosrapporten er altså endret. Det kan nå ta ca én dag fra registrering i arkivet til det er tilgjengelig i Elektronisk postjournal, kvitteringsfunksjonen er forbedret og overføringsformatet tas inn i NOARK 4. Oppdatering av Elektronisk postjournal ved endringer i arkivet er også mulig, men dette krever en rutine i arkivene som gjør at de oversender journalen på nytt når en rettelse er gjennomført.

Noen forslag til forbedringspunkter som har kommet frem gjennom kontakt med brukerne i denne undersøkelsen:

- Å få inn et eget journaldatofelt for hver post
- Å bedre mulighetene for å gjøre rettelser, gjennom å legge inn et endringsfelt

6.2 Brukerønsker ift allment tilgjengelig Elektronisk postjournal

6.2.1 Etterspørrere av informasjon fra tjenesten

En allment tilgjengelig Elektronisk postjournal vil rette seg mot nye brukergrupper. Det har ikke ligget innenfor rammen av dette oppdraget å ta kontakt med representanter for disse gruppene. Vi kan anta at brukerønskene knyttet til funksjonalitet fra journalistenes side, kan være dekkende også for nye brukere i en startfase. Det kan imidlertid være behov for å legge inn mer informasjon om offentlige journaler generelt og tjenesten spesielt, når andre enn journalister får tilgang.

6.2.2 Informasjonsleverandører

Antallet henvendelser om innsyn varierer sterkt mellom informasjonsleverandørene. De som i dag har størst pågang, er også de som er mest opptatt av de belastningsmessige konsekvensene av å gi allmenn tilgang. Finansdepartementet er bekymret for hva dette kan lede til. De ønsker ikke at allmennheten skal kunne bestille et ubegrenset antall dokumenter fra forvaltningen. En praktisk sperre på antall bestillinger bør legges inn, etter dette departementets syn.

Andre departementer, med mindre pågang, er i mindre grad bekymret for disse konsekvensene.

Det er også fra enkelte etater meldt om massebestillinger av de samme dokumenter fra departement og underliggende etat. Eksempelvis ble de samme 160 dokumentene bestilt samtidig fra MD og SFT. Det kan virke som hensikten kan ha vært å teste forvaltningen, for eksempel på praktisering av offentlighetsloven eller svartid på henvendelser. Det er også av denne grunn bekymring i departementene om en generell åpning av tjenesten Elektronisk postjournal uten praktisk sperre på bestillingsvolum.

Forøvrig vil allmenn tilgang til tjenesten ytterligere aktualisere tiltak som gjør det lettere å sikre at det som legges inn i Elektronisk postjournal har tilfredsstillende kvalitet. Dette gjelder både systemendringer i forhold til å gjøre det enklere å gjennomføre rettelser i Elektronisk postjournal ved endringer i arkivet, men også innskjerping av rutiner i arkivene. Rutinepunktet gjelder både det at den enkelte informasjonsleverandør følger de rutiner det er lagt opp til, og at det er et samsvar med hensyn til hvordan informasjonsleverandørene forstår rutinene.

Allmenn tilgang utløser også, etter noen informasjonsleverandørers mening, et behov for kvalitetssikring av det materialet som allerede ligger inne. Allmenn tilgang var ikke i diskusjonen da prøveprosjektet startet, samtidig som rutinene på det tidspunktet ikke var fullt innarbeidet.

6.3 Konklusjon

Hovedkonklusjonen slik systemet nå fungerer, er at mye av det som kan karakteriseres som brukerønsker allerede er innfridd. Fortsatt eksisterer det et forbedringspotensiale ift å gjøre tjenesten lettere å bruke for arkiver og journalister. For begge gruppene vil det imidlertid være andre elementer som har langt større betydning enn de rent brukermessige, jf diskusjonen ellers i rapporten om økning i antall informasjonsleverandører og allmenn tilgang til tjenesten.

Når det gjelder spørsmålet knyttet til begrensning av antall bestillinger, åpner offentlighetslovens § 8 for at forvaltningen i en viss grad balanserer anmodninger om innsyn i forhold til arbeidsbelastning. Det å legge inn en begrensning når det gjelder antall dokumenter det er mulig å bestille på en gang, kan synes som en hensiktsmessig måte å balansere dette på.

Vi vil understreke at det fra informasjonsleverandørhold legges meget stor vekt på å rense det materialet som nå ligger inne før allmenn tilgang ev gis. En mulighet er ikke å gi tilgang til det eldste materialet ved en utvidelse av antall informasjonsetterspørrere.

7. Vedrørende alternative tekniske løsninger

Det er i det foreliggende arbeid ikke gjort en systematisk gjennomgang av alternative tekniske løsningskonsepter i forhold til dagens løsning levert fra Posten SDS. Dette fordi en slik gjennomgang har ligget utenfor omforenet omfang av konsekvensutredningen.

Vi vil her likevel knytte noen kommentarer til mulige alternative måter å løse det systemtekniske på. Videre vil vi kommentere hva som må gjøres for å komme frem til en teknisk løsning på den skisserte sladdingen av navn på fysisk person i avsender-/mottakerfeltet som i kapittel 5.6.4 av tekniske hensyn ble anbefalt utført hos operatøren.

Med dagens rolle- og ansvarsfordeling, kan det overordnede tekniske løsningskonseptet virke hensiktsmessig. Ut fra en kost/nytte antagelse synes det ikke å eksistere klare eller nærliggende alternative tekniske løsningskonsepter for tjenesten slik den er lagt opp i dag. Alternative løsningskonsepter kan i denne sammenhengen tenkes å være basert på ny Internettorientert søketeknologi. En videre utredning omkring dette, samt konsekvensene av en vesentlig utvidelse av antall (flere hundre) og typer informasjonsleverandører (f eks mindre trygdekontorer) bør vurderes gjennomført. Dette må sees i nær sammenheng med virksomhetenes øvrige satsninger innen elektronisk datautveksling[41].

I vår vurdering og anbefaling vedrørende teknisk løsning for å hindre søk på personnavn etter en viss tid, ligger forslaget om at navn på fysisk person skal ligge søkbart i et antall måneder (12 er foreslått), og deretter ikke være søkbart, sentralt. Dette har ikke innvirkning på opplysninger som i seg selv er unntatt offentlighet; disse skal sladdes allerede i dag og skal ikke forefinnes verken i papirbasert eller elektronisk offentlig journal.

Vi har følgende kommentarer til hvordan en reduksjon i søkbarhet kan gjennomføres.

Arkivsystemet er originalen

Basis for problemstillingen er at arkivsystemet hos informasjonsleverandøren er og vil være originalen for postjournalen. Enhver Elektronisk postjournal vil kun være en kopi av (rapport fra) originalen. Ikke-søkbarhet på personnavn etter en viss tid vil kun omfatte den elektronisk søkbare versjonen av postjournalen.

Informasjonsleverandør er ansvarlig for innhold i Elektronisk postjournal

En hypotetisk fordeling av ansvaret for innhold i Elektronisk postjournal, for eksempel mellom informasjonsleverandør og Statens informasjonstjeneste, kan lede til uklarhet i ansvar ved feil og til uklarhet i ansvar for kvalitetskontroll av journalene. Det er derfor vanskelig å se for seg løsninger som fraviker prinsippet om at informasjonsleverandøren er ansvarlig for egen informasjon som reelt blir lagt allment tilgjenglig.

Om å fjerne søkemuligheten på feltene avsender /mottaker

Søkemuligheten på enkeltfelt kan, teknisk sett, fjernes relativt enkelt i løsninger som Elektronisk postjournal. Å fjerne søkemuligheten generelt for avsender/mottaker vil imidlertid gi store begrensninger i nytten på områder som ikke kommer inn under

[41] Se tiltaksområde 2 og 3 i kapittel 7 i rapporten "Elektronisk datautveksling og innrapportering", Statskonsult 1998, der tilgjengeliggjøring av databaser i sammenheng med Forvaltningsnettprosjektet er relevant for Elektronisk postjournal.

personvernhensyn. For eksempel vil det hindre søk på korrespondanse til og fra bedrifter, organisasjoner og offentlige etater (relevant for de som ennå ikke er med i ordningen) .

Videre vil fjerning av søkbarhet, men ikke sladding / fjerning av navn på fysisk person, føre til at personnavn stadig er elektronisk tilgjengelig ved nedlasting av kronologisk journal eller journal som er resultat av annet søk. Dette gjør det enkelt teknisk sett å laste ned store deler av journalene og søke på personnavn på sin egen PC.

Om å sladde/fjerne/redusere tilgjengeligheten til navn på fysisk person fra Elektronisk postjournal

I første omgang må det avklares om navn på fysisk person sladdes, fjernes eller gjøres vanskelig tilgjengelig i Elektronisk postjournal, eller ikke. I neste omgang må man finne en metode for å komme fram til hvilke navn som skal sladdes, fjernes eller gjøres vanskelig tilgjengelig. Til slutt må det avklares i hvor stor grad navnet skal være utilgjengelig.

Vedrørende det første forholdet, er det allerede i tidligere kapitler 4.3.2.6 slått fast at det av personvermessige hensyn ikke er ønskelig at navn på fysiske personer skal være fritt tilgjengelig i Internett-journalen etter 12 måneder.

Når det gjelder hvilke navn som skal sladdes, fjernes eller gjøres vanskelig tilgjengelig, er det i utgangspunktet bare navn på fysiske personer. En mulighet for at personer eksplisitt skal kunne be om at deres navn skal være tilgjengelige også etter 12 måneder, er vurdert i kapittel 4.3.2.6, men ikke anbefalt pga teknisk-administrativt merarbeid og potensiell kilde til feil. Da har en grovt sett to muligheter for å skille mellom det som er navn på fysiske personer og det som ikke er det:

- å gjøre en logisk analyse av innholdet i feltet, for eksempel ved å koble mot etablert navneregister (f eks en liste fra folkeregisteret).
- å etablere en kode for dette i journalposten fra arkivsystemet, enten på grunnlag av et 'sladde-tegn' som finnes allerede i dag i visse arkivløsninger (f .eks. '@' i DocuLive) eller basert på innføring av tillegg i NOARK-standarden, f eks et flagg som indikerer om feltet inneholder navn på fysisk person eller at innholdet i feltet skal sladdes etter en viss tid.

Første alternativ vil lett medføre fjerning av navn på offentlige personer som kommuniserer med forvaltningen i embeds medfør, noe som i seg selv er mindre ønskelig. Videre er metoden ikke helt sikker, f eks i forhold til navn som ikke er registrert. Den vil også kunne slette firmanavn som har navn som fysiske personer (f eks Andersen og Føyen, for å ta to nærliggende eksempler), eller f eks kommunenavn som er lik navn (Nes, Os, m fl). Denne metoden måtte ev suppleres med en manuell rutine.

Andre alternativ synes enklere å implementere. Journalposten inneholder en kode eller et flagg som indikerer om et felt inneholder navn på fysisk person eller om innholdet skal sladdes etter 12 måneder. Metoden har en liten risiko for at det kan skje feil, men sannsynligheten for at det skal skje flere feil knyttet til samme person er meget liten. Risikoen for at det skal være mulig å bygge personprofiler basert på slike feil, er forsvinnende liten.

Når det gjelder i hvor stor grad navnet på fysisk person skal være utilgjengelig i Internett-journalen etter 12 måneder, er det to måter å justere dette på. For det første vil det enten journalpostene vises gjennom kronologisk blaing eller som et resultat av søk, er det hensiktsmessig å begrense antall journalposter som vises på samme side. Dette for å redusere den ekstra søkekapasiteten brukeren får gjennom nettleserens søkefunksjon. I dag er maksimalt antall journalposter som kan vises på samme side satt til 50, noe som synes hensiktsmessig.

For det andre må det vurderes om navn på fysiske personer skal stå i klar tekst i liste over komplette journalposter. En mulighet er å fjerne all visning av navn på fysisk person etter 12 måneder. En annen er å vise navnet indirekte, f eks ved at navnet kun kan lese ved å klikke en hyperkobling i avsender / mottakerfeltet i journalposten, eller at en såkalt ShowTips-funksjon viser navnet på personen først når musepekeren holdes over feltet.

Det er også verd å merke seg at en fjerning eller sladding av personnavn ikke behøver å være 100% effektiv for å oppnå målet, nemlig å hindre mulighetene for å etablere personprofiler. En effektivitet på 98% i fjerning av personnavn vil – litt unøyaktig sagt – være tilstrekkelig. Det er verd å merke at denne feilprosenten i så fall må være tilfeldig fordelt, dvs være vilkårlig på tvers av personer i motsetning til konsekvent å la 2% av alle fysiske personer bli blottstilt.

Oppsummert er det noen tekniske og sikkerhetsmessige utfordringer knyttet til å begrense søkbarheten på personnavn, men problemene er klart løsbare gjennom ulike teknikker.

Etter vår mening bør metode for å begrense søkbarhet på personnavn vurderes nærmere før innføring av denne typen teknisk løsning igangsettes. Dette som en del av utforming av teknisk løsning, dvs: *Hva* som skal gjøres (søkebegrensning) er en premiss; *hvordan* det gjøres er opp til leverandør av teknisk løsning. Det er ikke grunn til å forsinke den videre diskusjon rundt prinsippene for begrensninger søkbarhet i en allment tilgjengelig postjournal på Internett på grunn av dette.

8. Konklusjon og anbefaling

8.1 Videreføring av dagens løsning, tilgang gis til en avgrenset brukergruppe

Som nevnt i diskusjonen av offentlighetsprinsippet i kapittel 4, mener vi at dagens prøveordning innebærer en særbehandling av en begrenset gruppe medlemmer av offentligheten, nemlig massemediene (og heller ikke alle mediene). De som har tilgang til Elektronisk postjournal via passord, må sies å ha fått et informasjonsprivilegium. Slike informasjonsprivilegier for mediene eller andre enkeltgrupper kan vanskelig forsvares med bakgrunn i offentlighetsprinsippet. Dette prinsipp forutsetter tvert i mot at rett til innsyn i den offentlige forvaltnings saksdokumenter tilkommer enhver i egenskap av samfunnsborger. Mye taler for å se dette prinsipp som så fundamentalt at det kan betegnes som en grunnleggende menneskerettighet eller en grunnrettighet, jf forslaget om å ta dette inn i grl § 100 om ytringsfriheten. Slike grunnrettigheter kan ikke noen ha i større grad enn andre. De må nødvendigvis tilligge alle borgere på like linje.

Det er derfor i høy grad et spørsmål om den prøveordning som nå har eksistert i flere år, bryter grunnleggende med offentlighetsprinsippet. Dette hører det ikke til den vurderingen å ta stilling til, men vårt syn er i hvert fall at med tanke på en varig og regulær ordning må utgangspunktet være at en ikke kan løse personvernproblematikken ved å begrense tilgangen til visse grupper, mens flertallet stenges ute.

Vi kan derfor ikke anbefale en permanent videreføring av dagens løsning.

8.2 Anbefaling vedrørende personvernmessige forhold, slik at allmenn tilgang kan gis

I kapittel 4, konkluderes det med at vi tror en oppnår det beste kompromiss ved en kombinasjon av tidsbegrensning og innholdsbegrensning i Internett-journalen. Dersom journalen ikke inneholder personopplysninger, er det ikke personvernmessige betenkeligheter ved et historisk Internett-arkiv. Vi vil i dette avsnittet redegjøre for hvilken løsning vi mener vil være mest hensiktsmessig.

Vi vil diskutere dette i forhold til de feltene i Elektronisk postjournal der personopplysninger forekommer.

8.2.1 Feltet avsender/mottaker

8.2.1.1 Tidsbegrensning

En tidsbegrensning (dvs at navn på fysiske personer gjøres utilgjengelig eller vanskelig tilgjengelig etter en tid) ivaretar hensynet til at offentlig informasjon er offentlig også i Elektronisk postjournal, samtidig som muligheten til å bygge personprofiler begrenses.

Hvilken tidsramme som skal benyttes, vil være et avveiningsspørsmål. Ser man hensynet til

pressens bruk av journalen isolert, kan kanskje en 3 måneders grense være akseptabel, ut fra at pressen uansett er mest opptatt av de dagsaktuelle sakene og at redaksjonene løpende følger med i Elektronisk postjournal. Ved å gi allmenn tilgang, vil dessuten nye brukergrupper komme til. Disse vil ha en mer sporadisk bruk av Elektronisk postjournal og ser det kanskje som verdifullt at journalene er tilgjengelige i full tekst over lengere tid. Vi mener derfor samlet sett at 12 måneder er en grense som ivaretar balansen i forhold til profilbygging.

8.2.1.2 Innholdsbegrensning

En løsning knyttet til innholdsbegrensning, kunne være å slette avsender / mottakerfeltet helt i Elektronisk postjournal. Dermed ville det ikke være risiko for at personopplysninger fremkommer i dette feltet. Denne løsningen er imidlertid ikke akseptabel; informasjon knyttet til avsendere eller mottakere som ikke er fysiske personer er for sentral til at den kan slettes.

Det bør derfor vurderes å innføres en metode for å gjøre navn på fysisk person utilgjengelig eller vanskelig tilgjengelig etter 12 måneder. Med vanskelig tilgjengelig navn, menes f eks at navnet kun kan lese ved å klikke en hyperkobling i avsender / mottakerfeltet i journalposten, eller at en såkalt ShowTips-funksjon brukes.
At et felt inneholder navn på fysisk person bør indikeres f eks ved et flagg i journalposten. Dette krever at både NOARK-definisjon på "Offentlig journal" endres og at det innføres et nytt felt for dette flagget i databasen. Se forøvrig kapittel 7.

Det understrekes at det uavhengig av Elektronisk postjournal vil være mulig å få vite hvem som er avsender / mottager uavhengig av 12-månedersgrensen, ved å bestille dokumentet. Det er søke- og visningsmuligheten, og dermed muligheten for å bygge profiler, som fjernes eller reduseres ved dette tiltaket. Dette vil, avhengig av tiltaket, i noen tilfeller kunne føre til at det bestilles dokumenter som ellers ikke ville ha blitt bestilt.

Det er også et motargument mot enhver form for tidsbegrensning at det enkelt vil kunne omgås ved systematisk nedlasting av det som publiseres. Det lar seg gjøre å legge inn tekniske hindre som vanskeliggjør slik nedlasting, men slike hindre vil alltid kunne overkommes. Vi ser imidlertid ikke dette som et avgjørende argument. Ved at en samtidig innfører et forbud mot slik nedlasting, vil en i hvert fall avskjære de seriøse aktørene. Opplysning om dette forbudet bør kunngjøres på hjemmesidene. Pressen vil kunne få særskilt tillatelse til å nedlaste data og bygge opp sitt eget register, i tråd med de begrensede regulatoriske krav som stilles ved behandling av personopplysninger for journalistiske formål.

8.2.1.3 Anbefaling

Vi anbefaler at navn på fysisk person i avsender / mottakerfeltet gjøres ikke-søkbart etter 12 måneder.

I tillegg anbefaler vi at det vurderes om navnet skal gjøres vanskeligere tilgjengelig eller begrense visningen av navnet etter 12 måneder som beskrevet i kapittel 8.2.1.2.

Det er en del tekniske utfordringer knyttet til å sikre begrenset søkbarheten på personnavn, men problemene er klart løsbare. Nærmere spesifisering av løsningen er altså nødvendig.

Etter vår mening bør metode for å begrense søkbarhet på personnavn vurderes nærmere før innføring av denne typen teknisk løsning igangsettes, gjerne som en del av teknisk utforming av en løsning. Dette behøver ikke å forsinke den videre diskusjon rundt prinsippene for begrensinger søkbarhet i en allment tilgjengelig postjournal på Internett.

8.2.2 Feltet innhold/emne

8.2.2.1 Innskjerping/justering av praksis

I forhold til gjeldende lovgivning vil navn være fjernes i dette feltet dersom hensynet til personvern tilsier det. Ved å gjøre Elektronisk postjournal allment tilgjengelig, er det nødvendig å innskjerpe at denne praksisen følges. Samtidig må behovet for at også andre opplysninger enn navn fjernes i slike saker, dersom de er egnet til å identifisere enkeltpersoner. Eksempler kan være gårdsnummer / bruksnummer eller adresse. Det er også vesentlig at personnavn slettes i et "ufarlig" svarbrev, dersom det via saksnummeret kan kobles til et dokument med personopplysninger som ikke skal offentliggjøres. I de spesialtilfellene der en sak kan utvikle seg til å inneholde opplysninger som gjør at navn skal sladdes, bør det opprettes nytt saksnummer når denne situasjonen oppstår. Et tenkt eksempel kan være søknad om prosjektmidler fra NN, tildeling av prosjektmidler til NN, underslag av prosjektmidler av NN.

Personer som omtales ved navn i disse feltene i kraft av sin stilling (f eks som leder av Telia / Telenor) bør uansett bli stående, uavhengig av tidsdimensjonen.

Vi står da igjen med muligheten for å bygge personprofiler i forhold til saker der ikke personvernmessige forhold gjør at navnet blir slettet og der personene ikke kan betegnes som offentlige. Så langt vi har kunnet bringe i erfaring, er ikke registreringen av denne type navn i feltene innhold / emne særlig omfattende. Vi anbefaler at det for fremtiden ikke registreres personnavn i disse feltene. Dersom det ut fra arkivmessige vurderinger er stort behov for å gjøre det, kan to løsninger skisseres:

- valg av samme løsning som for avsender / mottager, dvs merking av navn med en kode slik at det skjer sletting etter 12 måneder.
- det kan vurderes slik at omfanget er så begrenset, at muligheten for å bygge profiler er for liten til at tiltak bør gjennomføres

8.2.2.2 Anbefaling

Vi anbefaler at det settes i verk tiltak for å sikre at dagens rutiner følges, og at disse innskjerpes for å sikre at ikke personer kan identifiseres selv om navn er sladdet. Forøvrig antar vi at det ikke er behov for spesielle tiltak for å hindre at det kan bygges personprofiler med utgangspunkt i feltene innhold / emne. Skulle dette ikke medføre riktighet, anbefales samme løsning som for avsender / mottager.

8.2.3 Feltet saksbehandler

Det er i dag frivillig å føre saksbehandlers initialer i den offentlige journalen. Vi anbefaler at denne praksis fortsetter, slik at den enkelte informasjonsleverandør selv vurderer om dette skal tas inn. Det bør oppfordres til å føre denne informasjonen, slik at det er kun er for spesielt følsomme saksområder at denne informasjonen uteblir. Skulle det bli vanlig praksis ikke å oppgi saksbehandler, kan en regelendring vurderes.

8.2.4 Forholdet til det materialet som er lagt inn i løpet av prøveprosjektet

Ut fra hensynet til offentligheten er det ønskelig at så mye som mulig av materialet fra prøveprosjektet legges ut i en allment tilgjengelig Elektronisk postjournal. En situasjon der historikken fjernes hvis en allment tilgjengelig Elektronisk postjournal etableres er ikke hensiktsmessig.

På den annen side er det informasjonsleverandører som hevder at det ikke er god kvalitet på det

materialet som ble lagt i prosjektets tidligste fase. Vi har slått fast at det er informasjonsleverandøren som er ansvarlig for det innholdsmessige i Elektronisk postjournal, det er derfor disse som må vurdere hvor mye som skal tas med over i allment tilgjengelig Elektronisk postjournal.

Vi anbefaler at de informasjonsleverandører som mener det er nødvendig, gjør egne gjennomganger av materialet i Elektronisk postjournal før de tillater at det gjøres allment tilgjengelig. Eventuelt kan hele årganger slettes, dersom feilene er vesentlige og ressursbruken for å finne dem vil være for stor. Skulle behovet for denne type gjennomgang være omfattende, kan det etableres en vaskefunksjon (jf avsnitt 0).

8.2.5 Begrensning av antall bestillinger

Når det gjelder spørsmålet knyttet til begrensning av antall bestillinger, åpner offentlighetslovens § 8 for at forvaltningen i en viss grad balanserer anmodninger om innsyn i forhold til arbeidsbelastning. Det å legge inn en teknisk eller manuell begrensning når det gjelder antall dokumenter det er mulig å bestille på en gang fra Internett-journalen, kan synes som en hensiktsmessig måte å balansere dette på.

Hvilket nivå legger denne grensen på, må vurderes i forhold til erfaringene med allment tilgjengelig Elektronisk postjournal. Vi anbefaler ikke at antall bestillinger over lang tid legges på et lavt nivå som en sikkerhet; det må takles som det balansespørsmål det er. Vi anbefaler heller at antall samtidige bestillinger settes relativt høyt, og at tallet eventuelt kan reduseres dersom dette skulle vise seg å gi vesentlig arbeidsbelastning for forvaltningen.

8.2.6 Spørsmålet bør reguleres i offentlighetslov/arkivlov

Prinsipielt er det vår vurdering at bestemmelser som regulerer Elektronisk postjournal bør tas inn i offentlighetslovgivningen og/eller arkivlovgivningen, da ordningen springer ut av offentlighetsprinsippet og bør reguleres i det samme lovverk som regulerer de øvrige sider ved dette. Det presiserer at denne løsningen ikke er avgjørende for det personvernmessige beskyttelsesnivå man legger seg på. Hvis ikke journalen reguleres i dette lovverket, vil ordningen falle inn under persondataloven som den generelle lov om behandling av personopplysninger, jf § 5.

8.2.7 Hvorvidt bestemmelsene i persondataloven bør gis anvendelse

I kapittel 4.2.2.4 er det - med hovedvekt på Elektronisk postjournal - foretatt en detaljert vurdering av i hvilken utstrekning de materielle bestemmelser i persondataloven bør gis tilsvarende anvendelse på den behandling av personopplysninger som skjer etter offentlighetsloven og arkivloven. Vurderingen er gjort med EU-direktiv 95/46/EF som bakgrunn, idet vi etter EØS-avtalen er forpliktet til å implementere dette. Vi anbefaler stort sett å gjøre persondataloven tilsvarende gjeldende, med visse unntak. Det vises til kap 4.2.2.4 for detaljer, men noen hovedpunkter skal nevnes:

Informasjonsplikten etter persondataloven vil etter vårt syn langt på vei kunne ivaretas gjennom at relevant informasjon er tilgjengelig på journalens web-sider. Vi anser at direktivet under visse forutsetninger er forenlig med vår anbefalinger. Journalen er i utgangspunktet et meldepliktig register etter persondataloven § 31. Det bør gjøres unntak fra meldeplikten ved forskrift etter bestemmelsens fjerde ledd. Vi anbefaler at den generelle påleggskompetanse for Datatilsynet etter persondataloven § 46 ikke gis anvendelse.

8.2.8 Hvem bør være behandlingsansvarlig

Persondataloven definerer to kategorier pliktsubjekter. Den klart viktigste er behandlingsansvarlig, som er definert i loven som «den som bestemmer formålet med

behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.» Det andre pliktsubjekt er databehandler, definert i § 2 nr 5 som «den som behandler personopplysninger på vegne av den behandlingsansvarlige».

I kap 4.2.2.5 behandles spørsmålet om hvem som bør ha status som behandlingsansvarlig for den Elektronisk postjournalen. Konklusjonen er at dette bør være den enkelte informasjonsleverandør. I den grad Statens informasjonstjeneste engasjeres for å utføre noe av arbeidet ved dette, endrer ikke dette på at ansvaret utad ligger hos informasjonsleverandør. Den som mottar dataene og teknisk gjør journalene tilgjengelig på Internett, i dag Posten SDS, vil være databehandler med ansvar definert i kontrakt med hver enkelt informasjonsleverandør. I begrenset utstrekning er databehandler også pålagt plikter direkte etter bestemmelser i persondataloven som foreslås gitt tilsvarende anvendelse, jf pkt 8.2.7.

8.3 Anbefaling knyttet til teknisk løsning og sikkerhet

Overordnet inntrykk er at teknisk løsning og IT sikkerhet i Elektronisk postjournal er relativt bra, dog med unntak. Det foreslås i det følgende en del tiltak som vil forbedre sikkerheten i dagens løsning. I tillegg foreslås tiltak som ansees nødvendig ved en utvidelse av av løsningen på både informasjonsleverandørsiden og brukersiden. Se kap 5.7 for nærmere beskrivelse av tiltakene.

8.3.1 Forslag til tekniske og sikkerhetsmessige tiltak som bedrer situasjonen i dagens løsning

Vi har identifisert tre særlig viktig tiltak vi mener er nødvendig å gjennomføre for å bedre sikkerheten i dagens løsning.
For å kunne avdekke eventuelle feil under overføring, konvertering og innlegging av postjournaler på en raskere og sikrere måte, bør det innføres bedre rutiner og systemer hos informasjonsleverandøren for kontroll av datakvaliteten. Denne kontrollen bør spesielt rettes inn mot mottaksrapportene.
Videre må rutiner og mekanismer hos operatøren forbedres for å verifisere avsendere av e-post med postjournal-filene. Så lenge dette ikke er på plass, er det sannsynlig at feil som oppstår under overføring og innlegging ikke oppdages, og at feil legges ut i Elektronisk postjournal.
Databasen og Web-applikasjonen hos operatøren kjører på samme maskin i dag, men bør av sikkerhetshensyn kjøre på separate maskiner for å sikre mot angrep og innbrudd.

Videre har vi i kapittel 5.5.4 identifisert flere tiltak som vil sikre mot det vi har betegnet som middels eller lav risiko. De fleste av disse retter seg mot å bedre sikkerheten hos informasjonsleverandørene. Tiltakene knytter seg både til endring av rutiner, standardisering av formater og til forbedring av tekniske løsninger. Operatørens systemer for kvalitetssikring og feilhåndtering av innkommende postjournaler er også tiltak som kan forbedres.

8.3.2 Forslag til tekniske og sikkerhetsmessige tiltak ved utvidelse av antall informasjonsleverandører

På dette området er det innføring av system for autentisering av avsender og sikring av integritet under overføring, f eks digital signatur eller lignende sikkerhetstjeneste som fremstår som tiltak av stor betydning sikkerhetsmessig.

Også rutiner og systemer for autorisering av postjournaler hos informasjonsleverandøren er tiltak som bør iverksettes. Disse kommer i tillegg til de tiltakene som er anbefalt for å bedre situasjonen i dagens løsning.

8.3.3 Forslag til tekniske og sikkerhetsmessige tiltak ved åpen tilgang

På dette området er det å legge om og utvide dagens brannmurløsning og å oppgradere eller

bytte ut SIFT-databasen for å kunne håndtere flere informasjonsleverandører, de absolutt nødvendige tiltakene. Vi ser at alle disse ligger hos operatøren.

Det vil også være sentralt å etablere et regelverk som er enkelt og lett å forstå. Tilsvarende gjelder for innskjerping av rutiner ved sladding av sensitive personopplysninger. For å hindre søk på og evt visning av personopplysninger, samt ulovlig nedlasting eller kopiering av databasen, anbefales det i innføre innholds- og tidsbegrensning i databasen som beskrevet i kapittel 5.5.

8.4 Konklusjon

Gitt de prinsipielle innvendingene mot dagens løsning, blir det viktig Arbeids- og administrasjonsdepartementet å komme raskt videre i prosessen med å etablere en allment tilgjengelig Elektronisk postjournal.

Vi mener derfor at departementet så raskt som mulig bør se til at de nødvendige avklaringer med hensyn til utforming av en allment tilgjengelig Elektronisk postjournal blir gjort. Vi har i avsnittene over gitt våre anbefalinger om dette.

Etter en slik avklaring, vil den tekniske og sikkerhetsmessige løsningen måtte re-designes, før det konkrete utviklingsarbeidet starter. En viktig suksessfaktor vil være at det rettes spesiell oppmerksomhet mot de av våre forslag som har med innskjerping og endring av rutiner å gjøre. I tillegg må prosjektet ta høyde for en omfattende utvidelse av antall brukere og informasjonsleverandører, som både krever en generell oppskalering av de tekniske systemene på operatørsiden og re-design av datamodellen og dataformater.

I forbindelse med implementering av den nye løsningen, må skaleringsaspektet tillegges spesiell vekt, da antallet brukere vil øke betydelig, og det vil være vanskelig å forutse hvordan bruken av en allment tilgjengelig Elektronisk postjournal vil være.