

COMPLEX

INSTITUTT FOR
RETTSINFORMATIKK

JOHS. HANSEN

**SAFE P:
SIKRING AV
FORETAK,
EDB-ANLEGG OG
PERSONVERN-
INTERESSER
ETTER
PERSONREGISTER-
LOVEN**

TERESA (50)



12/88



Hovedkontor: Rosenholmvn. 25, 1410 Kolbotn, tlf. (02) 99 80 00

Bergen: Dreggsalmenningen 10/12, tlf. (05) 31 65 00

Stavanger: Auglendsdalen 81, tlf. (04) 58 85 00

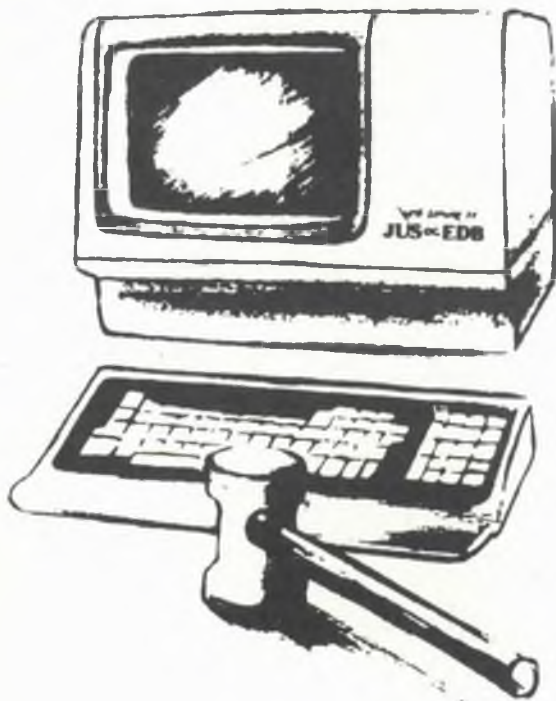
Trondheim: Kongensgt. 60, tlf. (07) 53 06 14

Norsk forening for **JUS og EDB**

Postboks 7557, Skillebekk, OSLO 2

Postgiro 5 13 96 54 Bankgiro 8200 42 49727

Postgiro ComPlex 2 12 16 63



Foreningen står bl.a. for
salget av CompLex-heftene
og vedlikeholder abonnements-
ordningene for serien.

SamvirkendeDataSystemerSamvirkendeDataSystemer
DataSystemerSamvirkendeDataSystemerSamvirkende
SystemerSamvirkendeDataSystemerSamvirkendeData
SamvirkendeDataSystemerSamvirkendeDataSystemer
DataSystemerSamvirkendeDataSystemerSamvirkende
SystemerSamvirkendeDataSystemerSamvirkendeData
SamvirkendeDataSystemerSamvirkendeDataSystemer
DataSystemerSamvirkendeDataSystemerSamvirkende
SystemerSamvirkendeDataSystemerSamvirkendeData
SamvirkendeDataSystemerSamvirkendeDataSystemer
DataSystemerSamvirkendeDataSystemerSamvirkende
SystemerSamvirkendeDataSystemerSamvirkendeData
DataSystemerSamvirkendeDataSystemerSamvirkende
SystemerSamvirkendeDataSystemerSamvirkendeData

Samvirkende
Data
Systemer



Statens DataSentral a.s

FOYEN

Ved behov for juridisk bistand,
kontakt FOYEN i Norge, Sverige,
England, USA og Brasil.

Rådgivning, bistand i forhandlinger
og prosedyre innenfor et bredt
forretningsjuridisk spekter, bl.a.:

Selskapsrett
Etableringsrett
Arbeidsrett
Internasjonalisering
Skatterett
Entrepriserett
EDB-rett
Kontrakts- og kjøpsrett
Forsikringsrett
Tingsrett
Personrett
Gjeldsforhandlinger og konkurs
Sjørett

NORWAY

**ADVOKATFIRMAET
FØYEN & CO ANS.**

Oscars gate 52, 0258 OSLO 2
Tel. (02) 44 46 40, Telex 181165 foyen n,
Fax (02) 44 89 27

P.O. box 253 Nesbru Senter,
1360 NESBRU
Tel. (02) 84 52 80, Telex 181165 foyen n,
Fax (02) 84 85 88

Moses Plass, 6500 KRISTIANSUND
Tel. (073) 76 944, Telex 15479,
Fax (073) 72 381

DBC Senteret, 3550 GOL
Tel. (067) 74 544, Fax (067) 75 509

SWEDEN

**ADVOKATFIRMAN
FOYEN & PEDERSEN**

Regeringsgatan 67, P.O. Box 7269,
S-103 89 STOCKHOLM
Tel. (08) 24 94 50,
Telex 12242 foplaw s,
Fax (08) 20 09 21

ENGLAND

FOYEN & BELL SOLICITORS

Norway House,
21/24 Cockspur Street,
LONDON SW1Y 5BN
Tel. (01) 839 7307,
Telex 265635 exnor g,
Fax (01) 839 5995

2 White House, Beacon Road,
CROWBOROUGH,
EAST SUSSEX TN6 1AB
Tel. 08926-65088, Fax 08926-65257

USA

**FOYEN & PERI
ATTORNEYS AT LAW**

250 Park Avenue 19th Floor,
NEW YORK N.Y. 10177
Tel. (212) 687 0100,
Fax (212) 687 0659

636 Morris Turnpike,
SHORT HILLS, NEW JERSEY 07078
Tel. (201) 564-6116,
Fax (201) 564 7665

BRAZIL

FOYEN CONSULTORES S/C

Rio Sul Tower, Suite 2308
Rua Lauro Müller 116
RIO DE JANEIRO CEP 22290
Tel. (21) 541 8896, Telex 21985,
Fax (21) 541 7295

CompLex no. 12/88

Institutt for rettsinformatikk
Universitetet i Oslo
Niels Juels gate 16
N-0272 OSLO 2

Johs Hansen

**SAFE-P:
SIKRING AV FORETAK,
EDB-ANLEGG OG
PERSON-
VERNINTERESSE
ETTER
PERSONREGISTER-
LOVEN**

TERESA (50)

TANO

© Tano A.S. 1988
ISBN 82-518-2596-2

Den norske Advokatforening
Den norske Bankforening
Digital Equipment Corporation A/S
Ericsson Information Systems A/S
IDA, Integrert Databehandling a.s
Industriforbundets Servicekontor
K-link, Kreditkassen
Lovdata
Norges Forsikringsforbund
Norges Statsautoriserte Revisorers Forening
Televerket
Wikbort, Rein & Co

Fotografisk opptrykk ved
Engers Boktrykkeri A/S, Otta

Forord

I 1981 avga ei arbeidsgruppe, som skulle utrede sikring av personregistre, sin instilling. Daværende kontorsjef ved Datatilsynet, Arve Føyen, var formann. Arbeidsgruppa tok som utgangspunkt å sikre personverninteresser. Dette synes å være det eneste riktige - når disse oppfattes slik som Selmer og Blekeli har beskrevet begrepet. Arbeidsgruppa kom fram til et repertoar av sikkerhetstyper som kunne refereres til ved den enkelte konsesjon. Repertoaret besto av fire grunntyper av sikkerhetsregler. Disse er navngitt "sikring mot uautorisert tilgang til data", "sletting, forvanskning og ødelegging av data", "kontroll og oppfølgingstiltak" og "sikring av tilgjengelighet og restituering av persondata". Hver av typene har igjen tre nivåer, der påbudene i et høyere nivå inkluderer påbudene fra et lavere.

Høringsuttalelsene var noe varierte, med en negativ trend. Det vesentligste her var kritikk av for stor kompleksitet, dårlig systematikk og manglende vurderinger av kostnader av påleggene. På grunn av den noe negative mottakelsen ble arbeidet stilt i bero i påvente av tilsetning av spesialrådgiver i EDB ved Datatilsynet. I august 84 ble Johs Hansen ansatt som spesialrådgiver ved Datatilsynet. Han kom fra IRI, der han var ansatt mellom 1978 og 1985.

IRI hadde i 1984 opplevd en økende interesse for data- og informasjonssikring. Instituttet har gjort mindre utredninger om sårbarhet som følge av EDB i tilfelle krig. Videre om informasjonssikring knyttet til identitetsinformasjon og produksjon av identitetsinformasjon. Disse prosjektene er utført av Dag Schartum.

Dag Schartum IRI, Anette Klafstad, BBS, (tidligere student ved IRI) og Johs Hansen tok initiativ til et prosjekt ved IRI for å diskutere krav til sikring av personverninteresser etter personregisterloven. Dette for å utvikle egen kompetanse og for å være med å diskutere rammene for en sikringsforskrift.

Målsetninga for prosjektet har vært å utforme prinsipper for sikring av personverninteresser, foretak og EDB-anlegg. Om mulig også utkast til deler eller et fullstendig utkast til forskrifter. Prosjektet har vært utført som et prosjekt ved IRI og har hatt som fast kjerne Anette Klafstad, Dag Schartum, Eirik Djønne, Datatilsynet, og Johs Hansen.

Det har hatt en referansegruppe bestående av Knut S. Selmer, styreformann i Datatilsynet og instituttbestyrer ved IRI, Kjetil Johnsen, da konsulent i Rasjonaliseringsdirektoratet, Tor Hafli, da kontorsjef i Datatilsynet og Kristian Jahr, byråsjef i Justisdepartementet.

Justisdepartementet nedsatte den 26.4.86 en ny arbeidsgruppe for å utforme forskrifter for sikring av personregistre. Den hadde som medlemmer Eirik Djønne (formann), Kristian Jahr, Birger Melgård og Johs Hansen. Melgård ble oppnevnt som representant av Den Norske Dataforening.

Etter at arbeidsgruppa ble oppnevnt har ikke IRI-prosjektgruppa hatt noe møte. Arbeidsgruppa har benyttet et foreløpig utkast av denne rapport i sitt arbeid.

Prosjektgruppa har ikke funnet det riktig å føre dette arbeidet videre etter at Justisdepartementet nedsatte sin arbeidsgruppe. Denne rapporten er derfor relativt ufullstendig. Noe som skyldtes den overraskende terminering av prosjektet.

Allikevel tror vi det kan ha interesse å få tilgang til vurderinger Justisdepartementet's arbeidsgruppe har bygd på i sitt utkast til forskrifter.

Enkelte tilføyelser er gjort i denne rapporten etter at arbeidsgruppas rapport forelå. Tilføyelsene er skrevet i petit. Det samme har vært sjebnen til mindre sentrale tema og til utdypninger.

For helhetens skyld er også arbeidsgruppas rapport trykt som vedlegg.

På grunn av arbeidsdelinga i prosjektgruppa og avbrytelsen av prosjektet, er det ikke naturlig at hele gruppa står som forfattere. Tankene i rapporten er ført i penna av undertegnede. Ikke desto mindre har Djønne, Klafstad og Schartum - og referansegruppa - gitt nyttige bidrag til utforminga av det "sikkerhetsapparat" som foreslås for regulering av sikkerhet rundt personregistre i denne rapporten. Djønne har også skrevet avsnitt 2.3 i denne rapporten. Prosjektgruppa skal berømmes for uten vederlag å ha lagt ned mye arbeid i prosjektet. Det vitner om ikke så rent lite idealisme.

En mer bearbeidet gjennomgang av hele materialet er sterkt ønskelig. Det får utstå inntil videre. Allikevel er det å håpe at det kan være et og annet "korn" å hente i denne rapporten.

Skillebekk, 29.7 1988

Johs Hansen

INNHALDSFORTEGNELSE

1	INNLEDNING	6
2	UTGANGSPUNKT FOR SIKRINGSPROBLEMATIKKEN	7
2.1	Realisering av personverninteresser	7
2.2	Avgrensning av omfanget til en sikringsforskrift	7
2.3	Personverninteresser	8
2.3.1	Det teoretiske personvernbegrep	9
2.3.2	Personvern i lovgivningen	10
2.3.3	Personvern i enkeltvedtak etter personregisterloven	13
2.3.4	Datatilsynets personvernbegrep	16
2.4	Teknisk utvikling og dens innvirkning på personvernet	19
2.5	Ajourføring av personvernbegrepet	19
3	OM SIKKERHET OG SIKRING	25
3.1	Sikkerhet og risiko	25
3.2	Sikring	26
3.2.1	Sikring og personvern	26
4	RISIKOANALYSE AV ANLEGG OG FORETAK SOM BEHANDLER PERSONREGISTRE	28
4.1	Situasjonsbeskrivelse	28
4.2	Hvilke trusler står en ovenfor?	28
4.3	Sårbarhetsvurdering	29
4.4	Risikovurdering	29
5	SIKKERHETSMODELL BYGD PÅ RESSURSBEGREPET	30
5.1	Ressurser	30
5.1.1	Ressursers natur	30
5.1.2	Komplekse ressurser	30
5.2	Ressursers livsløp	31
5.2.1	Produsjon av en ressurs	31
5.2.2	Tilegnelse av ressurs	31
5.2.3	Operasjon på ressurs	31
5.2.4	Avhendelse av ressurs	32
5.3	Ressurssikkerhet	32
5.3.1	Ressursers kvalitet	32
5.3.2	Autorisasjon av operasjoner	32
5.3.3	Sertifisering	34
5.3.4	Identifikasjon	35
5.3.5	Autentisering	35
5.3.6	Tilgjengelighet	35
5.3.7	Administrasjon av ressurs	35

6	SENSITIVITET	37
6.1	Personvern-orientert sensitivitet	37
6.2	Sensitivitet for personopplysning	38
6.3	Akseptabel risiko	39
6.4	Noen trussetyper mot personopplysninger	40
6.4.1	Identifisering	40
6.4.2	Autentisering	41
6.4.3	Tilgjengelighet	41
6.4.4	Kvalitet	42
6.4.5	Operasjoner på personopplysninger	42
6.5	Grovdeling av trussetyper. Graderingsforslag	42
6.5.1	Kompromittering av opplysninger	43
6.5.2	Trusler mot kvaliteten av opplysninger	43
6.5.3	Trusler mot kvalitet i behandling av opplysninger	43
7	SÅRBARHETSGRADER	44
7.1	Hva skal vi forstå med de ulike sårbarhets-gradene?	45
7.1.1	Betydelig skade	45
7.1.2	Skade	45
7.1.3	Mindre skade	45
8	SENSITIVITETSMODELL	48
8.1	Sensitivitetsgrader	48
8.2	Modellen	48
8.2.1	Sensitivitet for kompromittering av opplysninger	48
8.2.2	Sensitivitet for datakvalitet	48
8.2.3	Sensitivitet for rutinekvalitet	54
8.2.4	Sammenheng mellom sensitivitet for opplysningstype, post, register og samling av registre	54
8.3	Sensitivitet og alder på opplysninger	55
8.4	Noen mulige regler om sensitivitetsgradering	55
9	INFORMASJONSSIKKERHET	56
9.1	Informasjonskvalitet	56
9.1.1	Modellkvalitet	58
9.1.2	Datakvalitet	58
9.1.3	Tolking	59
9.2	Registerkvalitet og kvalitet ved bruk av register	59

10 OPPSUMMERING OG DRØFTING AV SENTRALE SPØRSMÅL FOR UTFORMING OG ADMINISTRASJON AV SIKKERHETSFORSKRIFTEN	62
10.1 Regulering av sikkerheten rundt personregister eller ikke?	62
10.2 Reguleringsform	63
10.3 Hvem skal fastsette sikkerhetsnivå?	63
10.4 Hvordan skal sikkerhetsnivået fastlegges?	64
10.4.1 RP-orientert analyse	64
10.4.2 Ved sårbarhets eller risikoanalyse?	64
10.5 Kommunisering av pålegg om sikring	65
10.5.1 Kommunikasjon av regler	65
10.5.2 Kommunikasjon av sensitivitetsgrader	65
10.5.3 Kommunikasjon av tiltak	65
10.6 Forskriftene	66
10.6.1 Omfang	66
10.6.2 Reglene	66
10.6.3 Systematikk	69
10.6.4 Detaljeringsgrad og bruk av rundskriv	70
10.7 Administrasjon og bruk av sikkerhets- forskriften	71
10.7.1 Registereier	71
10.7.2 Datatilsynet	72
LITTERATUROVERSIKT	74
VEDLEGG: RAPPORT FRA JUSTISDEPARTEMENTETS ARBEIDS- GRUPPE MED UTKAST TIL FORSKRIFT FOR SIKRING AV PERSONREGISTRE	76

SIKRING AV FORETAK, EDB-ANLEGG OG PERSONVERNINTERESSER ETTER PERSONREGISTERLOVEN (SAFE-P)

1. INNLEDNING.

De fleste som har arbeid der EDB er et vesentlig innslag vil være enig i at det er behov for styrking av datasikkerheten. Dette gjelder alle ledd i kjeden fra maskinprodusentene og softwareleverandører til sluttbrukerne.

I en god del år har vi hørt om ulike krenkelser av personvern- og økonomiske interesser i forbindelse med EDB. Lar vi den økonomiske delen ligge - og konsentrerer oss om norske eksempler har vi likevel en kilde å øse av. Mange systemer gir relativt ubeskyttet tilgang for skjermbrukere til personopplysninger av variert slag. Studenter har skaffet seg tilgang til eksamensregister og endret karakterer. Mange er lempfelidige i sin bruk av passord. Administratorer er ikke nok lydhøre for behovet for bedret sikring.

I det hele tatt er situasjonen lite god: Behovet for bedret EDB-sikkerhet er stor og forståelsen for at dette trengs hos de som må treffe beslutningene er liten. Sårbarhetsutvalget har anslått investeringsbehovet i EDB-sikkerhet ut fra et nasjonalt sårbarhetsperspektiv å være i størrelsesorden 100-talls millioner kroner. Tallet ble tilkjennegitt i forbindelse med presentasjon av utredninga (NOU 1986:12).

Denne tilstand skyldes nok at det EDB-faglige miljøet i Norge har vært lite opptatt av sikkerhet og at vi er så heldige å ha et åpent og relativt trygt samfunn. Ikke desto mindre er det grunn til å bedre datasikkerheten. Selvsagt må den veies mot sosial sikkerhet og andre interesser i samfunnet.

Om vi skjeler litt til det som vil være nært forestående bruksutvikling innen informasjonsteknologien understrekes ytterligere behovet for EDB-sikkerhet med personverninkling.

Bare noen få eksempler:

Innen helsesektoren ønsker en å kunne sende sensitive personopplysninger over telenett. f eks i forbindelse med pasientoverføring. Dermed aktualiseres behovet for tilgangskontroll, kryptering av data og også sikring mot manipulasjon ved overføring, m m.

Også deling av kostbare ressurser som kraftige datamaskiner mellom flere registreiere vil være ønskelig blant annet av økonomiske årsaker. Ønskes sensitive data lagret ved anlegg som deles av svært mange brukere stilles store tekniske krav til sikring av anlegget.

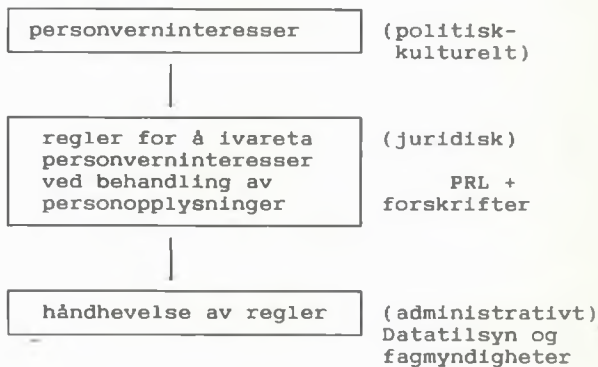
2 UTGANGSPUNKT FOR SIKRINGSPROBLEMATIKKEN.

2.1 Realisering av personverninteresser

Utgangspunktet for sikringsproblematikken er å sikre legitime personverninteresser. Det vil si å realisere personvern ved hjelp av politiske, juridiske, tekniske, organisatoriske og administrative tiltak.

En abstrakt modell av realisering av personverninteresser kan beskrives som tre ordnede lag av verdier, prinsipper og normer. Det mest abstrakte er personverninteressene i seg selv. Dette kan vi oppfatte som et politisk-kulturelt lag. Det neste lag er reglene for å realisere personverninteressene. Dette er et juridisk lag med en nærmere - juridisk - bestemmelse av personverninteressene. Det tredje lag er det vi kan kalle håndhevelse av reglene for realisering av personverninteresser. Dette er et administrativt lag.

I hovedsak går påvirkingsstrømmen mellom lagene nedover. Vi kan derfor beskrive modellen slik:



2.2 Avgrensning av omfanget til en sikringsforskrift

Hvordan skal en avgrense en sikringsforskrift? For det første må de begrenses til å sikre personvern. Men de bør ikke inneholde generelle regler om etablering og bruk av registre. Dette dekkes i lov og generelle forskrifter.

En kunne tenke seg å nedfelle regler om tekniske, administrative og organisatoriske forhold vedrørende drift av registeret for å fremme personverninteressene etter loven og forskriftene. Man kunne da gi regler om sikring av opplysthetsinteresser og av interesser i borgervennlig administrasjon. Dette kunne f.eks. skje ved pålegg om innsynsterminaler, om lettfattelige utskrifter, m.m. Altså pålegg som går utover det som EDB-sikkerheten omfatter. Dette ville bli en meget vid avgrensning.

Det betviles å være hensiktsmessig i første omgang. Prinsipielt er det ønskelig med en så vid avgrensning, men en prioritering av ressursene taler for at en konsentrerer seg om sikkerheten for manuelle og EDB-registre.

En avgrensning å anbefale vil være å utforme regler om tekniske-, administrative- og organisatoriske forhold for å fremme sikkerhet for personregistre, EDB-anlegg og foretak som behandler personregistre.

Særlig er sikring av tilstrekkelig god datakvalitet et viktig punkt i tillegg til det som tradisjonelt oppfattes som EDB-sikkerhet.

Arbeidsgruppa har senere avgrenset omfanget til sikring

- mot kompromittering,
- av datakvalitet, og
- av tilgjengelighet av

personopplysninger, jfr §§ 1-3.1-4 og 1-5 i utkastet til forskrift.

Ei forutsetning for å gi forskrifter er at det politisk bestemte personvernbegrep ligger fast. På den måte at disse kan legges til grunn for påbud om tekniske tiltak etc. Det som definerer dette relativt stabile personvernbegrep er det som kan utledes av personregisterloven, dens forskrifter og Datatilsynet's presedenser.

2.3 Personverninteresser

Personvern er et begrep som trekkes fram i ulike sammenhenger. I vid forstand er det knyttet til retten til å være i fred. En aktiv presse fokuserer gjerningsmannen i en drapssak og familien ber om å slippe omtale av navn, fotografier av impliserte, boligen, press for å uttale seg o.s.v. Personvernet ble det kallet på da fjernsynet til slutt ikke fikk overføre direkte opplesningen av tiltalebeslutningen i Norges største spionsak. Hva veies personvernet mot i denne relasjon, frihet til informasjon - folkets rett til å vite hva som skjer? I Kina oppfordres folk til å angi naboer eller kolleger som trosser statens fødselsbegrensende tiltak og vil føde mer enn ett barn. I Norge vil vi si at dette i utilbørlig grad krenker personvernet, mens man i Kina ser dette i lys av den befolkningseksplasjon som truer og vektlegger det siste.

Personvern må veies mot de interesser som måtte tilsi at personvernet ikke kan få hel eller vesentlig uttelling. Noen krenkelser er åpenbare for alle, men samfunnspolitisk oppfatning, eller videre- verdisyn- vil normalt prege resultatet av den enkeltes avveininger.

I denne sammenhengen vil personverninteresser knyttet til bruk av personopplysninger bli behandlet.

2.3.1 Det teoretiske personvernbegrep

I norsk juridisk teori er personvern definert som den mulige interesse den enkelte har i å føre kontroll med den informasjon som beskriver en selv. Det er lagt til grunn at det er aktuell eller potensiell bruk av opplysningene som kan føre til krenkelser av personvernet. Dersom opplysninger er lagret slik at ingen praktisk eller teoretisk kan bruke opplysningene, skulle det etter dette ikke være noen fare for personvernkretnkelse.

Bruken knyttes til beslutning, formell eller uformell. En formell beslutning kan f.eks. være vedtak om stønad etter Lov om sosial omsorg. En uformell beslutning kan være at opplysning om politisk oppfatning fører til sosial utstøtelse i bolig- eller arbeidsmiljø.

Blekeli opererer med et knippe av delinteresser i personvernbegrepet og han er supplert av Selmer.

Den første interessen er interessen i diskresjon. Opplysninger som ikke har noe med saken å gjøre vil den enkelte ønske å holde utenfor en beslutningstakers rekkevidde. Dette særlig hvis opplysningene kan få betydning for utfallet eller det må oppfattes som en unødig spredning av opplysninger.

Interessen i fullstendighet er knyttet til ønske om at alle relevante opplysninger er tatt med. Opplysningene skal være korrekte, tilstrekkelige og presise.

En tredje interesse er i interessen i opplysthet. Denne er nødvendig for meningsfylt utøvelse av de to foregående. Den enkelte skal gis medinnflytelse. For å realisere det må det gis adgang til informasjon om hvilke opplysninger som blir brukt til hva og hvorfor.

Selmer supplerer listen med ytterligere to delinteresser.

Interessen i å ha en borgervennlig administrasjon er knyttet til individets ønske om å bli møtt med et vennlig ansikt. Individet har normalt liten mulighet til å påvirke beslutningstakernes arbeidsmåter. Et eksempel på dette kan være klartekst utskrifter fra registre og veiledning på andre språk for de som trenger det.

Den femte, og siste, delinteressen er interessen i å unngå overdreven kontroll eller uhjemlet maktbruk. Denne interessen er knyttet til utvikling mot et strammere samfunn og har elementer i seg av andre personverninteresser og rettferds-idealene. For å bekjempe et narkotikamisbruk de fleste av oss vil til livs, vil man lett få aksept på ubehagelige kontrolltiltak. For å ta de få skal alle ha det "litt ekkelt". Summen av kontrolltiltakene kan bli uakseptabel.

2.3.2 Personvern i lovgivningen

Det finnes rettslige normer utenfor personregisterlovgivningen som gjelder personvern i den sammenheng jeg har definert ovenfor under pkt 2.3.1. Taushetspliktregler i forvaltningsloven og i særlovgivning vil gjenspeile interesse i diskresjon. Diskresjonsinteressen slår også igjennom i den såkalte brevbruddsparagrafen, strl § 145. Det samme gjelder strl § 390 og § 390 a som verner om privatlivets fred. Regler om innsyn i opplysninger om seg selv finnes i legeloven, skatteloven, strafferegistreringslovgivningen. Reglene om partsinnsikt, varslingsplikt og offentlighetens rett til innsyn kommer også inn.

Opplysningspliktregler kan gjenspeile interessen i fullstendighet. Kvaliteten i beslutningsgrunnlaget søkes styrket gjennom forvaltningslovens krav til opplysning av saken før vedtak treffes. Eksempler på dette finnes i Ligningsloven kap. 6 og Lov om sosial omsorg § 20.

Lov om personregistre m.m. av 9. juni 1978 inneholder ingen egen programmerklæring, formålsangivelse eller generalklausul. I forarbeidene er det gjort forsøk på å definere hvilke interesser en personvernlovgivning må ta sikte på å beskytte.

Sandvik-utvalget peker på at begrepet "personlig integritet" er mangetydig og gis varierende meningsinnhold i den offentlige debatt omkring personopplysninger og databehandling. I denne sammenheng hevdes det gjerne at kravet om personlig integritet bl.a. bør innebære at en må ha rett til å avvise en så detaljert registrering av egne persondata at de sammenlagt gir et nærgående mer eller mindre fullstendig bilde av hva en som individ står for i alle viktige relasjoner". Utvalget peker på at selv om det finnes regler som beskytter mot rettstridig innsamling av opplysninger, så er ikke besittelsen rettstridig. Latent fare for misbruk hadde til da ikke ført til rettsregler som forhindrer innsamling.

Utvalget tar som utgangspunkt den enkeltes rett til å influere på bruken av opplysninger som gjelder ham selv. Samlivet i samfunnet medfører at den enkelte blir tvunget til å gi opplysninger og i en del sammenhenger ønsker å gi opplysninger. Registrering må knyttes til behov sett i relasjon til formål. Det advares også mot å bruke opplysninger fra en kontekst i en annen. Diskresjonsplikt er en nødvendig forutsetning. Utvalget avviser å sette klart forbud mot registrering av visse typer opplysninger. Relasjonen må avgjøre nødvendigheten av å registrere en følsom opplysning. Hovedkjernen i dette utvalgets forslag til Lov om innsamling, registrering, bruk og meddelelse av opplysninger i privat virksomhet ble en relevansregel og en diskresjonsregel (taushetspliktregel).

Seip-utvalget peker på utgangspunktet "privatlivets fred"

eller "personlig integritet". Personvernet er å beskytte individet mot utilbørlige inngrep i integriteten. Grunntanken er at den enkelte skal ha en fredet sektor som offentlige myndigheter og andre utenforstående ikke skal kunne gripe inn i. Utvalget fant det ikke formålstjenlig å definere begrepet. En definisjon vil ikke gi noe svar på den praktiske avveining som må foretas mellom individets behov for kontroll og samfunnets interesse i å nytte de data det er spørsmål om.

Sten Markgren, forsker ved Umeå universitet, har i sitt doktorgradarbeide vurdert den svenske Datatinspektionens arbeid i årene 1976 til 1978. Han drøfter blant annet personvernbegrepet i teori, lovgivning og praksis. Han vurderer praksis mot lovgivers intensjoner.

Integritetsskyddskomiteens første og andre delbetenkning forsøker følgende definisjon av integritetsvern: "Den enkeltes krav på at informasjonen om hans private forhold ikke skal være tilgjengelig for eller kunne brukes av utenforstående uten hans vilje."

Datasamordningskomiteens definisjon lyder: "En rett til privatliv som ikke myndighetene eller noen annen skal kunne trenge seg inn i. I dette inngår at individet suverent skal kunne bestemme over hvordan opplysninger om ham og hans privatliv blir anvendt og også ha rett å holde slike opplysninger for seg selv".

Datalagens formål er å hindre at utilbørlig inntrengen i den personlige integritet oppstår ved EDB. Utilbørlig er definert som ubegrunnet eller svakt begrunnet. Hva som er utilbørlig inntrengen bør oppfattes som et fenomen med grader, der graden avgjøres ut fra informasjonens art, aktualitetsgrad, korrekthet, bruk og hvilket formål den skal anvendes til, videre lagring og bearbeiding.

Det følger av prl § 1 at personvernproblemene ikke bare knyttes til EDB, men til manuelle registre også. Og juridiske personer får også nytte godt av lovens vern. Dette representerer en utvidelse i forhold til det teoretiske personvernbegrepet som i hovedsak har vært knyttet til fysiske personers interesser.

§ 6 er en relevansregel og gjelder alle personregistre. Registrering av personopplysninger skal være saklig begrunnet ut fra hensynet til administrasjon og virksomhet i det organ som foretar registreringen. En skjerpet relevansregel gjelder for registrering av nærmere spesifiserte følsomme opplysninger, se prl § 6.2.

Relevansregelen ivaretar diskresjonsinteressen i form av en prinsippklæring som samtidig er en norm uten skarpe grenser. Men den knyttes til registrators behov. En konkret vurdering av en type opplysning mot relevansregelen bør ta utgangspunkt i det. Men vurderingen blir relasjonsorientert. Det er ikke nødvendigvis slik at det for alle registrerte foreligger tilstrekkelig relevans. Arbeidsformidlingen kan

trengte flere opplysninger om arbeidssøker Hansen som skal i vernet arbeid enn om Olsen som er en "ordinær" søker. Opplysning om seksuell legning kan være relevant for homoseksuelle rekrutter som av den grunn ønsker fritak fra tjeneste, men ikke som generell opplysningstype. Av betydning for relevansvurdering er ikke bare interne rutiner, men også forhold til omverden. Registratør kan være pålagt i lovgivning eller ved avtaler å innhente og registrere visse opplysninger.

Diskresjonsinteressen ivaretas også av andre paragrafer, som f.eks. prl §§ 10 og 11, som gjelder konsesjonsbehandlingen. I lys av relevansregelen i § 6 skal det vurderes om opprettelse og bruk av et personregister kan volde problemer for den enkelte som ikke kan løses tilfredsstillende ved vilkår satt i henhold til prl § 11. Flere av de angitte vilkår vil dreie seg om sikring av diskresjonsinteressene. Forskriftenes kapittel 2 fritar en del typer registre fra konsesjonsplikten, men på konsesjonslignende vilkår.

Videre finnes diskresjonsregler i §§ 15, 16, 17 og 18 som gjelder kredittopplysningsforetak. § 4-3 i forskriftene setter forbud mot fødselsnummer utenpå postsendinger fra kredittopplysningsbyråer, og tilsvarende regel er satt for registre regulert i kapittel 2 i forskriftene, f.eks. bankers kunderegistre og lønnstaker- personalregistre.

For databasebehandlingsforetak gjelder § 23, som begrenser bruken av opplysninger til de formål oppdragsgiver har angitt. For adresseringsforetak er § 26, jfr § 27, særlig diskresjon ved følsomme opplysninger, og § 28 om sletting i adresseregistre, typiske diskresjonsregler. Utdyping og utvidelse av reglene finnes i forskriftenes kap. 6. § 32 og § 33, se også forskriftenes kap. 7 ivaretar diskresjonsinteressen for deltakerer i markeds- og opinionsundersøkelser og endelig § 36 som regulerer overføring av personregistre/personopplysninger til utlandet.

Prl § 8 bidrar til håndheving av relevansnormen. Dersom det ikke er adgang til å innta en opplysning etter relevansvurderingen skal opplysningen slettes. Datatilsynet kan gi pålegg om sletting. Prl § 8 gjenspeiler diskresjonsinteressen også i det at opplysninger skal slettes når de ikke lenger har betydning og kan få betydning for den registrerte.

Interessen i fullstendighet ivaretas blant annet ved at uriktige eller ufullstendige opplysninger skal rettes eller suppleres. Regulering av interessen i fullstendighet finnes også i prl § 11 og prl § 15.

Prl § 7 gir den enkelte rett til innsyn i hva som er registrert om seg selv, se også forskriftenes kap. 1. § 1-5 i forskriftene er eksempel på at adgangen til å utvide området for innsyn er nyttet, jfr prl § 7.4. Egne innsynsrettsregler finnes i prl § 19, gjenpart av kredittopplysninger, § 20, innsynsrett i kredittopplysninger og § 28, opplysning om kilde.

For å kunne finne fram til registre, skal det føres en

offentlig tilgjengelig oversikt over konsesjonspliktige registre, se prl § 4.

2.3.3 Personvern i enkeltvedtak etter personregisterloven

Datatilsynet har siden 1980 rimeligvis fått en rik praksis å hente fra. Noen saker vil bli trukket fram som eksempler på vurderinger der de ulike personverninteressene har kommet fram. Eksemplene er stort sett hentet fra styrevedtak, men bredere presentasjon vil komme under drøftingen av de enkelte paragrafer i loven.

Gjennomgående har Datatilsynet vist stor forsiktighet med å tillate registrering av fødselsnummer, et uttrykk for ivaretagelse av diskresjonsinteressen.

Et flertall i styret gikk imot at fødselsnummer skulle stå på masseutskrifter fra Løsøreregistret.

Det ble gitt konsesjon til opprettelse av adresseregistre til utgivelse av Veivisere forutsatt at folk i kommunen fikk underretning om den planlagte utgivelsen slik at de kunne reservere seg. En person som ved en feil ble tatt med, krevde erstatning på kr. 30.000, idet han måtte flytte etter at adressen var gjort kjent for almenheten.

Det ble i en sak som gjaldt opprettelse av personregister i forskningsøyemed slått fast at oppbevaring til senere undersøkelser kunne foretas dersom navneregister og opplysningene forøvrig ble oppbevart atskilt på betryggende måte.

Den såkalte båtavgiftsaken dreide seg om Toll- og avgiftsdirektoratet skulle få lovhjemmel til innhenting av opplysninger om forsikrede lystbåter. Slik hjemmel ble gitt, men under forutsetning av at opplysningene ble brukt til kontroll av om båtavgift ble betalt. Skattemyndighetene viste imidlertid til den nye ligningsloven § 6-13, og gjeldende skl § 66 og mente vilkåret i praksis avskar deres lovhjemlete rett til opplysninger fra offentlige myndigheter.

Smokeenders, et røykeavvenningsforetak, fikk vesentlig beskåret sin liste over opplysninger de ønsket å registrere. Den skjerpete relevansregelen i prl § 6.2 kom til anvendelse.

Opplysning om NS-medlemskap i Justisdepartementets advokatregister ble ansett som nødvendig idet opplysningen hadde betydning for om advokatbevilling kunne gis. Men det ble innført særskilt slettingsbestemmelse.

Norges Blindforbund krevde utfyllt et omfattende skjema for sosialtjenesten selv om man bare skulle låne bøker i blindebiblioteket. Denne "kobling" ble ansett for å være

i strid med formål/relevans.

De fleste sakene som er knyttet til fullstendighetsinteressen er av tre kategorier. Det er sosialrapporter som finnes i sosialkontorenes klientarkiver, det er kredittopplysningsregistre og endelig ligningsetatens kontrollvirksomhet.

En sosialrapport vil kunne være et dokument som er utarbeidet av kurator etter hjembesøk. Datatilsynet har påvist at det ofte er laget bilder av familiesituasjon som bygger på sviktende grunnlag. Det er tildels en tendens til generalisering ut fra enkeltepisoder, manglende kildehenvisninger og manglende sonndring mellom vurderinger og fakta.

I forbindelse med kontroll av kredittopplysningsforetak er det påvist usikker identifikasjon med forvekslingsfare, og manglende opplysning om at en misligholdt fordring er omstridt eller oppgjort.

Ligningsmyndighetenes kontroll med skattyterne har vært gjenstand for omfattende diskusjon. Fare for uriktig sammenstilling av opplysninger på grunn av sviktende identifikasjon og usikkerhet med hensyn til hvilken informasjon en bestemt opplysning representerer er sentral.

Det er naturlig å ta for seg hvilke begrensninger som ved enkeltvedtak er foretatt i innsynsretten og eventuelle utvidelser. Dette gjelder interessen i opplysthet.

Det er gitt unntak fra innsynsretten etter prl § 7 for adopsjonsregistret i Justisdepartementet. Innsyn i skatteetatens personregistre er begrenset slik at det ikke er innsyn i siste års ligning inntil behandlingen er avsluttet, og ligningsloven § 3-4 skal danne rammen for innsyn i manuelle registre. Søknader om unntak fra innsyn i politiets registre er under behandling. Det er gjort unntak fra innsynsrett i sosialkontorenes klientregistre på visse vilkår hva angår opplysninger som kan røpe kilde for opplysninger. IBM har fått unntak fra innsynsrett i leverandøropplysninger i kunderegistret.

Innsynsretten er utvidet i noen sammenhenger ved at registreierer er pålagt å forelegge opplysninger for den registrerte. Elevmappen skal f.eks. forelegges en gang i året.

Et vanlig vilkår i konsesjon for forskningsregistre er at de registrerte skal forespørres før opplysninger om dem innhentes.

Registrerte i kredittopplysningsregistre skal ha kopi av kredittopplysninger som gis om dem, dersom de er privatpersoner, se prl § 19. Det ble i et tilfelle dispensert fra denne plikten forutsatt at mottaker sendte

gjenpart.

I et tilfelle ble det satt som vilkår i konsesjon for et forskningsregister at rapport med anonymiserte opplysninger skulle gis de registrerte til kontroll før utgivelse. Dette vilkåret er for såvidt knyttet til såvel diskresjons- som opplysthetsinteresse.

Det foreligger også eksempler på konflikt med interessen i et borgervennlig samfunn.

Ved et sykehuslaboratorium ble prøver fra pasienter returnert fordi legen ikke hadde påført fødselsnummer. Fødselsnummer var det eneste søkekriterium EDB-systemet aksepterte. Den praktiske løsning ble at prøveanalyse ble foretatt selv om fødselsnummer manglet, men resultatet ble ikke registrert i EDB-registret.

I Oslo kommune har man innført et register for tildeling av barnehageplasser. Den opprinnelige systemløsning forutsatte at barna skulle stilles i datokø etter fødselsdato og bak de prioriterte. Søknadsskjemaet ble enklere, men samtidig ble det mindre rom for vurdering av plassbehov ut fra totalvurderinger. Men kommunen kunne selv velge hvilke kriterier som skulle legges til grunn.

Automatiserte beslutningsprosesser generelt kan føre til økt avstand mellom publikum og beslutning og det frie skjønn (mer eller mindre) vil lett forsvinne. Beslutningene vil lettere fortone seg som urimelige. Et kjent eksempel fra 70-årene er innføringen av automatisert beslutningssystem for bostøtte. Stor saksmengde medfører ofte at rettsikkerhetsgarantier blir lempet på. I perioden med prisstopp 1978-79 ble såvel grunnlegingsplikt som klageadgang suspendert hva angikk søknader om dispensasjon fra prisstoppen.

Publikum bør ha lett tilgang til opplysninger om seg selv og det innebærer også at utskrifter må være i klartekst og på språk man skjønner.

Videre foreligger det eksempler på krenkelse av interessen i å unngå overdreven kontroll eller uhjemlet maktbruk.

Datatilsynet uttalte seg sterkt imot innføring av rom-avlytting. I tillegg til at interesser i diskresjon, opplysthet og fullstendighet ville kunne bli krenket, var overvåkningsaspektet sterkt framme. For å bekjempe narkotikaondet skulle en streng kontrollmekanisme innføres.

De samme hensyn gjorde seg også gjeldende i vurdering av automatisk trafikkovervåkning.

Datatilsynet har gjentatte ganger vurdert i hvilken grad det skal være tillatt å registrere oppringt telefonnummer i såkalte telefondebiteringssystemer. På hoteller har behovet vært tilstede, mens det for arbeidsplassers vedkommende

normalt ikke har foreligget slikt behov at konsesjon er gitt. Hensikten med slikt utstyr kan være å få dokumentert overfor brukeren hvilke samtaler han har hatt, men en overordnet disiplinerings-effekt kan også spores. Videoovervåkning har gitt grunn til restriktive vurderinger. Datatilsynet har foreslått at Justisdepartementet utreder behovet for lovregulering.

2.3.4 Datatilsynets personvernbegrep

Datatilsynet har så vidt vites aldri forsøkt å gi noen presisering av hva personvern er. Men alle de interesser som er nevnt foran er momenter i avveiningene ved konsesjonsgiving.

Diskresjonsinteressen er den dominerende faktor. Ved konsesjonsbehandling har svært mye av oppmerksomheten vært knyttet til hvilke typer opplysninger et register kan inneholde. Det er få eksempler på avslåtte konsesjonssøknader, men "sensur" av innholdet er forholdsvis vanlig. Dette gjør seg mest gjeldende i administrative systemer. Bare unntaksvis er innholdet i forskningsregistre vurdert. Dette har delvis sammenheng med at det er vanskelig å overprøve relevans i forskningsprosjekter og delvis sammenheng med en noe forsiktig holdning til faglig kontroll med forskning. Men slettingsregler blir normalt fastsatt.

Diskresjonshensynet har etterhvert også kommet klarere fram ved korte slettingsfrister for følsomme opplysninger. I de tidligste sakene ble vilkår om sletting av opplysninger stort sett bare en henvisning til den generelle slettingsregel i prl § 8.

Det er i varierende grad presisert hvem som skal ha tilgang til opplysninger. Delvis er en "need to know"-formulering nyttet, mens det særlig i forskningsprosjekter er foretatt mer konkret angivelse.

Det er i konsesjonene inntatt et punkt om hva registret kan brukes til. En slik bruks-/formålsangivelse har ofte ikke gjenspeilet den utlevering av opplysninger som skjer fra registret. Punktene om bruk, utlevering og kobling må derfor som regel vurderes under ett for å kunne se formålet med registret.

Fullstendighetsinteressen har i den senere tid kommet mer i fokus. Dette gjelder bl.a. i saker om mangelfulle sosialrapporter og kredittopplysningsregistre. Bevissthet på entydig identifikasjon har preget bl.a. holdningen til fødselsnummer i kredittopplysningsregistre og ved kobling i skatteetaten. Krav til ajourhold av registre har også blitt skjerpet. Når det skal vurderes om samkjøring/kobling av registre skal tillates, har datakvaliteten stor betydning. Videre bør den registrerte ha kunnskap om samkjøringen og resultatet av denne.

Datatilsynet har vært restriktivt med å gi unntak fra innsynsrett. Interessen i opplysthet er ivaretatt godt, men særegent er det at Datatilsynet ikke kan gi pålegg om at innsyn skal gis. I forbindelse med en utredning om barnemishandling og omsorgssvikt ble det foreslått at personer som ga opplysninger ved mistanke om mishandling skulle være sikret full anonymitet. Datatilsynet pekte på det betenkelige i dette.

Interessen i en borgervennlig administrasjon kan spores i argumentasjonen rundt enkeltsaker. Problematikken med omvendt bevisbyrde har flere ganger vært fremme i diskusjonene. Gjennom samkjøring av registre kan administrasjonen gjøre "funn" som indikerer at borgeren ikke har rent mel i posen. Borgeren må så påvise hvordan de faktiske forhold er. I Sverige førte nylig en samkjøring i kontrollformål til at oppunder 1000 personer ble anmeldt for å ha mottatt bostadsbidrag ulovlig. Tross innsigelser fra en tjenestemann i politiet om at uriktig inntektsbegrep var nyttet ble det først ved rettergangen fastslått at så var tilfelle.

Datatilsynet har generelt og i forbindelse med enkeltsaker påpekt utviklingen mot et strammere samfunn. Den gode hensikt er pådriver for nye kontrolltiltak.

Selmer har i senere teori pekt på Datatilsynets legalitetskontrollerende virksomhet. Den fri evaluering av personverninteressene mot registreiers/samfunnets behov får lett lodd på den ene eller annen vektskål etter lovgivning. Dersom det i en formell lov fastslås at et register med opplysning om straffbart forhold skal føres, settes relevansvurderingen etter prl § 6.2 lett ut av kraft. Ulike opplysningspliktregler kan forutsette en utleveringsadgang som krenker diskresjonsinteressen. Et annet spørsmål er om det kan være grunn til å stille spørsmål ved hjemmelen for selve den virksomhet som ligger til grunn for en registrering. (Selmer har, etter at denne framstilling ble laget, i innledningen til "Personregisterloven med kommentarer" TANO 1987 gjennomgått personvernbegrepet og utvidet det noe.)

I en sak som gjaldt register over innsatte i fylle-arresten ble det lagt vekt på at det ikke var nødvendig å føre eget register, jfr prl § 6.2. Dette fordi selve innbringelsen sto i den kronologisk vaktjournal og at fyll i seg selv ikke var straffbar handling. Men et tilleggshensyn ble trukket inn: Registreringen hadde elementer av sosial urettferdighet i seg. Et argument for registreringen var at opplysninger om opphold i fyllearrest skulle brukes ved utstedelse av våpentillatelse. Det forelå en krenkelse av et likhetshensyn, samtidig som registret var ufullstendig i og med at det ikke inneholdt alle personer med en høy promille.

Relevansregelen i prl § 6 er som tidligere nevnt en diskresjonsregel, men samtidig markeres en interesse i definert formål; "...saklig begrunnet ut fra hensynet til

administrasjon og virksomhet i det organ eller foretak som foretar registreringen." Prl § 9 angir også at det i en konsesjon skal fastsettes hva et register kan brukes til. § 2-1 nr 1 i forskriftene til prl setter som vilkår for konsesjonsfritak at registret "ikke brukes til annet formål enn det som..."

På det internasjonale datatilsynsjefmøte i London 1982 ble det fastslått som prinsipp at opplysninger skal brukes til de formål de er innhentet for.

I forbindelse med diskusjonen om listbroking av kunde- og adresseregistre har også formålsdebatten vært i fokus.

Klart definert formål er sentralt for ivaretagelse av personverninteressene. Diskresjon, fullstendighet og opplysthetsinteresser som ikke kan utøves meningsfylt uten at det knyttes til hva opplysningene skal brukes til.

Formålet med et register vil være en viss bruk av personopplysninger til en bestemt administrativ-, kontroll- eller forskningsoppgave. Formålet vil ofte være politisk bestemt og typer opplysninger vil ofte følge av de kriterier som skal tillegges vekt. Formålet kan i seg selv være uakseptabelt ut fra personvern hensyn. Medisinsk fødselsregister har et administrativt og forskningsmessig formål. I Norge ville registret ikke være akseptabelt dersom formålet var å sterilisere alle som hadde fått et barn.

Det ideelle utgangspunkt og praksis.

"Den mulige interesse den enkelte har i å føre kontroll med den informasjon som beskriver dem selv", er som nevnt foran en definisjon av personvern.

Den enkelte har gjennom sin kontakt med registreierne en viss mulighet til å reagere på feil. Lønnsslipper, kontoutskrifter, adressetiketter gir mulighet til kontroll fra individets side.

Utlevering av opplysninger krever ofte hans samtykke, men i stadig større grad erstattes individuelt samtykke med opplysningsplikt registreiere imellom. Deltakelsen i samfunnet medfører en viss avgivelse av opplysninger, dels for å oppnå gode deler etter plikt.

I noen få tilfelle har individet en reell disposisjonsrett over sine opplysninger. Han kan kreve seg slettet i adresseregistre og han kan nekte forskere å få opplysninger om ham. Han har mulighet til bestemme over "sine" opplysninger.

Innsynsretten brukes lite, noe som dels beror på manglende kjennskap til rettigheten.

Datatilsynet, personregisterlovgivningen, annen lovgivning

og avtaleverk må derfor i stort monn forsøke å ivareta individets personverninteresser.

2.4 Teknisk utvikling og dens innvirkning på personvernet

Personvernet påvirkes av to hovedkilder: politisk/ kulturell- og teknisk utvikling. Her er det ingen vits å spå om framtidige politiske spiraler. Men det er høyst relevant å se noe på nært forestående teknisk utvikling og bruk. Det er tilstrekkelig å vise til de muligheter fritekstsøking åpner, distribuerte informasjonssystemer med personinformasjon, kommunikasjon av personopplysninger, digitaliserte bilder etc.

Ethvert arbeid med regler om personregistre må ha et våkent øye for ny teknologisk forandring av personvernbehovet. Prosjektgruppa har ikke tatt seg tid til å diskutere dette.

2.5 Ajourføring av personvernbegrepet.

Det kan være av interesse å spørre om ikke personvernteorien bør oppdateres. Denne oppgaven har ikke prosjektet drøftet.

(1) Rådende personvernteori

Personvern kan sies å omfatte en persons interesse i å utøve kontroll med opplysninger om seg selv (Blekeli:229) og vern om privatlivets fred (Selmer:9).

Personvernet blir her antatt å omfatte en annen person eller etats ivarettelse av registrerte personers interesser. Dette er et noe vanskelig forhold, først og fremst fordi det ikke er noen gitt å ha en dyp formening om en annens persons interesse uten å kjenne personen nærmere. Dermed vil det være stor variasjon mellom personer vedrørende hva som faktisk er deres interesser i samme situasjon. Derfor vil det å ta personvern hensyn i større eller mindre grad bygge på antakelser om andre personers ønsker.

Dette punkt diskuteres ikke nærmere.

Knut S Selmer har avgrenset personvern til også å omfatte en interesse i at opplysninger ikke brukes til overdreven kontroll eller maktmisbruk og en interesse i borgervennlig forvaltning.

I forordet til kommentarene til personregisterloven har Selmer presisert personvernbegrepet slik at det også omfatter en interesse i robust forvaltning.

Disse tre interessene kan noe mer generelt formuleres som en interesse knyttet til registreiers bruk av registeret.

Interessen i kontroll med opplysninger om seg selv presiseres gjerne til interesser i diskresjon, fullstendighet (og korrekthet) og opplysthet.

Diskresjonsinteressen er virksom i spørsmål om hva som kan legges, utleveres, hvem som kan få tilgang til data, m.m. Fullstendighetsinteressen er særlig virksom i beslutningssituasjoner: man skal ha tilstrekkelig grunnlag for å treffe sin beslutning - og grunnlaget skal være riktig. Både interessene i diskresjon og fullstendighet er relative til en eller annen bruk av opplysninger. Diskresjonsinteressen vil f.eks. variere for de samme data avhengig av bruk.

Opplysthet er en forutsetning for at en person skal kunne utøve en kontroll med opplysninger om seg selv og omfatter hvem som har opplysninger, hva som finnes, og hvorfor det finnes lagret.

I arbeidet med utkastet til sikringsforskrift har det vært et ønske å relatere sikringskravene til personvernteorien. Dette har vært mulig, men relasjonene er blitt noe svakere enn det en kunne ønske seg.

Arbeidsgruppe har konsentrert seg om å utforme regler for å sikre registre mot kompromittering, sikre kvaliteten av personopplysninger og å sikre tilgjengelighet av personopplysninger.

Kvalitet og tilgjengelighet relateres til fullstendighetsbegrepet. Mens kompromittering nærmest pr. def. er diskresjonsbrudd.

Diskresjonsbrudd kan skje ved at en registrerer for mange opplysningstyper, ved at en legger vekt på irrelevante hensyn, ved at uvedkommende får tilgang til opplysninger, m.m. Mens kompromittering utelukkende er knyttet til det sieste forhold.

Det er forøvrigt ikke noe problem når forskriften dekker ett snere område enn det personvernet omfatter. Det er verre når det motsatte er tilfelle (etter teorien).

Fullstendighetsinteresse er en rent for snever formulering av en kvalitetsinteresse som personvernet bør omfatte, men som ikke er artikulert i teorien. Det bør være en del av personvernet at personopplysninger har tilstrekkelig god kvalitet for det formål de skal nyttes. Dvs. at en person har en interesse i kvalitet av opplysninger om seg selv. Dette omfatter kvalitet i datamodell.

data og tolkning.

Krav til tilgjengelighet av data kan utledes av den presiserte interesse i robust forvaltning.

Personvernteorien bygger på et ganske relativt interesse-begrep. En person har oftest (ikke alltid) en interesse i at det skal legges vekt på relevante opplysninger og ha et fullstendig beslutningsgrunnlag. Unntak er situasjoner der det legges vekt på fordelaktige irrelevante momenter eller der ufordelaktige relevante opplysninger mangler. Med andre ord har en person først og fremst en interesse i et så fordelaktig resultat som mulig, med hensyn til en gitt beslutning.

(2) Alternativ formulering av personvernet

En kunne alternativt premisere den del av personvernet som har med kontroll av opplysninger om seg selv og gjøre til kontroll med (1) produksjon, (2) distribusjon, (3) kvalitet, (4) bruk, (5) lagring, (6) vedlikehold og (7) sletting av personopplysninger.

Om en person hadde fullstendig kontroll med alle disse interesser, så ville (8) innsynsrett være overflødig. Siden dette ikke kan være tilfelle, er innsyn en nødvendighet for personens videre kontroll.

Denne opplistingen kan sammenlignes med Blekeli's opplisting av komponenter i "informasjonssirkulasjonen" (Blekeli:232) i innsamling, bruk, lagring og utlevering.

I forbindelse med produksjon av data er den del av personvernet som har med privtlivets fred å gjøre aktuell.

Også andre aktører enn personen selv kan ha legitime interesser i å utøve kontroll med opplysninger om den aktuelle person. Disse interessene kan av og til kollidere med hverandre.

Fullstendighets- og diskresjonsinteressene er gjerne aktuelle ved produksjon, bruk, lagring og distribusjonspunktene i forslaget.

En fordel med den alternative formulering av interessene er at disse interesser er mindre relative (altså mer absolutte) enn fullstendighets- og diskresjonsinteressene.

En annen fordel er at den tydeliggjør mulige konflikter mellom de kontrollinteressene forskjellige aktører kan ha med de samme opplysninger. Dette gir for eksempel god veiledning for Datatilsynet, som må avveie forskjellige hensyn der konfliktene dominerer.

Dessuten fokuseres de ulike faser i dataenes "livsløp" i større grad i den alternative formulering. Dette er nyttig fordi forskjellige problemer reises ved hver av fasene. Ser vi nærmere på bruks-punktet, må omfatter dette begrensning av bruk til bestemte formål. Skal dataene nyttes til andre formål, kan en i prinsippet tenke seg at dette ligger eksklusivt innenfor den registrertes kontroll (samtykke kreves) eller at kontrollen ikke er eksklusiv (alternative samtykker).

Med hensyn til avveining av motstridende interesser vedrørende hvilke opplysninger som kan registreres, brukes til et bestemt formål, etc., så vil både diskresjons- og fullstendighetsinteresser komme inn. Mens diskresjon tjener til å begrense registrering så tjener fullstendighet til å sikre at et minimum av opplysninger finnes.

I tillegg til interessene (1)-(6) foran virker overordnede interesser i (9) diskresjon og (10) fullstendighet inn ved fasene (1)-(7) ovenfor.

Resultatet av Datatilsynets avveiling av kolliderende interesser mellom ulike aktører vedrørende diskresjon og fullstendighet vil sterkt avhenge av formålet med (1)-(7).

(8) opplysthet er en forutsetning for å kunne utøve den øvrige kontroll.

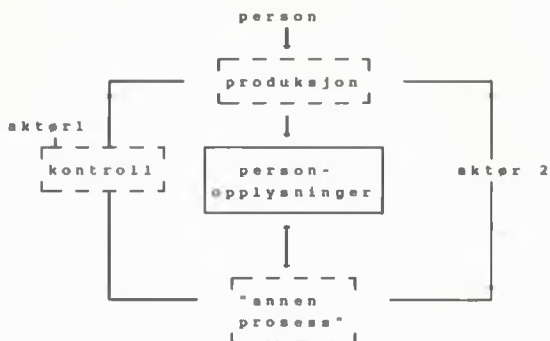
Selters tre presiseringer: interesser

- mot overdreven kontroll og maktmisbruk
- i borgervennlig forvaltning
- i robust forvaltning

angår antakelig alle punkt (4) over.

Interessen i privatlivets fred berøres bare i liten grad av disse vurderinger.

Følgende figur kan være nyttig ved diskusjonen av personvernbegrepet:



I figuren betyr stiplede bokser prosesser, mens heltrukne betyr produkter. En enslig pil angir en opplysningsstrøm, mens de rettede kanter angir at en aktør utøver en prosess. Aktør 2 kan for eksempel produsere personopplysninger. I det tilfelle at prosessen er kontroll er meningsvidere at det utøves kontroll med produksjon eller med "annen prosess". "Annen prosess" kan være distribusjon, bruk, vedlikehold, lagring, sletting eller bearbeidning.

I "personvern-spillet" fra figuren, er det i tillegg til den registrerte, kalt personen, to viktige posisjoner. En utøverposisjon, kalt aktør 2, og en kontrollposisjon kalt aktør 1. Utøveren utfører (eller er interessert i å utføre) en aktivitet der personopplysningene er, eller for produksjon: blir, "gjenstand" for aktiviteten. Kontrollposisjonen får sitt innhold bestemt av å skulle kontrollere den primære aktivitet, nevnt foran.

En aktør som er i utøverposisjon i en sammenheng, kan være i kontrollposisjon i en annen. Registrereier er i utøverposisjon i forhold til Datatilsynet ved konsesjonssøknad og gjerne i kontrollposisjon i forhold til registerbrukerne.

Både i utøverposisjon og kontrollposisjon vil det normalt være flere aktører samtidig. De har forskjellige roller og utfører forskjellige aktiviteter. Samme opplysning kan være lokalisert flere steder, f.eks. i flere registre, med flere registreiere og ansvarelige i kontrollposisjoner, og med forskjellige brukere, dvs. aktører i utøverposisjon.

Det kan skilles mellom flere betydninger av kontroll-betegnelsen: å gi regler (kontroll i forkent), faktisk kontroll (kontroll i øyeblikket) og kontroll i ettertid.

Ulike regler kan regulere bruk av personopplysninger på et generelt plan. Regelgiver kan være Storting, departementer, Datatilsynet og øvrige myndigheter, firmaer, m fl.

I forhold til konkret bruk kan en person (eller flere) ha den faktiske kontroll med om bruk kan finne sted. Akter 2's anledning til å utføre en aktivitet er da avhengig av akter 1's tillatelse.

(3) En ny personverndebatt?

Bruk av informasjonsteknologi er ennå i et tidlig utviklingstrinn. Men endel erfaringer har men troes på. Kanskje kan det være nyttig å oppsummere erfaringer og staks ut veien videre.

Det kan være nyttig å granske hvem som har hva slags kontroll vedrørende fasene (1)-(7). Særlig interessante aktører er den registrerte, registeransvarlig og registreier, Datatilsynet og øvrige myndigheter. Det kan også være nyttig å spørre om det burde skje endringer av kontrollmulighetene for enkelte av aktørene.

Videre kan det være nyttig å spørre hvilke kontrollinstrumenter de ulike aktører har - og eventuelt om det er ønskelig å endre disse. Særlig er spørsmålet aktuelt for de registrerte.

3 OM SIKKERHET OG SIKRING

3.1 Sikkerhet og risiko.

Det er forbløffende å oppdage hvor ofte ordet sikkerhet brukes. Det fins knapt ei avis eller nyhetssending der sikkerhet ikke er tema. Noen av de vante sammenhenger sikkerhet forekommer i er: mot ulykker i hjemmet, - på arbeidsplassen, - i trafikken, - i verdenssamfunnet: Sikkerhetsrådet, osv. Og i det siste oftere og oftere EDB-sikkerhet eller informasjonssikkerhet.

Dette kommer av at mennesker foretrekker å leve med så få trusler mot seg og sitt som råd er. Vi lever bedre i trygghet - og sikkerhet er med på å realisere trygghet.

Det er ønskelig å operere med praktiske definisjoner av sikkerhet. Avhengig av sikkerhetsproblemenes natur vil ulike definisjoner være velegnet. Donn B Parker sier at "Security is made up of six functions: avoidance, deterrence, prevention, detection, recovery and correction", (Parker:40).

Vi kunne definere sikkerhet, $s(t)$, som sannsynlighete for at en uønsket hendelse ikke inntreffer innen et tidsintervall t . Dette ville samstemme ganske bra med Parkers avgrensning. Risiko, $r(t)$, definerer vi som sannsynlighete for at en uønsket hendelse inntreffer i løpet av et tiderom, t , multiplisert med konsekvensene, k , av at den inntreffer.

$$r(t) = (1-s(t)) \cdot k.$$

Konsekvensene kan være økonomiske, personvernsmessige o.s.v., og tenkes her projisert inn på en dimensjon.

Om hendelsene er av en slik natur at de kan øke gjentatte ganger trengs en modifisert definisjon av sikkerhet og risiko.

Det kan være ønskelig å la sikkerheten omfatte sårbarhet også. La oss derfor definere sikkerhet som evnen til å unngå og motstå trusler og å få ønskede hendelser til å inntreffe eller tilstander til å vare ved. For den defensive delen er det evnen til å avdekke, varsle og fjerne, redusere eller bekjempe trusler og til å begrense skadene om trusler realiseres.

3.2 Sikring

Med å sikre kan vi forstå 'å sørge for høg sikkerhet for'.

En vil f eks sikre at tilstander skal vare, f eks at personverninteresser opprettholdes, eller at hendelser skal inntreffe, dørene låses ved arbeidstidas slutt, oppgaver løses, m.m.

3.2.1 Sikring av personvern

(1) Aktører

For personvernsituasjonen er det mange aktører som spiller en sentral rolle. Storting, Justisdepartement, Datatilsynet, registreier, eier av EDB-anlegg, eier av foretak, ansatte hos de forskjellige aktører, m fl.

(2) Intensjoner, "policy" og direktiver.

En aktør kan ha en personvernintensjon. Han kan sikre denne noe ved å utforme en "policy". Intensjonen sikres ytterligere ved å utforme direktiver for å realisere policyen. Vi kunne kalle dette horisontal sikring av personvern.

(3) Kompetansehierarkiet ved realisering av personvern.

Stortinget har gitt Personregisterloven av 9. juni 1978. Dette er det viktigste personverninstrument. Justisdepartementet gir forskrifter til loven og forestår behandling av klager på vedtak i Datatilsynet. Datatilsynet gir konsesjoner for føring av personregistre og enkelte typer virksomheter. Datatilsynet fatter også enkeltvedtak med virkning for konsesjonsinnehaver. Bruker (la det være registreier eller et foretak) kan så igjen gi interne direktiver som angår personvernet.



S: Storting

J: Justisdepartement

D: Datatilsyn

B: Bruker

a → b: a gir b direktiver

Vi kan si at vi har ei vertikal sikring av personvern når Stortinget gir personvernnormer for Justisdepartementet, Datatilsynet eller brukere. Eller når Datatilsynet gir pålegg i konsesjon til f eks registreier.

(4) Kontroll

For virkelig å forsikre seg om at direktiver er virksomme må en kontrollere at de etterleves. Kontrollen gjelder da først

og fremst den vertikale sikring.

Kontroll med den horisontale sikring vil bestå i å vurdere om egne direktiver svarer til intensjonen. Denne type kontroll vil da oftest være mindre vesentlig og omfattende.

Stortingets personvern-kontroll skjer ved diskusjon av Datatilsynets årsmelding, ved spørsmål til statsråden, ved den løpende personverndebatt i media, m.m.

Justisdepartementet kontrollerer Datatilsynet bl a gjennom behandlingen av klager på vedtak i Datatilsynet.

Den mest omfattende kontroll i personvernsammenheng er det likevel Datatilsynet som foretar, når registreiers eller foretaks etterlevelse av konsesjonene undersøkes.

4 RISIKOANALYSE AV ANLEGG OG FORETAK SOM BEHANDLER PERSON-REGISTRE.

Det er nødvendig å vurdere hvilke risiki en er utsatt for slik at en kan bli i stand til å oppnå så stor sikkerhet som en ønsker. At en ikke alltid ønsker maksimal sikkerhet er klart. Sikkerhet koster og ofte reduseres brukervennlighet og effektivitet. I dette kapittel redegjøres stikkordsmessig for risikoanalyse. Ideene er vel etablerte i sikkerhetslitteraturen. På norsk er de blant annet benyttet i heftet EDB og sikkerhet, som er utgitt av Industriens Sikkerhetsutvalg.

En risikoanalyse bør inneholde situasjonsbeskrivelse, trusselvurdering, sårbarhetsvurdering og risikovurdering.

4.1 Situasjonsbeskrivelse

En situasjonsbeskrivelse omfatter geografiske og bygningsmessige forhold, etablerte sikringstiltak, tekniske anlegg og installasjoner, dataanlegg, m m.

I forbindelse med forskriftsarbeidet bør en opprette risikotyper som har rimelig likeartete risiki.

Denne anbefaling ble ikke fulgt av arbeidsgruppe. I stedet valgte man en forenklet løsning, der man bestemmer sikkerhetstiltak ut fra sensitivitetsgrader, omgivelsene til og bruk av et register eller personopplysninger.

Ressurser som en studerer sikkerheten til bør sees på som et (relativt) strukturert sett av ressurser og operasjoner på disse.

4.2 Hvilke trusler står en ovenfor?

Trusler kan inndeles i tilsiktede og utilsiktede hendelser. Tilsiktede er spionasje, sabotasje eller skade, misbruk av data, terror, m m. Utilsiktede er brann, vannlekkasje, eksplosjon, kabel og ledningsbrudd, m m.

Truslene kan også deles inn i trusler mot funksjonalitet og mot personvernet. For oss er det den delen av sikkerheten som kan få konsekvenser for personvernet som er mest interessant. Eller mao, skal det kunne gis pålegg om sikring av drift av EDB-anlegg under personregisterloven må det være fordi personvernet er truet om sikring ikke skjer.

Situasjonen på dette punkt er klargjort i og

med Selmers presisering av at interessen i robust forvaltning også bør være en personverninteresse.

4.3 Sårbarhetsvurdering

Denne består i å vurdere konsekvensene av at de forskjellige truselhendelser inntreffer.

4.4 Risikovurdering

Det vil være en eller annen ressurs som er gjenstand for trusler eller som er utsatt for risiko. Ressurser kan være foretak, EDB-anlegg, ansatte, programmer, registre, personopplysninger, m m.

Arbeidsgruppen har supplert liste med nettverk og kommunikasjonsutstyr, operativsystem, filsystem, databaser, maskinvare, lagringamedia og periferutstyr, jfr. utkastets innholdsfortegnelse.

I arbeidet med forskriftene bør det altså opprettes risikotyper på ulike nivåer. Det foreslås at det gjøres bl a for ressursene nevnt over unntatt for ansatte.

Det bør foretas ei sensitivitetsvurdering av personregistre som legges til grunn ved fastsettelse av tiltak for hvert register. For å vinne erfaring med sensitivitetsvurderinger bør ansatte ved Datatilsynet foreta slike. Man bør lage forslag til klassifikasjon og helst gi eksempler for hver av klassene. En sensitivitetsmodell må inneholde i alle fall opplysningstype (evt. med verdier) og formål med bruk. Det er mulig at en bør operere med sensitivitetstyper for de ulike personverninteresser.

Denne antydning er ikke fulgt av arbeidsgruppen. Man opererer med tre trusselområder der sensitiviteter vurderes: kompromittering av, lav datakvalitet i og lav tilgjengelighet av personopplysninger.

5 SIKKERHETSMODELL BYGD PÅ ET RESSURSBEGREP

I dette avsnittet etableres en enkel sikkerhetsmodell bygd på et ressursbegrep. Poenget er å etablere et rammeverk som er egnet for risikoanalyser og tiltaksbeskrivelser. Det er særlig et mål å få til en klar - og egnet - begrepsdannelse og systematikk. Modellen er abstrakt formulert.

5.1 Ressurser

En ressurs kan er noe som kan bidra ved frambringelsen av et ønsket resultat (tilstand, produkt). En ressurs kan være en "råvare" i en prosess for å frambringe et endelig produkt. (Riksmålsordboka: ressurs, "noe som kan utnyttes økonomisk eller som er til nytte på annen måte".)

Det som er en ressurs i en sammenheng er ikke nødvendigvis det i en annen: Sjøppel er en ressurs i et søppelforbrenningssystem og noen steder for fattige folk, men normalt ikke. En informasjonsmengde er en ressurs i en beslutning der den trengs.

Snakker vi om ressurser i organisasjonene kan vi legge i det noe å la de faktorer som bidrar til å realisere organisasjoners mål. Siden disse målene ofte er mange, vil ressurser fra flere prosesser måtte regnes med til organisasjoners ressurser.

5.1.1 Ressursers natur

Forskjellige ressurser har ulik natur. Truslene som kan settes inn mot en ressurs vil være sterkt avhengig av dens natur.

5.1.2 Komplekse ressurser

Basale ressurser kan settes sammen til komplekse. Om et EDB-register og et program for manipulering av registeret er to ressurser, så vil de hver for seg ikke være så interessante eller kraftige. Men sammen er de kanskje en kraftig ressurs for å løse problemer som registrering, søking, oppdatering og sletting av informasjon. Sett fra en avdelingsleder for en registreringsavdeling vil en person sammen med register og program være en mer kompleks ressurs egnet til å foreta registreringer.

Sett fra adm. direktør er registreringsavdelingen en ressurs for å foreta registreringer.

Komplekse ressurser er interessante fra et sikkerhetsynsspunkt

på grunn av sammenhengene mellom en delressurs sikkerhet og helhetens. Ulike sikkerhetsproblemer vil være naturlig å studere på ulike nivåer i en kompleks ressurs. Ei fornuftig strukturering av ressurser vil også være til hjelp i sikkerhetsarbeidet.

5.2 Ressursers livsløp

Produksjon, tilegnelse, bruk, modifikasjon og avhendelse av en ressurs er faser i livsløpet til en ressurs. Fasene er interessante i sikkerhetssammenheng.

5.2.1 Produksjon av ressurs.

Å produsere en ressurs består i å frambringe den som et resultat av en prosess med mange innsatsressurser. For å oppnå sikre produkter kan det være nødvendig å kontrollere produksjonsprosessen strengt slik at en f.eks. unngår "trojanske hester" i programmer, at ukorrekt informasjon produseres og legges inn som en økonomisk transaksjon etc.

Sikring av kvalitet og av dokumentasjon er spesielt viktig fra ei sikkerhetsside.

5.2.2 Tilegnelse av ressurs.

Produksjonen kan enten skje i den organisasjon som skal bruke ressursen eller i en annen. I det siste tilfelle må den tilegnes fra produsenten.

Sikkerheten ved bruk av en ressurs vil være avhengig av sikkerheten ved tilegnelsen.
Sikring mot forbyttinger, beviiste endringer,
m.m. i denne fasen er av betydning.

5.2.3 Operasjon på ressurs.

Operasjon må her forstås vidt. Å gå i et kontorlandskap kan oppfattes som en operasjon "gå" på en ressurs "kontorlandskap". Å endre et fødselsnummer vil minst bestå i operasjonen "skrive" på ressursen "fødselsnummer".

Bruken av en ressurs er mest interessant i livsløpet til en ressurs, sett fra et produksjonssynspunkt. Avhengig av ressursens natur vil ulike operasjoner være mulige.

Vedlikehold er nødvendig for å oppretthold kvaliteten til en ressurs.

Modifikasjon av en ressurs vil være alt fra mindre endringer til total destruering eller sletting. Ressursers natur endres som følge av modifikasjonen.

En endring kan være kvalitativ, da endres ressursens egenskaper, eller bare kvantitativ.

da endres bare tilstanden i ressursen uten at egenkapital endres.

5.2.4 Avhendelse av ressurs.

Avhendelse er av betydning for sikkerheten og kan ta form av salg, overlevering, overføring e l.

5.3 Ressurssikkerhet

Med 'sikring av en ressurs' skal vi forstå sikring av ressursens kvalitet, operasjoner på ressursen, identifikasjon av, tilgjengeligheten av og autentisering av ressursen og relevans av dens delressurser.

5.3.1 Ressursers kvalitet

Kvaliteten til en ressurs er viktig for mange forhold, bl.a. sikkerhet. En maskin med hardware-feil, et program med logiske feil, data med dårlig kvalitet, en person som lekket taushetsbelagte opplysninger skulle alle antyde mulige sikkerhets- og integritetsproblemer. Ressurskvalitet er gjenstand for en hovedtype av trusler.

Begrepet ressurs forstås relativt til formålet med bruken av den (jfr. 5.1). Kvaliteten må følgelig sikres relativt til dette formålet.

Krav til kvalitet kan man uttrykke som betingelser, kriteria, standarder, .. som ressursen skal oppfylle. Disse kan stilles på ressursen isolert eller på ressursen i den sammenheng den skal virke. I det siste tilfelle kan kriteria o.l. også inneholde variable fra omgivelsene.

For å sikre kvaliteten til en ressurs på en god måte må en først sørge for at kravene, stilt ved kriteriene, godt dekker det behovet en har. Og dernest at ressursen tilfredsstiller kravene.

5.3.2 Autorisasjon av operasjoner

Autorisasjon av aktører består i å bestemme regler for hvem som skal ha anledning til å gjøre hvilke operasjoner på hvilke ressurser. Det bør også være mulig å stille ytterligere restriksjoner som tidsbegrensinger, operasjon fra bestemt terminal, etc.

Dette kan noe formelt sammenfattes slik:

Autorisasjon: <Akte> tillates <operasjon> på
<ressurs> (evt. på <vilkår>)

Her kan både akte, operasjon og ressurs være sammensatte hver for seg. Parentesene rundt hvis <vilkår> skal indikere at vilkår ikke må

= men kan - oppgis:

Eksempel 1:

```

    akter      = operatør,
    operasjon  = å bevege seg
    ressurs    = maskinrom
    vilkår     = fottey ikke er piggako
  
```

Eksempel 2:

(TOPS-10's skema-beskyttelse av filer.
TOPS-10 er DEC-10's operativsystem).

Operasjonskode:

```

    7 - ingen aksess,
    6 - utfør program
    5 - les
    4 - tilføyselser
    3 - oppdatering
    2 - skriv
    1 - gi nytt filnavn
    0 - endre beskyttelse
  
```

En tillatelse på et gitt nivå inkluderer tillatelser på høyere. Har man leseaksess til en fil så har man også eksekveringsaksess til den.

Akterer er ulike programmerere som kan inndeles i prosjekter. Ved hjelp av 3 posisjoner uttrykker en nivået for egne privilegier, til de øvrige på prosjektet og for resten av programmererne - i den rekkefølgen. Standard beskyttelse - som er <057> - forteller at programmerer har alle rettigheter, prosjektet leseaksess og elmenheten ingen aksess.

Autoriserings angis ved å knytte de tre sifrene til hver fil, f eks

sikker<077>

som gir autorisasjoner til fila sikker.

Et autorisasjonsskjema vil være et sett med autorisasjonsregler på forma over. Det er selvsagt viktig å ha fleksible og uttrykkskraftige skjema slik at en effektivt får gitt de autorisasjoner en vil gi. Det fins mange slike skjematyper. Noen opererer ut fra prinsippet om at alt som ikke er ekplisitt forbudt er tillatt. Andre ut fra at alt som ikke er tillatt er forbudt.

Det er og viktig å skjelne mellom formelle autorisasjoner (slike som uttrykkes i formelle regler) og uformelle (slike som er gitt de ansatte i organisasjonen på uformelt vis).

En viktig egenskap ved autorisasjonsskjemaer er den mulighet de har for å uttrykke myndighet til å fastsette autorisasjoner. I store systemer (1000-vis av ansatte) er det en forutsetning å kunne delegere autorisasjonsmyndighet for å

ha god sikkerhet i autorisasjonssystemet.

Det kunne vært en interessant oppgave å vurdere ulike autorisasjonsskjema, men det ligger noe på siden av prosjektet, og er derfor ikke omfattet.

5.3.3 Sertifisering.

Ved all produksjon er det viktig at ressursene som inngår, såvel prosesser som produkter, holder visse kvalitative minstemål. Det er nødvendig med kvalitetskontroll av ressursene. Her vil en ta stilling til om en ressurs kan brukes til et bestemt formål. Slik evaluering kalles gjerne sertifisering.

Sertifisering kan sammenfattes:

Sertifisering: <Ressurs> tillates brukt til
<formål> (evt. på <vilkår>)

Alternativt kan en formulere en sertifisering:

<Ressurs> tildeles <sertifikat>

Sammen med en regel av typen

<Ressurs> med <sertifikat>
tillates brukt til <formål>
(evt. på <vilkår>)

passer dette inn i den mer generelle form
over.

Kvalitetskontrollen vil ofte skje på grunnlag av gitte kriterier eller standarder. Utforming av slike kan være viktige sikkerhetsmessige tiltak (jfr. USA's forsvarsdept.'s datasikkerhetskriteria). Sertifisering av en ressurs til kvalitetskontroll vil være en 2. ordens kvalitetskontroll. Og som sådan er den selvsagt særlig viktig.

Fr. 24.86 er det fremlagt to forslag til europeiske standarder, CEC Certif. 87/15 "General criteria and recommendations for testing laboratories and accreditation bodies" og CEC/Certif 87/16 "General criteria and recommendations for the competence of certification bodies". Disse standardfor-
slagene bygger i stor grad på ISO-
retningslinjer.

5.3.4 Identifikasjon.

Å identifisere en ressurs vil si å bringe på det rene hvilken ressurs av flere kandidater en står ovenfor. Eksempelvis: for å kunne vurdere om tillatelse til operasjoner skal gis forutsettes at aktøren er identifisert. Kontonummer, telefonnummer, linjenummer, personnummer, foretaksnummer,... identifiserer ulike ressurser.

5.3.5 Autentisering.

Å autentisere vil si å verifisere at en ressurs er den den påstås å være. For eksempel: å vise identifikasjonspapirer (legitimere seg) er en form for autentisering. Å gi passord ved pålogging er en annen form.

5.3.6 Tilgjengelighet.

Selv om autorisasjoner etterleves og ressursene har utmerket kvalitet kan en komme i sikkerhetsmessige problemer. For hva om en ressurs ikke er tilgjengelig i det den skal brukes. Problemet sorteres under driftssikkerhet. Tiltak for å realisere tilgjengelighet kan variere fra å ta sikringskopier, at de ansatte er tilstede når de skal være det, spredning av kompetanse og til beredskapsplaner.

Det er innlysende at tilgjengelighet delvis står i motsetning til annen sikkerhet. Sikkerhetstiltak mot kompromittering reduserer tilgjengelighet allment, men kan i verste fall føre til vranglås i et system om de autoriserte aktører er fraværende og løsning av videre oppgaver "henger" på en operasjon som de tilstedeværende aktører ikke er autorisert til å utføre.

5.3.7 Administrasjon av en ressurs

En organisasjon setter seg ulike mål som forsøkes oppnådd. Målene kan nås ved å løse en mengde oppgaver. Til dette har organisasjonen ulike ressurser til rådighet. Ressurser i organisasjonen må administreres for å realisere organisasjonens ulike mål.

Administrasjon av organisasjonen omfatter strategisk planlegging, gjennomføring og kontroll. Det omfatter organisatorisk planlegging, gjennomføring og kontroll, etc.

Ressursene er lokalisert i tid og rom. Hermed blir løsning av oppgavene også lokalisert.

Ressurser må allokeres til løsning av en oppgave.

Ser en administrasjonsproblemet med fokus på en ressurs i stedet for en oppgave kan en spørre hva ressursen skal brukes til, hvor og hvor lenge den skal brukes, hvilke mål den skal ha oppnådd, etc.

Hva en ressurs vil brukes til er avhengig av hva den kan brukes til. Det er i sin tur avhengig av de evner (muligheter, egenskaper) ressursen har og de vilkår som gjelder for bruk av den. Videre er det avhengig av de behov som foreligger for løsning av oppgaver.

Hva en ressurs skal brukes til kan uttrykkes ved plikter, tillatelser, ansvær, kompetanse, etc.

I en stor organisasjon vil slik ressursadministrasjon ikke kunne skje ved at noen få ledere administrerer det hele. Derfor bygger en opp organisasjoner i organisasjonen for å løse deloppgaver. Disse pålegges ansvar og gis myndighet for å løse sine oppgaver. Slik får en gjerne mange nivåer i en organisasjon.

Administrasjon av en ressurs vil innebære at noen har myndighet (kompetanse) til å bestemme hva ressursen skal brukes til, osv. Det kreves videre, for en effektiv utnyttelse av ressursen, at noen har ansvar for å administrere den.

6 SENSITIVITET

6.1 Personvern-orientert sensitivitet

Når en skal bestemme sikringsnivået for personopplysninger må en basere seg på ei risikovurdering med utgangspunkt i registrert person. Hvorfor forklares nedenfor. Risikoen består av to komponenter: en del angir sannsynlighet for at en trussel inntreffer. Den andre angir konsekvensen av at den inntreffer.

Med sårbarhet for en trussel mot en personopplysning, eller mot behandling av personopplysning, menes den skadevirkning en registrert person vil oppleve som følge av at trusselen gjennomføres.

Sensitivitet defineres ved hjelp av sårbarhet. Sensitivitet knyttes til personopplysning, eller til behandling av personopplysning. Sårbarhet knyttes til person.

Sensitivitetsbegrepet hviler på en ide om opplevelse av negative konsekvenser for den registrerte ved at en bestemt hendelse mot opplysninga inntreffer. Dette understrøkes jo også ved at vi kaller slike bestemte hendelser trusler. De må da antas i hovedsak å ha negative konsekvenser, selv om noen kan være positive.

Sensitivitetsgradene for personopplysninger varierer for ulike aktører rundt personregistre. Aktørene kan være registrert person, eller gruppe av personer, registreier, bruker av personopplysning og behandler av personopplysning (f eks databehandlingsforetak). Alle disse aktører er sårbare for trusler mot personopplysninger. En må ta stilling til hvilke aktørers sårbarhet som skal dekkes ved sikringsforskrifter.

Man bør begrense seg til registrerte personers sårbarhet. De risikoer som ikke berører personvernet får bruker, behandler og eier håndtere som de selv vil.

Dette spørsmålet er forevrig interessant i diskusjonen av hvordan EDB- sikkerheten generelt skal ivaretas og reguleres i Norge.

Nå vil det vel langt på vei være positivt korrelert sensitivitet (sensitiviteten svinger i takt) mellom de ulike aktører. Derfor vil personvernrettede tiltak ofte medføre registreiervern, brukervern og behandlervern. Men det vil også være negativt korrelert (svinger motsatt) sensitivitet mellom aktører i enkelte tilfeller. F eks mellom brukere av personopplysning og de registrerte. Bruker ønsker tilgang til

ei opplysning. Den aktuelle person vil nødig at den skal gis.

Siden vi foreslår å uttrykke sårbarhet for registrerte personer kaller vi den personvernorientert sårbarhet. Tilsvarende benevnes sensitiviteten personvernorientert sensitivitet.

6.2 Sensitivitet for personopplysning

Sensitivitet for personopplysninger vil variere med de ulike typer trusler og trusselformål som kan forekomme mot personopplysninger, typen av opplysninger og opplysningenes innhold.

Det er opplagt at opplysningstypen forteller mye om hvilket sensitivitetsnivå ei personopplysning har. §6.2 lister opp eksempler på spesielt sensitive typer: rase, politisk eller religiøs tilhørighet, seksuelle forhold, kriminell belastning, helseforhold og misbruk av rusmidler og spesielle familieforhold.

Men det burde være like klart at innholdet av ei opplysning vil influere på sensitiviteten. Det kan normalt ikke sies å være ei sensitiv opplysning at en person er heterofil. Annerledes er det ofte om personen er homofil. Og det er normalt ikke like sensitivt å ha 6 i norsk skriftlig fra gymnaset som 1.

Den følsomheten en person vil ha overfor en trussel rettet mot personopplysninger om seg selv vil sterkt avhenge av hva formålet med trusselen er. Ei adresseopplysning er normalt ikke særlig sensitiv. Men sett at det er den fraskilte ektemann, som forfølger sin eksfru, som er ute etter hennes adresse, så kan denne opplysningen være svært sensitiv. Hvis kompromittering av personopplysning skjer med det formål å skaffe seg en adresse med hensikt å legge press på, eller true en person, så vil denne opplysning måtte betraktes som ganske sensitiv i sammenheng.

Videre vil sensitiviteten variere med konsekvenstyper. Kompromittering av ei personopplysning kan få konsekvenser både for ens liv og helse, økonomi, rettigheter, karriere, omdømme, sosiale forhold, m.m. Men følsomheten vil neppe være like stor på alle områder.

Kompromittering av samme opplysning kan være svært uheldig for sosialt omdømme uten å ha særlig økonomisk betydning. Om formålet med kompromitteringa er utpressing, vil det oppleves verre enn om det kun er for å tilfresstille nysgjerrighet. Det oppleves gjerne mer følsomt å få utlevert sine medisinske opplysninger enn hvilke bøker en har lest.

Siden vi foreslår å uttrykke sensitivitet for registrerte personer kaller vi den RP-orientert sensitivitet.

Sett at en for en gitt trussel og gitt opplysningstype, for hvert formål med trusselen og hvert innhold av opplysningstypen hadde et mer eller mindre presist uttrykk for sensitiviteten. Hvordan skal en da kunne utlede sensitiviteten for opplysningstypen? Kan en for eksempel

summere sensitiviteten for alle kombinasjoner av innhold og formål? Dette er ikke tilfelle. For sett at en gjorde likeartede formål mer spesifikke, for dermed å øke antallet trusler, mens sensitiviteten for hvert av formålene er tilnærmet konstant, da skulle samla sensitivitet øke. Dette er klart helt urimelig. Summen av sensitivitetene for ulike innhold og formål vil ikke gi dekkende uttrykk for sensitiviteten av opplysninga.

Da ville muligens gjennomsnittlig sensitivitet være mer dekkende. Gjennomsnittet korrigerer jo for antallet forskjellige innhold og formål.

Men hva da med tilfeller hvor mange formål leder til liten sensitivitet, mens noen få har svært stor. Kan det kanskje være bedre å bruke maksimal sensitivitet?

Det ser ut til å være relativt vanskelig å finne noe egna kvantitativt mål for sensitiviteten for en opplysningstype på grunnlag sensitivitetene for alle innhold og formål, selv om en hadde en presis angivelse av disse.

Det ser også ut til å være nødvendig at sensitiviteten av en opplysningstype fastsettes skjønnsmessig. Og da vil det være et skjønnsmessig maksimum og gjennomsnitt en kan ha forhåpninger om å fange. Skjønt en kan tenke seg skjønnsmessige uttrykk for gjennomsnittlig variasjon, mål som "x % av truslene ligger under sensitivitet y", etc. Fortsatt er det ønskelig å skjelve mellom ulike konsekvenstyper. Men det er neppe praktisk å fastsette mer enn f.eks. en kompromitteringssensitivitet for en og samme opplysningstype.

En skjønnsmessig fastsatt, gjennomsnittlig sensitivitet (også gjennomsnitt for alle personer) for hver opplysningstype virker hensiktsmessig å bruke. Verken maksimal eller minimal sensitivitet vil være egnet. Det vil si at en ikke kan ta utgangspunkt i verken de over- eller underfølsomme personer.

I noen tilfeller kunne en likevel tenke seg at opplysninger for bestemte personer, som av spesielle grunner er særlig følsomme, kunne gis ekstra beskyttelse. Her måtte den registrerte gis en ekstra rettighet i så fall.

6.3 Akseptabel risiko

Drivkraften bak registrering og bruk av personopplysninger er et eller annet aktualisert eller mulig behov for opplysningene. Hadde søkeren ikke behov for - eller trodde at han kunne komme til å få behov for - opplysningene, ville han ikke ta seg bryet med å skaffe disse. Når Datatilsynet skal vurdere søknader om konsesjon må således søkerens behov for opplysninger (§ 6, 1.ledd) veies mot borgernes behov for personvern. Kan behovet argumenteres med lov-, forskrifts- eller kongelig res. hjemler vil det veie tyngst. Er behovet ikke så sterkt og opplysningene av sensitiv art, kan personvernet veie tyngst. Altså kunne vi si at vurderinga om en søker skal få tilgang til ei opplysning styres bl. a. av Datatilsynet's svar på spørsmålene:

- Har søkeren saklig behov for opplysningene?
- Er sensitiviteten av personopplysningene akseptabel i forhold til det behov brukeren har?

Her er vi først og fremst ute etter å beskrive hva som er akseptabelt. Vi skal ikke gå inn på de øvrige forhold som styrer Datatilsynet's vurdering om tillatelse til bruk av opplysninger.

Den registrerte person, Datatilsynet og øvrige myndigheter, bruker, behandler- og eier av registre, og øvrige interesser vil gjerne ha selvstendige meninger om sensitiviteten er akseptabel i forhold til en gitt bruk. formålet for bruken av opplysningene. Begrepet akseptabel sensitivitet vil ikke være til hjelp i sensitivitetsklassifikasjonen.

6.4 Noen typer trusler mot personopplysninger

Sensitivitet betyr i dette avsnitt sensitivitet for kompromittering.

Her får vi anledning til en praktisk demonstrasjon av ressurs-modellen der gjenstanden som studeres er ei personopplysning.

6.4.1 Identifisering

Hva identifiseringa innebærer vil variere. Her skal vi betrakte det som identifikasjon av en bestemt person og ei bestemt opplysning om personen.

Jo mindre sikker identifikasjonen av en person er, jo mindre sensitiv vil personopplysninga være for den antatt identifiserte. Forbud mot registrering av fødselsnummer (og annen sikker individ-identifiserende informasjon) kan derfor være en måte å redusere sensitivitet i et register på.

Fullstendig anonymisering vil gjøre opplysningene ikke-sensitive.

Med identifikasjon av opplysning kan siktes til identifikasjon av innhold av opplysning og kilde(r). Jo mer usikker bestemmelsen av innholdet er, jo mindre sensitiv er opplysninga. Det samme gjelder for kilder.

En usikker identifikasjon av kilden vil ha varierende konsekvenser. Fra at opplysninga blir verdiløs, til at den har full verdi. Et eksempel på det siste kan vi ha i et saksbehandlingssystem der man ikke klarer å spore tilbake til saksbehandler.

Sensitiviteten for ei opplysning vil derfor normalt reduseres med økende usikkerhet i identifikasjon av kilden.

Feilidentifikasjon av person har to konsekvenser. Personen er inntil videre ikke sårbar for opplysninga, mens den person den feilaktig knyttes til er sårbar for opplysninga.

Feilidentifikasjon av opplysning kan føre til både øket og redusert sårbarhet for den registrerte avhengig av hvilken feil som gjøres.

Ei feilidentifisering av kilde kan gi ei opplysning mer eller mindre verdi og således øke eller minske sårbarheten for den registrerte.

6.4.2 Autentisering

Autentisering i denne sammenheng vil si å verifisere at personopplysninga faktisk er autentisk, både med hensyn til omhandlet person, innhold, kilder til opplysninga og saksbehandlere.

Det kan her bemerkes at autentisering ikke omfatter validering. Dvs å vurdere korrektheten av opplysninga.

Den skal lede til en bekreftelse eller avkreftelse av identifikasjonen. Ei dårlig autentisering kan lede til akseptering av feilidentifisert opplysning.

Autentisering av personidentifikasjon vil bety å sannsynliggjøre at identifikasjonen er riktig.

Å få bekreftet at ei opplysning er riktig kan gjøres på mange nivåer fra paritetssjekk, segl på informasjonen til separat autentisering. En trussel mot autentiseringa kan lede til akseptering av feil informasjon.

6.4.3 Tilgjengelighet

Både tilgjengelighet og mangel på tilgjengelighet av personopplysning kan medføre økt sårbarhet for en aktuell person. Er ei opplysning nødvendig i ei beslutning som en person er interessert i å få gjort, men ikke foreliggende, så kan ikke beslutninga foretas. Det kan medføre forsinkelser for personen, som forsåvidt er en egen type konsekvens.

At en aktør har tilgang til ei personopplysning som den registrerte helst så aktøren ikke hadde, er et eksempel der sårbarheten øker som følge av tilgang.

Skal en bruker ha tilgang til ei opplysning så må brukeren ha saklig behov for den. Har han behov for opplysninga så får han tilgang om Datatilsynet vurderer sensitiviteten som akseptabel for hans formål. Hvis ikke, får han neppe tilgang, med mindre brukeren har hjemmel for det.

Noen eksempler på sårbarhet:

konsekvens	tilgjengelig	ikke tilgjengelig
type		
økonomisk	bankkonti	fradragsdata skatt
sosiale	irrelevante-	relevante opplysn.
livstruende	feil i	helsedata
	helsedata	

For de tre konsekvenstypene kan Skattedirektoratet, sosialetat og sykehus være typiske behandlingsorgan.

Er bankkonti tilgjengelig for Skattedirektoratet, kan det føre til økt skatt. Tilsvarende om fradragdata mangler. En kan betrakte dette som økonomisk sårbarhet.

6.4.4 Kvalitet

En trussel mot kvalitet av personopplysninger kan også redusere eller øke sårbarheten for den registrerte, avhengig av om feilen leder til en forbedring eller forverring. Særlig kan økonomiske konsekvenser og konsekvenser for rettigheter være viktige som følge av dårlig kvalitet. Helsemessige konsekvenser kan bli svært alvorlige om helsedata inneholder feil. Også for de andre konsekvenstypene kan følgene bli store.

Datatilsynet bør arbeide for å fremme god datakvalitet, uavhengig av hvordan det slår ut for personvernmessig.

6.4.5 Operasjoner på personopplysninger

Operasjoner på personopplysninger kan være innsamling (mottak), koding, registrering, endring, tilføyelser, korreksjon, sletting, transport (utlevering), lagring, framhenting, søking, utlistering, sortering, kobling, primær bruk, m.m..

Autorisasjoner av operasjoner er av største viktighet for personvernet. Autorisasjonene bør styres av et "need-to-do"-prinsipp. Risikoen for opplysninger kan endres som følge av endrede autorisasjoner. Enkelte trusseltyper kan fjernes helt og sannsynlighetene for at andre typer trusler blir gjennomført kan også endres.

Det ovenfor nevnte "need-to-do" prinsipp er ment som en ren generalisering av det mer velkjente "need-to-know"-prinsippet.

Den myndighet, som den enkelte utøver ved administrasjon av personopplysninger, innvirker både på konsekvenser og sannsynligheter for at andre trusler inntreffer.

Klare plikter og ansvar ved administrasjon av personopplysninger tjener gjerne til å svekke personvernrisikoen.

6.5 Grovdeling av trusseltyper. Graderingsforslag

Hvor langt er det ønskelig å smelte sammen sensitivitetene for de ulike trusseltyper for å få færrest mulig sensitivitetsmål for samme opplysning? Kan vi kanskje med fordel operere med ett sensitivitetsmål for personopplysninger? Etter vårt syn er dette ikke

ønskelig om sensitivitetsangivelse skal lede til fastsettelse av sikkerhetstiltak. Da trengs flere mål. Det kan være verdt å skille mellom sensitivitet for minst tre forhold: kompromittering av opplysninger, kvalitet av opplysninger og kvalitet i behandling av opplysninger. Men det er godt mulig at det vil være fordelaktig å skille mellom flere typer trusler.

Istedet for kvalitet ved behandling av opplysninger har arbeidsgruppa tatt med sensitivitetsmål for tilgjengelighet. Kvalitet ved behandling søkes dekket gjennom datakvalitetsbehovet.

6.5.1 Kompromittering

Lesing, fotografering, eller annen registrering av materiale, samt påfølgende utlevering til ikke autorisert mottaker, er kompromittering av opplysninger. Det allmene ved denne trusselen er at den bringer en type opplysning ut av den autoriserte krets.

6.5.2 Trusler mot kvaliteten av opplysninger

Trusselen her retter seg mot fullstendighet og korrekthet i de registrerte opplysninger. Trusselen kan realiseres ved manuell registrering, endring eller sletting av opplysninger. Den kan også realiseres ved automatisk bearbeidning.

6.5.3 Trusler mot kvalitet i behandling av opplysninger

Det siktes til trusler som verken leder til kompromittering av opplysninger eller dårlig datakvalitet. Dette dekkes av punktene 5.1 og 5.2.

Arbeidsgruppa har gjort tilgjengelighet til den tredje hovedgruppe av trusler. 6.5.3 er ikke dekket i utkastet til forskrift.

7 SÅRBARHETSGRADER

Sårbarheten vil være forskjellig for kompromittering, dårlig datakvalitet og dårlig bearbeidning. Kompromittering av ei adresseopplysning er ikke like følbart om den brukes til reklamesending som til psykisk press, etc.

Det vil være upraktisk å operere med for mange sårbarhets- og sensitivitetsgrader, samtidig gi for få nyanser med for få. 3-6 grader er antakelig passe yttergrenser. Gradene bør tilpasses Beskyttelsesinstruksens når det gjelder kompromitteringsfare. Beskyttelsesinstruksen opererer med to grader: STRENGT FORTROLIG og FORTROLIG (jfr. Beskyttelsesinstruksen §4). "STRENGT FORTROLIG nyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende. FORTROLIG nyttes dersom det vil kunne skade offentlige interesser ...".

En kunne forsøksvis nytte sårbarhetsgradene livstruende(4), betydelig skade(3), skade(2), mindre skade(1) og ingen skade(0).

Er sårbarhetsgraden livstruende, bør spesielle rutiner igangsettes for å forhindre at slike trussel-virkninger oppstår. Om en beskrivelse av dette hører hjemme i forskrifter annet enn i form av generelle normer er tvilsomt. Normer som de to etterfølgende kan imidlertid tenkes: Personopplysning som kan medføre fare for tap av liv om den blir kompromittert eller er uriktig skal sikres slik at slik fare ikke oppstår. Behandling av personopplysninger skal skje på slik måte at liv ikke trues.

Prosjektgruppa finner liten grunn til å foreslå at kategorien livstruende tas med. Hvis det skal innføres regler for å bedre sikkerheten for så stor sårbarhet antas det at de vil være så spesielle at de må komme inn ved konsesjons-behandling.

Arbeidsgruppa har fulgt dette resonnement.

STRENGT FORTROLIG kunne passes inn til nivå 3 og FORTROLIG til nivå 2.

En kan diskutere behovet for grad 4 og 1 i tillegg til Beskyttelsesinstruksens to og offentlig tilgjengelig informasjon.

Mindre skade er en grad som det kan finnes behov for mellom offentlige opplysninger og FORTROLIGE når det gjelder kompromitteringsfare. Bare personer som har tjenestelig behov for opplysningene bør ha adgang til dem.

Datakvalitet og behandlingskvalitet omfattes ikke av Beskyttelsesinstruksen. Datasikkerhetsdirektivet omhandler heller ikke punktene, selv om punkt 6 omtaler funksjonell sikring. Når det gjelder sårbarhetsgrader for datakvalitet er

det ikke vanskelig å tenke seg livstruende feil i personopplysninger, f. eks medisinske opplysninger. Betydelig skade vil kunne oppstå etter feil som leder til økonomisk tap, dårligere omdømme, tap av rettigheter, o.l.

Tilsvarende gjelder for behandlingskvalitet.

7.1 Hva skal vi forstå med de ulike sårbarhetsgradene?

Spesifikk sårbarhet uttrykkes i forhold til konsekvenstyper (se 6.2).

Skaden ved at en uønsket hendelse inntreffer kan dels uttrykkes ved hvor intens virkningen er og dels ved hvor varig den er. Siden vi antar at skaden fører til en forverret tilstand for registrert person skulle dette være opplagt.

Nå er det slik at folk ikke er like sårbare for samme trussel, selv om de vesentlige forhold som berøres ved truslene er like. Dette er tilfellet for svekking av omdømme siden de sosiale omgivelser her er svært ulike. En må derfor operere med en slags forventet (eller gjennomsnittlig) sårbarhet (se 6.2).

Nedenfor fins noen forslag til momenter til presisering av begrepene betydelig skade, skade og mindre (ubetydelig) skade. Disse, eller tilsvarende, bør stå i forskriftene.

Arbeidsgruppen kom fram til at ei slik avgrensning ikke var enkel å gi noenlunde generelt og presist. Arbeidsgruppen har derfor utelatt å indikere hvor sårbarhetstermene skal plasseres.

7.1.1 Betydelig skade

En trussel mot personopplysning eller mot behandling av personopplysning fører til betydelig skade om den fører til skade på legeme eller helbred (jfr. strl §229), til alminnelig, sterkt svekket omdømme (jfr. strl §247) eller ære (jfr. strl § 246), til langvarig utestenging fra forening eller fratakelse av tillitsverv eller lignende, til betydelig økonomisk tap som ved oppsigelse fra stilling eller tilsvarende forringelse av ervervsmuligheter, til tap av rettigheter, m.m.

7.1.2 Skade

En trussel mot personopplysning fører til skade om den fører til alminnelig, svekket omdømme eller ære, til utestenging fra forening, fratakelse av tillitsverv eller lignende, til merkbart økonomisk tap eller tap av rettigheter, m.m.

7.1.3 Mindre skade

En trussel mot personopplysning fører til mindre skade om den fører til tvil om en persons omdømme eller ære, til ubehageligheter i sin omgang med andre personer, selskaper, myndigheter, m.m.

Premiseringen av definisjonene i 7.1.1-3.

En trussel "fører til" en ulempe om det er en årsakssammenheng mellom trusselen og ulempen, om enn ikke direkte. Før således en ektemann rede på at hans kone har en elsker vis et register, hvoretter han påfører sin kone skade, skal definisjonen forstås slik at kompromitterings har ført til betydelig skade.

Om en lege legger til grunn feilaktige diagnosedata for en operasjon med skade til følge, er det en årsakssammenheng mellom diagnosen og skaden, vil en si at feilen førte til skaden. Dette gjelder selv om legen ikke har utvist tilstrekkelig aktsomhet.

Det er heller ikke vanakelig å forestille seg at en saksbehandling kan føre til skade for en person. Et slikt tilfelle kan oppstå om en person søker om behandling for et medisinsk problem. Før saksbehandlingen er ferdig kan problemet ha blitt langt alvorligere. Her er det jo ikke årsakssammenheng mellom saksbehandling og skade, men om mer effektiv saksbehandling kan antas å ha forhindret skade, eller omfanget av skaden, vil man si at en saksbehandling fører til skade.

"Svekket omdømme" kan forklares analogt til krenkelse av omdømme i injurienesammenheng (Andenaa 114-125). Det er dog den antatt faktiske virkning av trusselen en tar sikte på å dekke. Ikke om den er injurierende eller ikke. Det apiller ingen rolle for å bestemme om betydelig skade = f.eks. foreligger. Er det ikke noen grunn til å tro at den faktiske virkning vil være betydelig skade graderes ikke personopplysnings eller behandlingsprosessen tilsvarende høgt.

Mens opplistingen i §247 (gode navn og rykte (moralisk omdømme), utsette for hat eller ringeakt (sosialt omdømme) eller den for stillingen eller næring fornødne tillit) betraktes som uttømmende, er det ingen grunn for å gjøre dette ved fastsetting av sensitivitetsgrad. Andre typer svekkelse av omdømme bør altså også omfattes.

"Svekket are" tolkes analogt til arekrenkelse (Andenaa 125-163) i straffelovens §246.

For at svekkelsen av omdømme eller are skal være sterk, må det antas at den vil føre til et kvalitetsaspirang. Slik som ved at det blir kjent at en person er prostituert, er tidligere straffedømt for usaktsomt drep, grovt underslag, - bedrageri, - utroskap, - skadeverk, e.l.

Det antas å være tilstrekkelig til å

svekke omdømme - f.eks. - at en er straffedømt for underlag, bedrageri, utroskap, skadeverk, e.l.

Med 'langvarig utestenging fra forening, tillitsverv, e.l.' siktes det til utestenging utover 5 år. Tillitsverv kan være verv i foreninger eller i offentlig styrer, utvalg og nemnder, m.m.

Med 'forringelse av ervervsmuligheter' siktes det til at stillinger en ellers er kvalifisert for utelukkes på grunn av hendelsen.

Med 'tap av rettigheter' siktes det til økonomiske, borgerlige og andre juridiske rettigheter av en viss betydning som registrert person er i rettmessig besittelse av.

For 'fører til betydelig økonomisk tap' antas årsakssammenheng mellom den realiserede trusselen og tapet. Det trenger ikke være noen straffbar handling forvoldt av andre som ligger bak tapet.

For at tapet skal være betydelig bør det tilsvare om lag et kvartals netto inntekt.

Det skal ikke regnes som tap om en person fratras verdier som han ikke ansees som eier av eller rettmessig disponerer.

'Ubehageligheter i sin omgang med andre personer, selskaper, myndigheter, m.m.' kan være nedsettende omtale, uhøflig behandling, mistenksomhet, uvanlig sen saksbehandling og lignende brudd på vanlig god omgangstone, forretnings- og saksbehandlingspraksis.

8 SENSITIVITETSMODELL

8.1 Sensitivitetsgrader

Nedenfor foreslås regler som relaterer sårbarhet til sensitivitet: opplysning om en person eller behandling av opplysning er SÆRLIG SENSITIV for en trussel om denne fører til betydelig skade for personen, er SENSITIV om den fører til skade, er MINDRE SENSITIV om den fører til mindre skade og er IKKE SENSITIV om den ikke engang fører til mindre skade.

8.2 Modellen

8.2.1 Sensitivitet for kompromittering av opplysninger

Sensitiviteten varierer med type konsekvens, formål med trussel, med opplysningstype og med opplysningas innhold (se 6.2).

Kompromittering av samme opplysning kan være svært uheldig for sosialt omdømme uten å ha særlig økonomisk betydning. Om formålet med kompromitteringa er utpressing vil det oppleves verre enn om det er å tilfredsstille nysgjerrighet.

Det oppleves gjerne mer føleomt å få utlevert mine medisinske data enn hvilke opplysninger om hvilke bøker en har lest. Og er det karakterer som repes, er det gjerne verre om de er dårlige enn om de er gode.

En skjønnsmessig fastsatt gjennomsnittlig sensitivitet for hver opplysningstype virker hensiktsmessig å bruke. En tar da utgangspunkt i verken de over- eller underfølsomme personer, ekstreme trusler, formål eller situasjoner.

8.2.2 Sensitivitet for datakvalitet

Sensitivitet betyr i dette avsnittet sensitivitet for datakvalitet.

I dette avsnitt drøftes hvordan en skal bestemme hvor viktig datakvaliteten er for et dataelement, en post eller et register.

En er opptatt av at resultatet av rutiner har en viss kvalitet. Skal en være sikret at kvaliteten holdes, må både grunnlagsdata og rutinene ha en tilstrekkelig god kvalitet. Kravet til kvalitet i resultatet kan altså videreføres som krav til grunnlagsdata og rutine.

Rutinekvalitet diskuteres for seg.

Skal en videreføre krav fra resultatet til grunnlagsdata, trenger en å kjenne rutina i minste detalj. Er rutina

automatisert er det et program en må kjenne. Å regne seg fram til et tilnærmet uttrykk for sammenhengen mellom feil i grunnlagsdata og feil i resultatet vil være rent for detaljert for de fleste anvendelser. Det må derfor søkes andre metoder for å uttrykke hvordan krav til kvalitet kan videreføres fra resultat til grunnlagsdata.

Siden ulike dataelementer ofte brukes av ulike rutiner med ulike formål vil sensitiviteten variere etter hvilke rutiner som gjør bruk av dataene. Dette skiller seg fra situasjonen for kompromittering.

Som for kompromitteringssensitivitet vil sensitiviteten for datakvalitet variere med opplysningstype og innhold av opplysninga. Trusseltypen vil ikke spille noen rolle for sensitiviteten her heller. Til forskjell fra kompromitterings-tilfellet spiller ikke formålet med trusselen noen rolle.

(1) Sensitivitetsmatrise

La oss tenke oss sensitiviteten for kvaliteten av opplysningstyper fylt ut i en todimensjonal sensitivitetssmatrise der opplysningstypene er tegnet inn redvis og de rutinene som bruker disse kolonnevis.

SENSITIVITETSMATRISSE: 8

	rutine	1	2	3	4
opplysningstype	1	0	0	1	2
	2	1	0	0	1
	3	0	0	0	0
	4	1	3	1	0

$S(i,j) = 0$, hvis sensitiviteten til opplysningstype i er IKKE SENSITIV i rutine j .
 = 1, hvis den er MINDRE SENSITIV.
 = 2, hvis den er SENSITIV, og
 = 3, hvis den er SÆRLIG SENSITIV.

Hvordan skal en uttrykke sensitiviteten for datakvalitet for en opplysningstype? Siden denne antas å variere for ulike rutiner kunne en tenke seg å bruke snittet av sensitivitetene, minimal eller maksimal sensitivitet. Hvilken bør en velge? Det turde være opplagt at kravet til datakvaliteten ikke bør være mindre enn det strengeste kravet fra noen rutine. Altså bør en velge maksimal sensitivitet under noen rutine.

Et eksempel på de tre alternativene over:

	r1	r2	r3	max	min	snitt
o1	0	1	2	2	0	1
o2	2	2	1	2	1	5/3 (2)
o3	3	0	1	3	0	4/3 (1)
o4	0	0	0	0	0	0

Hvis ei rutine brukes til flere formål, må må kravene til datakvaliteten for en opplysningstype som brukes av rutina være gode nok for det formål som krever best datakvalitet for opplysningstypen.

Et opplegg basert på ei sensitivitetsmatrise kan virke overdrevet når en har mange opplysningstyper, rutiner og formål. For 20 opplysningstyper og 15 rutiner vil en kunne trenge å spesifisere 300 sensitiviteter. Dette ville bli for omfattende om f.eks. DT skal foreta vurderings ved konsesjonsbehandling. Heller ikke denne løsningen kan anbefales.

(2) Aksessmatrise

Er det slik at sensitiviteten for resultatet av ei rutine alltid vil være større enn sensitiviteten for hvert enkelt av dataelementene som rutina bruker? Nei, slik er det ikke. Et viktig dataelement kan inngå i en uviktig bruk. Men det synes rimelig at en for ei gitt rutine ikke krever høyere datakvalitet for grunnlagsdata enn for resultatene. Dette poenget vil bli utnyttet i følgende forslag til system for fastsettelse av sensitivitet.

(a) For alle rutiner som bruker et register lages en rutinebeskrivelse. Manuelle rutiner oppføres også.

Rutinebeskrivelsen bør for hver rutine inneholde formål med rutina, input og outputvariable.

(b) For hver rutine fastsettes sensitiviteten til resultatene av rutina, som svarer til den sårbarhet den registrerte vil oppleve som følge av feil i resultatene. Datakvalitets-sensiviteten til rutina svarer til det mest sensitive resultatet.

(c) Alle dataelementer som er input til rutina listes opp og sensitivitetsvurderes.

La oss så innføre en regel for fastsettelse av sensitivitet som sier at input til ei rutine minst har samme sensitivitet som rutina.

(d) For endelig å fastsette sensitiviteten høynes sensitiviteten for input-data som har lavere sensitivitet enn rutine, slik at input-data minst får like høy sensitivitet som rutine.

For å løse (b) og (c) kan en lage en aksessmatrise. For hver rutine krysses det av hvilke opplysningstyper den aksesserer, dvs hvilke input- og outputvariable den har.

AKSESSMATRISE: A

	r1	r2	r3	r4	...	rm
o1	1	0	1	0		0
o2						
on	0	0	0	0		0

$A(o_i, r_j) = 1$ når r_j aksesserer o_i
 $= 0$ når r_j ikke aksesserer o_i

I eksempelet over aksesserer opplysningstype 1 av rutine 1 og 3, men ikke av 2, 4 og m.

(3) Avhengighetsmatrise

Det vil føre til usøyaktigheter å la sensitiviteter for rutiner være sentrale ved fastsettelse av sensitiviteter for opplysningstyper, som i de to forslagene foran. Forslaget foran kan også av den grunn ikke ansees som aktuelt å gjennomføre.

Det vil av rent praktiske grunner sjelden være aktuelt med en kvalitetskontroll som tar utgangspunkt i de funksjonelle avhengigheter.

En tredje mulighet for fastsettelse av sensitivitet for opplysningstyper vil være at registerer lager en rutinebeskrivelse og ei avhengighetsmatrise. Det vil gjerne være slik at resultatene fra rutine ansees som viktigere enn grunnlagsdata, og altså mer sensitive for datakvalitet, se (2). Avhengighetsmatrise har like rader og kolonner. Disse er registerets opplysningstyper og de opplysningstypene som registeret brukes til å produsere. I matrise kan en velge å la kolonner avhenge av rader

AVHENGIGHETSMATRISE: A

	o1	o2	o3	...	on	
o1	0	1	0		0	
o2	0	0	0		0	I eksempelet
o3	0	0	0		0	er opplysning
...						2 avhengig av
on	0	0	0		0	1.

$A(o_i, o_j) = 1$ om opplysningstype j avhenger av opplysningstype i .
 = 0 ellers.

En kan innføre en modifisert regel for videreføring av sensitivitet som er tilpasset bruk av avhengighetsmatriser: Grunnlagsdata en rutine er avhengig av skal minst ha samme sensitivitet som resultatet.

Ved denne regelen vil en komme i skade for å fastlegge for høy sensitivitet for noen grunnlagsdata.

Oppgaver som må utføres ved fastsettelse av sensitiviteter:

(a) List opp opplysningstypene i registeret. de som produseres automatisk med utgangspunkt i registeret og særlig sensitive opplysningstyper som produseres manuelt.

(b) Fastsett sensitivitet for disse opplysningene.

(c) Dann avhengighetsmatrise for opplysningstypene. Dette gjøres ved at en for hver rutine og hvert resultat krysser av de opplysningstyper som resultatet er avhengig av.

(d) Sett sensitivitet for grunnlagsdata lik resultatets, om dette er høyere enn grunnlagsdataa. Dette gjøres til ingen grunnlagsdata har lavere sensitivitet enn resultater som avhenger av dem.

I avhengighetsmatrisa gjelder såkalte transitive egenskaper: Det vil si at om a avhenger av b og b avhenger av c, så avhenger a av c. Dermed kunne en produsere ei avhengighetsmatrise der alle transitive avhengigheter er representert. Finnes det derfor ei avhengighetskjede fra a til z, så skal a minst ha samme sensitivitet som z.

Bør rutinebeskrivelsen bare inneholde rutiner

som oppdaterer en eller flere opplysningstyper, eller bør rutiner som har leseadgang også listes opp? Begge typer rutiner bør føres opp, som viat i (a). Rutiner med bare leseadgang kan være viktige for en registrert. Informasjonen kan brukes til å treffe en manuell beslutning.

Det er tidligere foreslått at automatisk produserte resultatstyper bør finnes i avhengighetsmatrisa. Bør kanakje også manuelt produserte resultatstyper finnes i matrisa? Det er tvilsomt om dette kan være en praktisk løsning for alle sensitive rutiner. Grunnen er at DT vanligvis gir en i denne sammenheng vag angivelse av bruken av registre. En sier vanligvis ikke i konsesjoner hva slags opplysningstyper et register kan brukes til å produsere. Og i motsetning til et program vil ikke alle opplysningstyper en produserer foreligge i en formell beskrivelse. Et krav om at manuelt produserte opplysningstyper skal inn i avhengighetsmatrisa vil derfor kunne påføre noe merarbeid for registreier. Men det kan jo være et spørsmål om det ikke er ønskelig med en mer formalisert beskrivelse av manuelle rutiner, med resultatstyper osv. Et kompromiss kan være å innlemme særlig sensitive resultatstyper i avhengighetsmatrisa.

Avhengighetsmatrisa vil da inneholde følgende opplysningstyper:

opplysningstype	ikke	mindre		særlig
	sensitiv	sensitiv	sensitiv	sensitiv
i register	x	x	x	x
automatisk produsert	x	x	x	x
manuelt produsert				x

Alternativet med sensitivitetmatrise vil gi mye arbeid for å fastsette sensitivitetene. Det kommer av at for hver rutine og opplysningstype må en sensitivitet fastsettes.

Ved å bruke aksessmatrisa vil arbeidsmengden reduseres (arbeidet blir mer mekanisk). Men også nøyaktighets i sensitivitetene vil bli redusert. Der dataordbok (data dictionary) brukes foreligger normalt aksessmatrisa. Det reduserer arbeidsmengden ytterligere.

Bruk av avhengighetsmatrise vil lede til mer presis videreføring av sensitiviteter og sensitivitetsfastsettelse totalt. Er imidlertid antallet rutiner lavt og antallet opplysningstyper stort, kan denne løsning være uaktuell mens en av de to foregående er mer aktuell.

Er antallet opplysningstyper over 15-20, vil det bli en for omfattende jobb å utforme avhengighetsmatrise.

Når en vurderer datakvalitetssensitivitet for en opplysningstype må en ta hensyn til om en opplysningstype bidrar i en nøkkel eller ikke. Bidrar den bør sensitiviteten i alle fall ikke reduseres.

8.2.3 Sensitivitet for rutinekvalitet

Om det er feil i ei rutine kan dette få følger for personer i registeret. Sensitiviteten for rutinekvalitet vil variere med formålet med rutina, med trussetyper og formål med trusler samt konsekvenstyper.

Ved fastsettelsen av sensitivitet for ei rutine får en ta et "worst case" utgangspunkt, unntatt at rutina går i stå. Det vil si at den produserer resultater, men at disse er mer eller mindre "ville". Sensitiviteten bør videre settes som sensitiviteten for rutina for det formålet der den største sensitiviteten oppstår.

8.2.4 Sammenheng mellom sensitivitet for opplysningstype, post, register og samling av registre.

Opplysningstyper om en og samme person i et register samles i en eller flere poster (records).

Hvilken sammenheng er det så mellom sensitiviteten for et sett av personopplysninger i en post og sensitiviteten for de enkelte opplysninger?

(1) Kompromitteringssensitivitet.

Hva kan vi si om sensitiviteten til to opplysninger o1 og o2 sammen, når en kjenner sensitiviteten til hver av dem?

La oss si at opplysninga o3 følger av o1 og o2. Altså at en kan slutte o3 fra o1 og o2. Det kan være at o1 og o2 er mindre sensitive og at o3 er særlig sensitiv.

Kobling med slike konsekvenser kan vi kalle sensitivitetsforsterkende.

Om o1 og o2 delvis er i motstrid med hverandre, kan kobling være sensitivitetsdempende. F eks kan ei opplysning fortelle at en person er mistenkt for et straffbart forhold, mens ei anna sier at tiltale er frafalt.

Sensitiviteten for en post kan fastsettes på samme måte som for en opplysningstype og bør være RP-orientert. Det vil altså si at den tar utgangspunkt i Registrert Person.

Hvordan skal en vurdere sensitiviteten til et helt register? Skal den være lik post-sensitiviteten? Dette er neppe

ønskelig. Den bør være større eller lik.

Først må det nevnes at en for registeret som helhet ikke lenger bør tale om RP-sensitivitet, men sensitiviteten for det kollektiv som er registrert (RK-sensitivitet).

Grunnen til at sensitiviteten bør betraktes som større eller lik er den kumulative effekt ved at en trussel kan ramme flere istedet for en.

Sensitivitet for samlinger av personregistre er langt på vei drøftet tidligere i form av kobling av opplysninger. Imidlertid dukker det opp ett nytt spørsmål som påvirker sensitiviteten: Anta at vi ser på to personregistre. Hvor stor er andelen av personer som tilhører begge registrene? Sensiviteten for samlinga vil nå være avhengig av hvert av registrene, og hvor stor fellesandelen av personene er. (Her er det selvsagt forutsatt at registrene kan kobles).

For koblede registre gjelder tilsvarende for RP-sensiviteten som for post-sensiviteten. Et sett av registre vil dermed kunne tilordnes en RP-sensitivitet og en RK-sensitivitet.

(2) Datakvalitet

En kan anta at sensitiviteten for datakvalitet for en post ikke overstiger maksimal sensitivitet for opplysningene i posten. Sensiviteten for posten bør derfor settes lik maksimal sensitivitet for noen opplysning.

Tilsvarende resonnement gjelder for RK-sensitivitet for datakvalitet som for RK-sensitivitet for kompromittering.

8.3 Sensitivitet og alder på opplysninger

Sensitivitet vil variere med alder på opplysninger, slik at en antar at jo eldre den er, jo mindre sensitiv blir den. Dette bygger på en antakelse om at den samtidig blir mindre aktuell, hvilket ikke alltid holder. Homofile er gjerne like homofile når de er 50 som når de er 20.

Opplysninger får imidlertid klassifiseres ut fra at de er aktuelle, slik at alder ikke spiller noen rolle. Er de uaktuelle får de heller slettes.

8.4 Noen mulige regler om sensitivitetsgradering

§ 6.2-opplysninger bør minst klassifiseres sensitiv med hensyn på kompromittering.

Personopplysninger som graderes FORTROLIG etter Beskyttelsesinstruksen graderes SENSITIV med hensyn på kompromittering. STRENGT FORTROLIG graderes SÆRLIG SENSITIV.

Personopplysninger som er taushetsbelagte i h.h.t lov graderes minst MINDRE SENSITIV med hensyn på kompromittering.

9 INFORMASJONSSIKKERHET

Med 'sikring av informasjon', eller 'informasjons-sikkerhet', skal vi forstå sikring av informasjonens kvalitet, sikring av administrasjon av informasjonen, av identifikasjon, tilgjengelighet og autentisering av informasjonen.

Prosjektgruppen har bare diskutert informasjonskvalitetsaspektet. En har spesielt sett på den situasjon at opplysninger lagres i personregister (9.2).

9.1 Informasjonsskvalitet

Vi har tidligere omtalt datakvalitet, men skal her sette det inn i en større sammenheng.

(Martin:1976) har listet opp 12 momenter som kan brukes ved vurdering av informasjonsskvalitet. Disse er informasjonens nøyaktighet, i hvilken grad den dekker brukerens behov, dens relevans, hvor punktlig den leveres og hvor lett den er å forstå.

Videre må informasjonsverdien være lett fattelig, presentasjonen attraktiv, informasjonen må være kort, ajour, pålitelig, komplett og lett tilgjengelig.

Når en skal vurdere kvaliteten av informasjon kan en ta utgangspunkt i hva informasjonen gir seg ut for å beskrive. Eller med andre ord: Hva informasjonen intenderer å beskrive. Sammenligner en det med hva informasjonen faktisk beskriver, så får en nøyaktighets i beskrivelsen.

En beskrivelse av et forhold kan være mer eller mindre presis. Selv om en beskriver det samme forhold kan intensjonsdybden variere.

For en mer presis definisjon av termene nøyaktighet og presisjon (accuracy og precision), se (Ivanov:1972, s. 4.48).

Kvaliteten av informasjon avhenger også av hvor komplett den er i forhold til intensjonen. Eller mao hvor godt den dekker det som skal beskrives. Om informasjon som skulle vært tilgjengelig ikke er det, forringer dette kvaliteten til informasjonen.

Informasjonen må også være relevant i forhold til intensjonen. I motsatt fall svekkes kvaliteten. Om redundant informasjon forekommer kan dette oppfattes som støy.

Informasjonens aktualitet er også et kvalitetsaspekt. Når tiden går foreldes tidsavhengig informasjon. Det som en gang var riktig blir feil.

Strengt tatt kan aktualitet betraktes som et underpunkt av nøyaktighet. Men siden så mange forfattere opererer med

aktualitet som et eget kvalitetspunkt, gjøres det også her.

Martin ramser opp flere punkter under tilgjengelighet som kvalitetskrav. Slike er fysisk tilgjengelighet, om informasjonsverdien er lett fattelig, attraktiv presentasjon og at informasjonen er kort. Vi skal ikke betrakte informasjonens tilgjengelighet som et trekk ved dens kvalitet. Således vil vi kunne si at informasjonen er lite tilgjengelig, men av god kvalitet. Imidlertid vil vi si at tilgjengeligheten av informasjonens deler spille en rolle for helhetens kvalitet.

Hvor lett det er å tolke data riktig er viktig for informasjonskvaliteten. Tolkbarhet skal vi si er et forhold som påvirker kvaliteten.

Kvaliteten til en mengde informasjon uttrykkes ved dens

- nøyaktighet
- presisjon
- kompletthet
- relevans
- tolkbarhet og
- aktualitet

En slik oppstilling av aspekter ved informasjonskvalitet tar utgangspunkt i hva informasjonen intenderer å dekke. Vi kunne kalle det intensjonsrelatert kvalitet.

Men kvalitet på informasjonen kan også sees i forhold til informasjonsbehovet. Hvor god er altså den informasjonen en har tilgjengelig for det behov en har? Det er klart at dette er den viktigste kvaliteten å sikre. Men det kan en bare gjøre ved å sikre at det er godt samsvar mellom intensjon og behov. Og ved at det en faktisk beskriver ligger nært det en intenderer å beskrive.

behov	=	intensjon	-	faktisk
(for å dekke)		(å dekke)		(dekker)

La oss for et øyeblikk se hvordan vi finner igjen krav til datakvalitet i PRL. §8 refererer hva som skal skje for "uriktige" (nøyaktighet eller presisjon) og "ufullstendige" (kompletthet) opplysninger og opplysninger "som ikke lenger har betydning" (relevans og aktualitet).

I sin artikkel om Informasjonskvalitet (behovsrelatert) i Nordisk Datanytt 14/85 skriver Rabbe Wrede (tidligere ansatt i Datainspektionen) at informasjonskvalitet avhenger av datakvalitet og tolking av data. Han utelater således krav til modellkvalitet. (I praksis lær han vel datakvalitet omfatte dette).

Videre sier han at tolking og datakvalitet avhenger av anvenderens kunnskap, av aktualitet, riktighet, fullstendighet og presentasjon av data.

Her kunne det være av interesse å skjelne mellom hva datakvalitet er og hva som påvirker datakvaliteten. Wrede begrenser seg altså til hva som påvirker kvaliteten.

Kvaliteten av en mengde informasjon for et bestemt formål er også avhengig av kvaliteten av den modell informasjonen uttrykkes i og kvaliteten av dataene i modellen.

9.1.1 Modellkvalitet

For å beskrive et visst forhold trenges en modell. Den vanligste er naturlig språk. Naturlig språk modellen er basert på en mengde ord som tilhører språket og en grammatikk som sier hvordan ord og setninger kan formes. Tolkningsregler trengs for å tolke setninger i språket.

Modeller inneholder generelt grunnelementer, struktur-elementer samt relasjoner mellom elementer. Hva som er hensiktsmessig å uttrykke i en modell er avhengig av modellens element-, struktur- og relasjonstyper.

Modellkvaliteten kan vurderes etter hvor effektiv modellen er til å uttrykke det en vil ha uttrykt og hvor effektivt en kan tolke data i modellen, m m.

En modelltype kan vi si er bestemt av modellens grunnelementtyper, strukturelementtyper og relasjonstyper.

En gitt modell vil ha et visst antall av de ulike primitive elementtyper, en viss struktur og visse relasjoner mellom elementene.

Om en modell er velegnet eller ikke beror i første omgang på om modelltypen er egnet.

Selv om modelltypen er velegnet, trenger ikke modellen være god. Dette kan skyldes uheldig valg av elementer, struktur eller relasjoner til å representere de fenomener som skal beskrives.

En modell er ikke komplett (fullstendig) om det mangler elementer, struktur eller relasjoner til å representere den gitte informasjon. I dette tilfellet mister en informasjon ved representasjon i modellen.

Brukes feil elementtype, struktur eller relasjon forandres informasjonen når den representeres i modellen.

En modell som inneholder ikke relevante deler har redundans.

En modell må ha tilknyttet tolkningsregler slik at det er mulig å tolke dataene i modellen, betingelser dataene skal oppfylle, ol.

9.1.2 Datakvalitet

Anta at en gitt modell er velegnet til å uttrykke en informasjonsmengde. Kvaliteten i den representerte

informasjonen, eller datakvaliteten, trenger selvsagt likevel ikke bli god.

Med 'datakvalitet' menes her at data er komplette (fullstendige), nøyaktige (korrekte), presise (detaljerte) og aktuelle nok for et bestemt formål.

9.1.3 Tolking

Tolkinga av data i modellen er avhengig av kunnskapen til tolkeren om modellen og dekningsområdet for informasjonen. Tolkinga avhenger også av den støtte for tolking av data som finnes.

Dokumentasjon av data og modeller er viktig. Dette gjelder både beskrivelser og betingelser.

9.2 Registerkvalitet og kvalitet ved bruk av register

La oss her med et personregister forstå en samling av poster (postforekomster) med personopplysninger. En posttype inneholder en samling opplysningstyper. En post inneholder opplysninger for de forskjellige opplysningstypene.

Med 'god registerkvalitet' menes at den informasjon som lagres i, og hentes ut av et gitt register og benyttes er god.

For at dekningsområdet over personer i registeret skal være bra må registeret være komplett og irrelevante poster ikke forekomme. Ei forutsetning for dette er at kriteriene for innlemmelse i registeret er gode. Videre at disse kriteriene etterleves godt ved oppdatering av registeret (tolkinga er god). Ei anna forutsetning er at identifikasjonsnøkklene som brukes i registeret er gode (kfr pkt 2).

For at dekningsområdet over opplysningstypene i registeret skal være bra, må de relevante typer finnes, men ingen irrelevante.

Registerkvaliteten er ellers avhengig av registerets modell og datakvaliteten i postene (kfr pkt 1).

Vi kan presisere 'god registerkvalitet' til (a) at kriteriene for innlemmelse i registeret er gode, (b) at ajourholdsrutiner er gode slik at de personer som burde finnes i registeret etter kriteriene finnes der og at ingen ander enn disse finnes og (c) at datakvaliteten i registeret er god og (d) at modellkvaliteten er god.

Om kriteriene for innlemmelse i registeret ikke er gode vil ikke formålet med registeret realiseres på en god måte. Om praktiseringen av kriteriene ikke er god vil likedan personer som burde være med i registeret kanskje ikke være det eller personer som ikke burde være med kan være det. Kort sagt svarer ikke registerets intensjon til dets ekstensjon. Nå kan det å være med i et register ha store praktiske følger. De kan

være positive eller negative, avhengig av registerets art og formål. La oss se på fire typiske eksempler. Medfører det en rettighet å stå i et register er det en ulempe, feilaktig å være utelatt av registeret. Det kan likedan kanskje betraktes som en fordel, feilaktig å være inkludert.

Medfører det plikter eller byrder å stå i et register er det en fordel, relativt til disse, feilaktig å være utelatt og en ulempe feilaktig å være inkludert.

For de personer som riktig nok er inkludert i et register kan likevel problemer forekomme på grunn av datakvaliteten, som nevnt.

(1) Kvalitet i dataelementer

Datakvaliteten for et dataelement (felttype) er bare avhengig av hvor fullstendig, aktuell, nøyaktig og presis opplysningen er. Dette skyldes at dataelementet ikke er en sammensatt datatype. (Selvsagt er datatypen satt sammen av visse tegn, men et tegn er ingen datatype).

For å bedre datakvaliteten kan en knytte betingelser til dataelementer som enhver forekomst av typen element skal tilfredsstille. Netto inntekt skal typisk være mindre enn brutto. Disse betingelsene kan bli meget kompliserte hvis forekomsten er resultat av en omfattende beslutnings- eller beregningsprosess. I vår sammenheng er det interessant at hvis det foreligger en formell beskrivelse av disse betingelsene, så kan en automatisere kontrollen med at forekomster tilfredsstiller betingelsene når de blir lagt inn i registeret.

Slike betingelser på dataelementer vil kunne variere med tiden for et register.

'Betingete dataelementer' kan vi kalle slike som ikke automatisk forekommer for en person, selv om personen forekommer i registeret. At man kan opplyse navnet på ektefelle er betinget av at man er gift.

Enkelte dataelementer trenger altså ikke forekomme for en person som finnes i et register. Følgelig er det av interesse å vite betingelsene for at opplysninger skal, bør, kan .. forekomme. Om disse betingelsene kan formaliseres, så kan det ved registrering gis varsel hvis opplysninger som ikke skal gis faktisk blir gitt eller hvis opplysninger som skal gis ikke blir gitt, etc.

Hvis ei opplysning er resultatet av ei vurdering, kan det være av interesse å vite hvem som har foretatt vurderinga. Eventuelt også hvem som har kontrollert eller godkjent vurderinga. Det samme kan gjelde for registrering av opplysninger.

Det kan også være av interesse å vite hvor gammel en opplysning er. Dato bør kanskje registreres. Eventuelt kan gyldighetsperiode registreres.

Man bør skille mellom datakvalitet for vanlige opplysninger og datakvalitet for identifikasjons- og koblingsnøkler i registrene, som normalt vil være ekstra sensitive.

(2) Tolkning

Ser vi imidlertid på informasjonskvaliteten for en type dataelement, så vil denne også avhenge av hvordan brukeren av dataelementet forstår denne. Hermed trekkes også brukerne inn ved vurdering av informasjonskvaliteten. Opplæring i bruk av systemer blir et viktig forhold ved informasjonskvaliteten, også utover datakvaliteten selv.

Tidligere direktør i den svenske Datainspektionen, Jan Freese, har påvist 26 forskjellige inntektsbegreper i Sverige. Noe som viser de rike muligheter for forringelse av informasjonskvaliteten ved tolking.

Et tiltak i tillegg til opplæring for å bedre informasjonskvaliteten er dokumentasjon av dataelementet. Her kan en tenke seg alt fra instruksjer, brukerveiledninger, etc, til at beskrivelsen kan hentes fram på skjerm ved bruk av et dataelement.

(3) Identifikasjonsnøkkel

En god identifikasjonsnøkkel skiller entydig mellom ulike entiteter (dvs personer for oss) i et register. Den må følgelig bygge på et identifikasjonskriterium som gir entydig resultat. Det bør videre være slik at det som brukes som identifikasjonsnøkkel er størrelser som er fast knyttet til entiteten og ikke varierer over tid.

En dårlig nøkkel skiller dårlig mellom entitetene, slik at flere finnes på samme nøkkel. En risikerer da å få overskuddsinformasjon som kan være skadelig for den aktuelle personen. Dette gjelder også selv om en har en manuell sjekk av de funne opplysningene, siden denne vurdering kan være beheftet med feil. Det å finne en god nøkkel er å finne et godt kriterium for å identifisere entitetene.

Et annet forhold er kvaliteten av en forekomst av nøkkelen. Selv om identifikasjonskriteriet er bra trenger ikke identifikasjonen bli god. Dette kan da skyldes nøkkelkvaliteten. 'Kvalitet for en identifikasjonsnøkkel' er datakvaliteten for nøkkelen. Det betyr altså etter definisjonen av datakvalitet at nøkkelen er fullstendig, korrekt, detaljert og aktuell nok til et bestemt formål. Dette formålet er altså identifikasjon av personopplysninger i registre.

Vi ser at om nøkkelen ikke er detaljert nok, så vil den ikke skille mellom ulike entiteter. Er den for detaljert vil den først og fremst være uøkonomisk å bruke.

Er den ikke korrekt og aktuell (i registeret), så kan opplysninger om feil person finnes og opplysninger om riktig person være utilgjengelig.

(4) Koblingssikkerhet

Med 'kobling av personregistre' menes at personopplysninger fra et register sammenstilles med opplysninger fra et annet register. I denne prosessen kan opplysningstyper fjernes, slås

sammen eller splittes.

Hér kan det være grunn til å skille mellom koblinger for samme person og koblinger av opplysninger for flere personer.

'God koblingskvalitet' er betinget av at (a) koblingskriteriet er godt og (b) at identifikasjonen av de to opplysningsgrupper som kobles er god og at (c) opplysningskvaliteten er god.

I prinsippet kan vi tenke oss at enhver kobling leder fram til etablering av et nytt register eller til oppdatering av eksisterende register. Kriteriet for koblinga er da kriteriet for innlemmelse i registeret. Avhengig av koblingskriteriene vil nye betingelser kunne framstå på opplysningstypene.

Sett at en vil koble to registre for alle personer over 67 år. I det nye "registeret" (koblingsresultatet) gjelder da betingelsen

alder > 67 år.

Og nye betingelser for eksistens av opplysningstype vil kunne oppstå som et resultat av koblingen.

(5) Koblingsnøkler

Det som er sagt for identifikasjonsnøkler gjelder også for koblingsnøkler. I tillegg kommer at koblingskriteriet må være godt.

10 OPPSUMMERING OG DRØFTING AV SENTRALE SPØRSMÅL FOR UTFORMING OG ADMINISTRASJON AV SIKKERHETSFORSKRIFTER

10.1 Regulering av sikkerheten rundt personregister eller ikke?

Pr. i dag er personregistre gjennomgående for dårlig sikret. Dette gjelder både rutiner, utstyr, personell, m m. Sårbarhetsutvalget har anslått sikringsbehovet ut fra et sårbarhetsperspektiv å være i størrelsesorden 100-talls millioner kroner. Årsakene til denne tilstand er mange. Tidligere har en operert med "stand-alone" maskiner. Høg sikkerhet kunne oppnås med god fysisk adgangskontroll. Nå er dette bildet endret svært ved oppringte linjer, nettverk, den sterke utbredelsen av arbeidsstasjoner og PC-er, etc.

Det har i EDB-miljøene fra databehandlingens barndom vært lagt stor vekt på funksjonell sikkerhet. Men man har ofret mindre tanke på kompromitteringsfarer. Dette har resultert i mange systemer med lav sikkerhet. Disse systemene er så gjerne i ettertid sikret noe med løsnigner av ad hoc natur.

Det er derfor nødvendig å bringe sikkerheten rundt personregistre på et høyere nivå.

Hvordan skal en oppnå tilstrekkelig sikkerhet? Her trengs økt kunnskap gjennom informasjon, kurser, tidskrifter, opplæring og annet. Mange trenger dessverre den ekstra motivasjon negative erfaringer gir. Men først og fremst trengs investeringer og drift av ulike sikkerhetstiltak.

Et par mulige løsninger uten bruk av offentlige regler kan nevnes. Den første er situasjonen der eier står helt fritt i å fastlegge sikkerheten. Denne løsningen forutsetter ikke noen offentlig kontrollmyndighet.

En annen løsning kunne være å gi regler som "Vurder følgende tiltak...", sammen med vage normer om sikkerhetsnivået og kontrollmyndigheten til Datatilsynet.

Den første løsningen er ikke nok for å oppnå tilstrekkelig sikkerhet fordi sikkerhetsnivået vil bli ujamt og en del ganske sikkert vil operere med for lavt nivå på grunn av manglende kunnskaper, økonomi eller lignende. Det bør altså ikke være fritt opp til registereier å bestemme sikkerhetsnivå.

For den andre løsningen vil svært omfattende kontroller trenges for å forsikre seg om at sikkerhetsnivået er passende. Det er viktig å huske at trusler mot personopplysninger først og fremst vil gå ut over de registrerte. Det må derfor nøye vurderes å kreve et minimum av sikkerhetstiltak rundt personregistre.

Tiltakene kan gis i form av pålegg fra offentlig myndighet til register- og foretakseier. Offentlig myndighet (gjørne en annen) bør kontrollere at reglene etterleves.

Dette standpunktet antas å være lite kontroversielt i Norge.

10.2 Reguleringsform

Gjennom hvilken reguleringsform er det aktuelt å gi påleggene? (a) Man kan tenke seg utvidelse av PRL, (b) forskrifter for PRL gitt av Justisdepartementet, (c) generelle EDB-forskrifter (f eks i form av utvidelse av Datasikkerhetsdirektivet, som i såfall måtte gjelde privat sektor også) og (d) Datatilsynet fastsetter i forbindelse med konsesjonsbehandlingen regler om sikkerhet. Andre mer perifere alternativer kan også konstrueres.

(d) er dagens system, som er ufullstendig og noe tilfeldig hva angår spesifiserte tiltak. Det er en tungvingdt løsning å administrere fra Datatilsynet når en ikke har forskrifter å referere til. (d) vil derfor helst være aktuelt i kombinasjon med (b).

(a) vil være ei for "høg" innplassering av sikkerhetsregler i regelverket. Dermed står valget mellom (b) (evt. i kombinasjon med (d)) og (c). (c) har sitt sterkeste argument i nasjonal koordinering av EDB-sikkerheten. Ett regelverk vil gi et enklere "grensesnitt" mot registreier, EDB-senter, etc, med felles ordbruk og harmoniserte krav.

For (b) taler at sikkerhetsproblemene rundt personopplysninger er særegne. En kan ikke legge en tradisjonell risikoanalyse til grunn, men må finne andre måter å bestemme sikkerhetsnivået på.

Prosjektgruppa anbefaler (b) som reguleringsform for fastlegging av sikkerhet rundt personregister. Det må skje i koordinering med øvrig regelverk, og gjerne involvere (d).

10.3 Hvem skal fastsette sikkerhetsnivå?

Hvem skal tolke reglene i sikkerhetsforskriftene og bestemme sikkerhetsnivået? Det antas at sikkerhetsnivået vil bestemmes bl a ved sensitivitetsgradene til personopplysningene. Det er egentlig bare to kandidater her: Datatilsynet og registreier/-ansvarlig. Det som taler for at det skal være registreier (sammen med evt. databehandlingsforetak) er deres kunnskap om egne omgivelser, EDB-utrustning, bruk av registre, mindre arbeidsbyrde i Datatilsynet, bl a. For at det skal være Datatilsynet taler en bedre offentlig styring av sikkerhetsnivået rundt personregistre. Dette følger ikke av seg selv av et forskriftssett som tolkes av eier og kontrolleres av Datatilsynet. Dette er spesielt viktig siden sikkerhetsnivået allerede kan sies å være for lavt rundt EDB-anlegg. Prosjektgruppa går inn for at Datatilsynet fastsetter sikkerhetsnivået.

10.4 Hvordan skal sikkerhetsnivået fastlegges?

10.4.1 RP-orientert analyse

Den tradisjonelle metode, når en står fritt, er å fastlegge nivå ut fra en risikovurdering. Dvs. at en ideelt sett innfører de tiltakene som etter risikovurdering av trusler er lønnsomme. Dette er de tiltak som forebygger mer enn de koster. Her er det samme kasse som får dekke investering og tap. Situasjonen blir en annen når det er trusler mot personopplysninger det skal sikres mot. Trusler mot opplysningene rammer ikke bare eier av opplysningene, men ofte i enda større grad den person som beskrivelsene gjelder. Altså passer ikke tradisjonell risikoanalyse til å fastlegge tiltaksnivå rundt personregistre. Tvert imot kan det være grunn for å måle sårbarhet for trusler for registrert person istedet for registreier eller databehandlingsforetak. En kan forsøke å dekke inn registreiers, databehandlingsforetaks og andres sårbarhet for trusler i tillegg til registrert person. Her må det foretas et valg av referansepunkt for forskriftene.

Forskriften bør begrense seg til tiltak for å sikre registrert person mot trusler mot opplysningene om ham. Trusler som ikke rammer registrert person i særlig grad bør forskriftene ikke dekke. Sikkerhetsnivået bør altså fastlegges på grunnlag av en vurdering som tar utgangspunkt i registrert person. Dette kan kalles en RP-orientert analyse.

10.4.2 Ved sårbarhets eller risikoanalyse?

Et annet spørsmål er så om en bør legge til grunn en (RP-orientert) sårbarhets- eller risikoanalyse for å fastlegge sikkerhetsnivået. Spørsmålet kan omformes til om en bør legge vekt på hvor hyppig en trussel inntreffer ved vurdering av tiltaksnivå, og ikke bare på konsekvensene av at den inntreffer. Svaret her bør neppe være et enten eller. Selv om RP-orientert sårbarhet vil være svært forskjellig for ulike trusler og personer (jfr. adresseeksempelet foran), virker det ikke uoverstigelig å operere med grovere rubriserte sårbarhetsgrader for opplysningstype, registre og sett av registre. Det antas at en kan opprette et administrerbart system med sentral fastsetting av sårbarhetsgrad, som i sin tur styrer tiltaksnivå. Sårbarheten av trusler mot opplysninger vil variere med omgivelsene for registeret. Dette skyldes spesielt de bevisste truslene mot det, siden sårbarhet kan variere med formålet med trusselen.

Den hyppighet trusler inntreffer med vil nok i enda større grad variere med omgivelsene. Både geografiske-, bygningsmessige, utstyrs- og personellmessige forhold spiller inn. Det virker derfor vanskeligere å fastlegge sikkerhetsnivå ut fra en RP-orientert risikoanalyse.

Lokal risikovurdering vil føre til et meget omfattende arbeid for Datatilsynet, blant annet inspeksjoner på stedet, og må av den grunn frarådes. Noen sentral fastsetting av risiko for registre, anlegg og foretak ansees for

uaktuelt. Dette råd står i motstrid til de mer ideelle tilstander Datautvalget (NOU 1975:10, s.64) la opp til: "Før det gis konsesjon til et persondatasystem, bør EDB-anleggene og de steder som skal oppbevares og behandles, inspiseres av Datatilsynet for å klarlegge om tiltakene er tilstrekkelige".

Det refereres her til sikkerhetstiltak.

Om en ønsker å legge en RP-orientert sårbarhetsangivelse til grunn ved fastlegging av sikkerhetsnivå, må en først utforme en modell og så vise at den er mulig å anvende og tjener sitt formål.

10.5 Kommunisering av pålegg om sikring

Et interessant og viktig spørsmål er hvordan påleggene om sikring skal kommuniseres til eier og behandler av register. Det vil være minst tre alternativer for slik kommunikasjon. Hvilket som velges avhenger av hvilken reguleringsform en velger, hvem som skal fastsette sikkerhetsnivået og hvordan sikkerhetsnivået fastsettes.

10.5.1 Kommunikasjon av regler

Justisdepartementet utformer forskrifter som eier og behandler må sette seg inn i og forholde seg etter. Disse må ha skarpe kriterier for å kunne fungere bra alene. I tillegg må kontrollfunksjonen i Datatilsynet prioriteres. Reglene må formidles, enten de skal virke alene eller sammen med en sensitivitetsfastsetting foretatt av DT.

```
JDEPT  --> [ forskrifter ] --> eier/behandler
                                   ↑
                                   Datatilsynets kontroll
```

10.5.2 Kommunikasjon av sensitivitetsgrader

I dette alternativ inngår opplegget fra 10.5.1. I tillegg fastsetter Datatilsynet sensitivitet for ulike opplysninger som kommuniseres til eier og behandler:

```
Data-  --> [ sensitivitet ] --> eier/behandler
tilsynet
```

Dette avlaster eier og behandler for vurdering av sensitiviteter og eventuelt risikoer og belaster Datatilsynet noe tilsvarende. Kommunikasjon av sensitivitetsgrad gir Datatilsynet noe mer styring med utforming av tiltakene enn regelkommunikasjon alene gir.

10.5.3 Kommunikasjon av tiltak

Datatilsynet fastsetter et minimum av tiltak som skal legges rundt personregistre hos eier og behandler:

Data- --> tiltak --> eier/behandler
tilsynet

Skal dette være en overkommelig oppgave for Datatilsynet må tiltakene organiseres i form av tiltakspakker. Det var en slik løsning Føyen-arbeidsgruppa la opp til. Farer her er at en enten mister fleksibilitet eller pådrar Datatilsynet ei urimelig stor arbeidsmengde.

10.6 Forskriften

10.6.1 Omfang

Sikringsforskrifter bør ikke omfatte mer enn å sikre personverninteresser. Forskriftene bør altså i utgangspunktet kunne inneholde regler for sikring av opplysthet, diskresjon, fullstendighet, borgervennlig administrasjon og interessen mot overdreven kontroll og uhjemlet maktbruk.

Man bør også søke å sikre at formålet med register og bruk av register etterleves. Men reglene bør selvstøtt utformes slik at andre legitime interesser knyttet til bruk av personregistre ivaretas.

Men omfanget bør ikke være så vidt som rammen over tillater. Istedet bør forskriftene begrense seg til informasjonssikkerhet, med særlig vekt på sikring mot kompromittering og sikring av datakvalitet. Noe perifert vil sikring av behandlingskvalitet måtte bli, siden det viktigste kravet til behandlingskvalitet vil være at utdata har god kvalitet.

Prosjektgruppa anbefaler å begrense forskriften til sikring mot kompromittering og sikring av datakvalitet.

Arbeidsgruppa har supplert lista med sikring av at informasjon er tilgjengelig.

Dette medfører ei svak dekning av opplysthet. Noe dekning for borgervennlig administrasjon (kvalitetsaspektene) og overdreven kontroll, men ei god dekning av diskresjon og fullstendighet.

10.6.2 Reglene

La oss tenke oss at det er gitt forskrifter med regler på formen:

Hvis sensitivitet (risiko) for <trussel> mot <ressurs> er større enn <terskel> så skal (bør, må, ...) <tiltak> gjennomføres.

Slike regler antas laget for ulike <ressurs>er og <trussel>er ved å bestemme <terskel>er og <tiltak>.

La oss si at <ressurs> er personopplysning og <trussel>en

er kompromittering. Et eksempel på en mulig regel er da:

Hvis en personopplysning ikke er offentlig tilgjengelig skal den oppbevares utilgjengelig for uvedkommende (jfr. Beskyttelsesinstruksen, §9,1.ledd).

(1) Ressurs

Forskriftene må stille krav til beskyttelse av en rekke ressurser. De mest sentrale vil være personopplysning, post, register og eventuelt også sett av personregistre.

Arbeidsgruppa har begrenset seg til de tre første størrelser.

(2) Trusler

Forskriftene må gi regler om vidt forskjellige trusler, men først og fremst dekke kompromitteringstrusler og trusler mot datakvalitet for personopplysninger.

(3) Terskler

Tersklene bør gis i form av sensitivitetsgradene SÆRLIG SENSITIV, SENSITIV, MINDRE SENSITIV og IKKE SENSITIV.

Risikograder foreslås altså ikke innført.

(4) Tiltak

Det sentrale aspekt i forskriften er å fastsette krav til sikkerhetstiltak.

For å få minimale sikkerhetskrav oppfylt, kan en regel kreve spesifiserte tiltak gjennomført (eksplisitt angivelse av tiltak), f eks: Halonanlegg skal installeres. Eller den kan stille krav til et tiltaks effekt uten å presisere tiltaket (implisitt angivelse av tiltak). F eks: Ethvert branntilløp skal slukkes automatisk innen ett minutt.

Av disse to måter å uttrykke reglene på vil den siste være å foretrekke. Den stiller krav til hvordan en gitt trussel skal møtes uten å spesifisere teknikk. Dermed kan nye teknikker tas i bruk uten endring i regelverk.

Siden en ønsker minimumskrav til sikkerheten oppfylt, er det nødvendig å fastsette ikke bare tiltakstype, men også tiltaksnivå. Ved fastsettelse av krav til sikkerhet kan en for eksempel referere til standarder, norske, europeiske, Nato, eller andre standarder.

Om det forutsettes at sikkerhetsregler bør etableres og at tiltakstype og tiltaksnivå bør angis, slik at minimumsnivå for sikkerhet for et gitt miljø kan bestemmes, så er de mest grunnleggende forutsetninger lagt.

10.6.3 Systematikk

(1) Kapittelinnndeling

Forskriftene kan med fordel deles inn i fire eller flere kapitler. Ett med generelle regler, ett for register, ett for anlegg (og databehandlingsforetak) og minst ett for de øvrige foretakene.

Dette rådet er ikke fulgt av arbeidsgruppa.

(2) Struktur for personopplysninger

Registerkapittelet bør tale om personopplysninger, poster og registre.

Opplysningstype trenger en for å slippe å stille samme høye krav til sikring av ikke sensitive opplysninger som til sensitive i samme register. Register trenger en å tale om når det gjelder oppbevaring av kopier, fastsetting av sikkerhetsnivå for anlegg, m m. Sensitivitet for poster kan være nyttig ved fastsetting av krav ved for eksempel enkeltforespørsler mot personopplysninger on-line, overføring av en post over telenettet, m m. Selv om sensitivitet for kompromittering for hver av opplysningstypene er lav, kan helheten være mer sensitiv enn delene. Og registersensitiviteten kan ikke brukes for dette tilfelle, siden den avhenger av registerets størrelse.

(3) Hvilken systematikk skal en nytte i forskriften?

Hva skal være det viktigste sorteringskriterium? Ved utforming av forskriftene vil truslene mot ressursene være sentrale. Det kunne tale for (ressurs, trussel) som de to hovedkriterier i den rekkefølge. Terskler og tiltak blir her et resultat av analyse og diskusjonsprosessen.

Ved Datatilsynet's fastlegging av sikkerhetsnivå vil sensitivitetsgradene være sentrale. Det kunne tale for (terskel, tiltak, trussel, ressurs) som kriterier i den rekkefølge. Grunnen er at DT vil ha behov for å vurdere konsekvensene av sitt skjønn ved sensitivitetsfastsettelsen. Da vil (terskel, tiltak) være viktigst.

Registereier vil motta sensitiviteter for datakvalitet og kompromittering for opplysningstype, post og register. På grunnlag av disse opplysningene skal så tiltakene iverksettes. Kapitlet som omhandler sikring av registre kan derfor med fordel ha (trussel, ressurs, terskel, tiltak) som systematikk.

Det betyr ei inndeling a la

- \$1 Tiltak mot kompromittering
- \$1-1 Personopplysning
 - a) SÆRLIG SENSITIV
 - b) SENSITIV
 - c) MINDRE SENSITIV
 - d) IKKE SENSITIV

§1-2 Post med personopplysninger

a-d)

§1-3 Personregister

a-d)

§2 Tiltak for å sikre datakvalitet

Arbeidsgruppe har valgt å dele forskriften i fem deler:

- (1) Omfang og bruk av forskriften.
- (2) Administrativ og organisatorisk sikkerhet.
- (3) Tilgangskontroll og fysisk sikkerhet.
- (4) Spesielle krav til EDB-utstyr og bruk av EDB-utstyr og
- (5) Spesielle krav til registerkvalitet.

Dette bryter med den mer tradisjonelle tiltaks-systematikken. Men den vil være effektiv å bruke for registerreier. Et argument for den foreslåtte systematikk er at god oversikt over hva som skal gjøres av tiltak fremmer gjennomføringa av disse.

Siden registerkapittelet vil være det mest sentrale foruten det generelle kapitlet, er systematikken velegnet ved utforming av forskriften og fullt brukbar for anvendelsen av forskriften, foreslås denne som systematikk for forskriften. Det taler imot at den bryter med den tiltaks-systematikken som er vanlig i regelverk og framstillinger av EDB-sikkerhet, m m.

Den systematikk arbeidsgruppe har valgt er langt på veg (ressurs, trussel, tærskel). Trussel er benyttet som inndelingskriterium ved utskillelse av et kapittel 15 om registerkvalitet og flere paragrafer. Dermed er systematikken i utkastet også tilpasset EDB-sikkerhetstradisjonen.

10.6.4 Detaljeringsgrad og bruk av rundskriv

Et spørsmål prosjektet har berørt ved flere anledninger er detaljeringsgraden i forskriftene. Vi har blant annet vært inne på spørsmål om referanse til Norsk og andre standarder. Dette er et punkt som må avklares før en går i gang med finarbeidet i regelutforminga.

Skal en ellers (a) bare operere med frittstående forskrifter (b) ha forskrifter sammen med mer spesifikke rundskriv. Rundskriv kan tenkes utformet mot noenlunde homogene miljøer med hensyn på ressurser og registertyper. Det synes som om (b) er et aktuelt alternativ. Med relativt generelle forskrifter som ønskes nokså statiske over tid. Og som derfor stiller krav til teknikker heller enn å referere til eksplisitte teknikker. Rundskrivene kan i større grad tillates å referere eksplisitt til bestemte teknikker.

Det kan muligens være passende å utforme rundskriv etter

virksomhetsinndelinga i PRL.

Velger en (a) unngår en ikke volumiøse forskrifter med behov for hyppig revisjon. Dette følger av at en ønsker å oppnå en relativt presis angivelse av sikkerhetsnivået.

En like aktuell motivasjon for rundskriv som den som nevnes i (b) er muligheten for å få et enklere regelverk å forholde seg til for registeransvarlig. Man kan tenke seg å utforme f.eks. bransjerundskriv som supplement til forskriften. Enkelte regler vil være uaktuelle for eksempelvis et legekontor. For manuelle registre er en lang rekke bestemmelser uaktuelle.

10.7 Administrasjon og bruk av sikkerhetsforskriftene

Det foreslåtte system for fastsettelse av sikkerhet for personregistre kan oppsummeres slik: Justisdepartementet gir sikkerhetsforskrifter. Eventuelt med rundskriv gitt av Justisdepartementet eller Datatilsynet i tillegg. Datatilsynet fastsetter sensitivitet for registre, poster og opplysninger i registre for kompromittering og datakvalitet. Datatilsynet gir også spesielle sikkerhetsregler i forbindelse med konsesjonsbehandling av registre og foretak.

De tiltakene som register- og foretakseier skal gjennomføre avhenger av sensitiviteten av opplysningene i registrene og miljøet rundt registrene og bruken av registrene.

Et slikt system forutsetter noe utvidet informasjon fra register- og foretakseier til Datatilsynet sammenlignet med dagens system, fastsetting av sensitivitet hos Datatilsynet og registreier, fastsetting av enkelte sikkerhetsregler hos Datatilsynet og anvendelse av sikringsforskriftene og sensitivitetsgradene hos register- og foretakseier. Det vil således virke inn på forholdet mellom registreier og eksterne databehandlingsforetak.

Systemet medfører forandringer for konsesjonssøknadene, forskriftsunntatte registre og registre som allerede har konsesjon.

10.7.1 Registereier

Til hver opplysningstype, post og register skal det hos registreier foreligge en sensitivitetsangivelse for trusler mot kompromittering og for datakvalitet.

(1) Konsesjonssøknader

Ved søknad om konsesjon for register lister registreier opp opplysningstypene i registeret som før, gjerne med forslag til sensitivitet.

(2) Når konsesjon ikke er nødvendig

Her er det fire hovedtyper av tilfeller. Det gjelder registre som allerede har konsesjon, forskriftsunntatte registre, registre som er opprettet ved lov (§41) og ved innføring, endring eller fjerning av rutiner eller opplysningstyper som ikke trenger konsesjon.

For forskriftsunntatte registre kan sensitivitetsgraden stå i forskriftene. Registerierei er trenger derfor ikke å få noen spesiell innplassering for sitt register.

For §41-registre og registre som allerede har konsesjon må registerierei sende inn informasjon om register for sensitivitetsfastsettelse, gjerne med forslag.

(3) Gjennomføring av pålegg

Ved hjelp av forskriftene og sensitivitetene fastsatt av DT for opplysningstyper, post og registre skal registerierei gjennomføre forskriftenes pålegg. La oss anta at en (trussel, terskel)-systematikk brukes. Registerierei kan først sjekke tiltakene mot kompromittering som gjelder for ikke sensitive, mindre sensitive, sensitive og særlig sensitive personopplysninger etter tur. Dernest sjekkes tiltakene for poster og etter det tiltakene for register. De tiltakene som mangler må innføres og de som er utilstrekkelige får bedres.

Tilsvarende sjekkes om tiltakene for å sikre datakvalitet er tilfredsstillende.

Hvorvidt det bør være anledning for å søke dispensasjon fra forskriften holdes åpent. Som en sikkerhetsventil bør nok en slik adgang tas inn.

10.7.2 Datatilsynet

(1) Konsesjonsbehandling

Datatilsynet bestemmer ved konsesjon sensitivitet for opplysninger for kompromittering og datakvalitet. Dette skjer for opplysningstype, post og register. Fastlegging av grader kan gjerne skje etter forslag fra eier.

La oss som et abstrakt eksempel tenke oss et register med fem opplysningstyper, o1, o2, ..., o5. La sensitivitetsgradene være særlig sensitiv(3)...ikke sensitiv(0). Ved å føye to kolonner bak opplysningstype kan en gjøre plass på søknadskjema for sensitivitetsgradene.

	k	d	
o1	1	2	k = kompromittering
o2	0	1	d = trussel mot
o3	3	2	datakvalitet
o4	1	2	
o5	2	0	

Eksempelet viser at opplyningstype 1 er mindre sensitiv for kompromittering og sensitiv for trusler mot datakvalitet.

Før en tar stilling til om denne skissen angir en farbar vei, bør en gå relativt langt i detaljering av regler, slik at en kan se at graderinga verken er særlig for grov eller for fin.

Skal noen myndighet bestemme et laveste sikkerhetsnivå rundt personregistre med noen særlig presisjon, ser dette ut til å være det eneste alternativ. Må det oppgis, må en nøye seg med en kontrollfunksjon for Datatilsynet.

(2) Register som allerede har konsesjon og §41-reistre

Datatilsynet fastsetter sensitivitet for §41-registre og registre som allerede har konsesjon på grunnlag av melding.

Datatilsynet må gå gjennom alle tidligere gitte konsesjoner for å kontrollere at sensitivitet faktisk blir fastsatt for slike registre.

Litteraturoversikt

Andenæs, Johs.;

Spesiell strafferett;
Universitetsforlaget, Oslo, 1971.

Blekeli, Ragnar Dag;

Individ og informasjonsbehandling - et teoribidrag, i
Hafli(red): Utvalgte emner i JUS OG EDB;
Skriftserien JUS OG EDB 38, 2. utgave, 1979,
Institutt for rettsinformatikk.

Department of Defense;

Trusted Computer System Evaluation Criteria;
CSC-STD-001-83, DoD Computer Security Center, Ft. Meade,
Maryland, 15 August 1983.

Forsvarets overkommando;

Datasikkerhetsdirektivet;
Forsvarets overkommando, 1984.

Ivanov, Kristo;

Quality-Control of Information;
The Royal Institute of Technology, Department of
information processing, Computer Science,
Fack, S 104 05 Stockholm 50.

Kgl. res. 17.3.1972;

Beskyttelsesinstruksen;
Statsministerens kontor.

Martin, James;

Principles of Data-base Management;
Prentice-Hall, Inc., Englewood-Cliffs, 1976.

Parker, Donn B.;

Computer Security Management;
Reston Publishing Company Inc., Reston, Virginia, 1981

Seip & al.;

Datateknikk og samfunnets sårbarhet;
NOU 1986:12.

Seip & al.;

Offentlige persondatasystem og personvern;
NOU 1975:10

Selmer, Knut S.;

Innledning, i Djønnø, Grønn og Hafli: Personregisterloven
med kommentarer;
TANO, Oslo, 1987

Stortinget;

Personregisterloven av 9. juni 1978, nr. 48;

-;

Størkersen & al.;
EDB og sikkerhet;
Industriens sikkerhetsutvalg, Oslo, 1984.

Wrede, Rabbe;
Informationskvalite;
Nordisk Datanytt 14/85.

VEDLEGG: RAPPORT FRA JUSTISDEPARTEMENTETS ARBEIDS-
GRUPPE MED UTKAST TIL FORSKRIFT FOR SIKRING AV
PERSONREGISTRE

Utkastet ble oversendt Justisdepartementet den
5.11.87.

5.11.87

DISPOSISJON FOR RAPPORT TIL JUSTISDEPARTEMENTET FRA
ARBEIDSGRUPPEN SOM ER NEDSATT FOR Å LAGE UTKAST TIL
SIKRINGSFORSKRIFTER FOR PERSONREGISTRE

1. Arbeidsgruppens mandat. Behovet for forskrifter.	side	2
2. Arbeidsgruppens sammensetning.	"	3
3. Tidligere utkast.	"	4
4. Krav til sikring av personopplysninger i Sverige og Danmark.	"	7
5. Gjeldende regulering i Norge. Hvilke krav har blitt stilt.	"	9
6. Område for nye forskrifter. Forholdet til annet regelverk.	"	11
7. Forskriftens systematikk. Sårbarhetsgrader og sikkerhetsnivå.	"	13
8. Gruppens avveininger hva angår måten forskriftene skal gjøres gjeldende på.	"	16
9. Alternative reguleringsformer.	"	17
10. Merknader til de enkelte bestemmelser i . utkastet.	"	19
11. Administrative og økonomiske konsekvenser.	"	33
12. Vedlegg: Utkast til forskrift.		

RAPPORT TIL JUSTISDEPARTEMENTET FRA ARBEIDSGRUPPEN SOM ER NEDSATT FOR Å LAGE UTKAST TIL SIKRINGSFORSKRIFTER FOR PERSONREGISTRE

1. ARBEIDSGRUPPENS MANDAT

Justisdepartementet nedsatte den 25.4.86 en arbeidsgruppe som fikk i oppdrag å utarbeide utkast til sikringsforskrifter for personregistre.

Arbeidsgruppen fikk følgende mandat:

Arbeidsgruppen skal utarbeide et nytt utkast til forskrifter om sikringstiltak for personregistre og foretak som behandler personopplysninger. Gruppen skal gjennomgå det tidligere utkast til forskrifter og de høringsuttalelser som inntok til dette. Videre skal gruppen i den utstrekning dette finnes hensiktsmessig bygge på det arbeid som siden våren 1985 er utført av arbeidsgruppen som har vurdert sikkerhetsspørsmål ved databaserte personregistre.

Det vil også være naturlig for arbeidsgruppen å se hen til de vurderinger og konklusjoner som fremkommer i Sårbarhetsutvalgets innstilling og til de øvrige utredninger som de senere år er foretatt i offentlig og privat regi omkring datasårbarhet. Videre bør gruppen se nærmere på hva som foreligger om spørsmålet i de andre nordiske land.

Utkastet til forskrifter skal primært regulere hvilke tiltak som skal iverksettes for å sikre mot tap og kompromittering av personopplysninger.

Utkastet skal legge til grunn de endringer som er foreslått i den foran nevnte odelstingsproposisjon og bygge på den forskriftshjemmel som er foreslått som ny § 8b i personregisterloven.

Gruppen skal påse at de bestemmelser som blir foreslått i utkastet såvidt mulig harmoniserer med bestemmelser som er gitt i andre lover og forskrifter, herunder Data-sikkerhetsdirektivet.

Det skal legges vekt på at utkastet får en enkel utforming, slik at det blir lett å forstå og praktisere.

Endelig skal gruppen utrede de administrative og økonomiske konsekvenser av det forslag gruppen kommer fram til.

2. ARBEIDSGRUPPENS SAMMENSETNING OG VIRKSOMHET

Som medlemmer av arbeidsgruppen ble oppnevnt:

førstekonsulent Eirik Djønne, Datatilsynet, formann, spesialrådgiver Johannes Hansen, Datatilsynet, byråsjef Kristian Jahr, Justisdepartementet, og avdelingssjef Birger Melgård, A/S EDB, som representant for den Norske Dataforening.

Gruppen har hatt 18 møter, og foretok høsten 1986 en kort studietur til Danmark og Sverige.

Arbeidsgruppen finner grunn til å framheve at arbeidet har vært langt mer omfattende enn man regnet med på forhånd. Utkastet bygger på et dyptgående forarbeid, som i hovedsak er utført av spesialrådgiver i EDB, Johannes Hansen. Han har nyttet to årsverk på dette. Arbeidet er også internasjonalt sett et nybrottsarbeid. Dersom forskriften blir vedtatt, vil Norge være et foregangsland på dette området.

3. TIDLIGERE UTKAST TIL FORSKRIFTER

En arbeidsgruppe nedsatt våren 1981 under ledelse av daværende kontorsjef Arve Føyen i Datatilsynet, fremla et utkast til forskrifter om sikringstiltak ved anlegg for drift av personregistre. Dette utkastet var ute til høring 1981/1982, og det innkom en god del merknader.

Forskriftene tok sikte på å dekke det sikringsbehov som foreligger i fredssituasjon.

Gruppen redegjorde for daværende hjemler til å gi sikringsregler, og pekte på at hjemlene til dels var uegnede og utilstrekkelige. Klarere hjemmel til å gi sikringsforskrifter er som nevnt foran nå gitt med virkning fra 1.10.87, ved ny § 8 b i personregisterloven.

Arbeidsgruppen fant det mest nærliggende å konsentrere seg om å gi sikringsregler for anlegg for drift av personregistre, og sikringsregler for personregistre.

Gruppen vurderte hvordan reglene skulle virke under hensyntagen til hva som er mest hensiktsmessig både for registeransvarlige og for konsesjonsgivende myndighet, Datatilsynet.

For en del registre som er unntatt fra konsesjon i forskriftene til personregisterloven, fant de at det måtte være mest hensiktsmessig for begge parter å ha et regelsett som gjelder automatisk uten at Datatilsynet må inn i bildet. Arbeidsgruppen la til grunn at disse registrene er unntatt fra konsesjonsplikt fordi de er av en slik karakter at de må anses mindre truende for personvernet, og at de derfor kunne vurderes likt med hensyn til behovene for sikringstiltak. (Motsatt vurdering er lagt til grunn av den nye arbeidsgruppen. Sensitivitetsnivået i f.eks. legers pasientregistre adskiller seg vesentlig fra sensitivitetsnivået i rene adresseregistre for utsendelse av publikasjoner og trykksaker.)

De konsesjonspliktige registre ble antatt å være mere varierende med hensyn til sensitivitetsgrad. Det ble pekt på momenter som burde legges til grunn for vurderingen, som f.eks. registerets verdi for andre enn de med autorisert tilgang, og konsekvensen av misbruk, forvanskning og ødeleggelse.

For å lette Datatilsynets fremfinning til relevante sikringstiltak, og for å gi de registeransvarlige en viss grad av forutberegnelighet, foreslo gruppen at tiltakene skulle deles i tre nivåer.

Tiltakene skulle virke additivt slik at nivå B inkluderte tiltak av samme type som på nivå A, og nivå C inkluderte tiltak som nevnt på nivå A og B.

For hvert nivå ble det i forskriftsutkastet laget et sett av sikringstiltak som Datatilsynet kunne henvise til i konsesjonen. Det ble Datatilsynet som skulle klassifisere registeret og bestemme hvilket nivå for sikring som skulle kreves.

Tiltakene ble delt inn i fire typer etter hvilken funksjon tiltakene skulle ha, dvs hva de skulle sikre mot.

Arbeidsgruppen kom på den bakgrunn fram til følgende fire tiltakstyper:

- type 1: tiltak for sikring mot uautorisert tilgang til persondata
- type 2: tiltak for sikring mot sletting, forvanskning og ødelegging av persondata
- type 3: tiltak som skal sikre muligheten for kontroll og oppfølging
- type 4: tiltak som skal sikre tilgjengelighet og restituering av persondata

Arbeidsgruppen valgte denne inndelingen for at Datatilsynet med utgangspunkt i en vurdering av hva det er aktuelt å beskytte det enkelte register mot, skulle kunne angi hvilke sikringstiltak som er nødvendig.

Arbeidsgruppen viste til at det har vært vanlig å foreta en inndeling av sikringstiltak med utgangspunkt i en systematisk inndeling av selve tiltakene basert på "arten" av tiltak (administrative og organisatoriske tiltak, fysiske tiltak, programtekniske tiltak osv.)

Tilsvarende inndeling ble ikke benyttet i utkastet fordi det etter arbeidsgruppens oppfatning ikke lot seg administrere på en like hensiktsmessig måte i forbindelse med Datatilsynets konsesjonsbehandling.

Det innkom 33 høringsuttalelser. De fleste uttalte seg positivt om systemet med fire tiltakstyper og tre sikkerhetsnivåer fordi dette kunne gi god oversikt. Et mindretall uttalte seg mot systemet og pekte istedet på den systematikk som for eksempel er nyttet i datasikkerhetsdirektivet til Forsvartets Overkommando.

Flere høringsuttalelser ga uttrykk for at forskriftsfor-slaget ikke var tilstrekkelig godt tilpasset allerede eksisterende regelverk. Det ble særlig nevnt beskyttelsesinstruksen, sikkerhetsinstruksen og datasikkerhetsdirektivet.

Forbruker- og administrasjonsdepartementet nevnte også ønske om samordning i forhold til regelverk som nå ventes å komme, nemlig regler om datasikkerhet i krigssituasjoner og regler om datasikkerhet utifra vurderinger knyttet til datasamfunnets sårbarhet. Det ble også reist en viss kritikk mot bruken av fagtermer og forståelsen av de enkelte uttrykk.

Flere høringsinstanser pekte på at forskriftene var for detaljerte. Detaljeringsnivået ble hevdet å hindre nødvendig fleksibilitet og på den annen side ble forskriftene hevdet å være for lite nyanserte og fullstendige.

Noen hevdet at forskriftene ga for dårlig forutberegnelig -het og savnet en vurdering av økonomiske konsekvenser av tiltakene.

4. KRAV TIL SIKRING AV PERSONOPPLYSNINGER I SVERIGE OG DANMARK

Gruppen har foretatt en studietur til Danmark og Sverige for å gjøre seg kjent med det regelverk som eksisterer for sikring av personopplysninger i våre naboland. Dette hadde særlig interesse fordi de to nabolandene har hatt personregisterlovgivning lengre enn Norge, og ressursene på EDB-siden og sikringssiden har vært bedre.

4.1 Danmark

Gruppen hadde møte med representanter for Registertilsynet. I Danmark er det en lov for offentlig sektor og en for privat sektor.

Man begynte tidlig med utarbeidelse av regelverk for sikring ved EDB-sentraler, og krav til de enkelte myndigheter, og til terminalsystemene. Det ble innledet en dialog med datasentralene allerede i 1979-1980. Man ønsket generelle krav til sentralene og mer individuelt tilpassede krav til registrene.

Man fant at det ville vært tungvint for en sentral om den skulle ha oversikt over alle enkeltregler for de registre som inngikk i porteføljen. Registerne ble rubrisert i tre hovednivå:

1. mer eller mindre alminnelige registre
2. registre innenfor skatt, trygd og sosialsektor
3. helse- og strafferegistre

Registertilsynet gir på offentlig sektor uttalelse om hvert register og servicebyrå. Man har fått en forvaltningslov med taushetsregler fra 1.1.87.

Det er ikke stilt eksakte krav til makulering og transport, og det var heller ikke ønske om å gjøre det. I enkelttilfelle kunne det være aktuelt å fastsette slike vilkår. Sykehus skulle for eksempel ha kurér som fulgte dokumenter til makuleringsstedet.

Det var ikke aktuelt å innføre system med sertifisering av utstyr, rutiner etc.

Dersom det ved kontroll blir påvist at sikringen er for dårlig, blir det gitt en politisk innberettelse som sanksjon.

Man fant det vanskelig å gi sikringsregler på opplysnings-typenivå, men unntaksvis ble det fastsatt spesielle regler for deler av registre.

Detaljeringsgraden i sikringskravene er ikke stor. Man fastsetter for eksempel at det skal være adgangskontroll, men presiserer ikke hva den skal gå ut på.

Det er hittil ikke krevet kryptering på transmisjonslinjer, men skattemyndighetene bruker lukket brukergruppe. Det er innført kryptering av nøkkelfil ved Universitet. Ved kontroller blir det sjekket om reglene og regelsettet er godt nok.

Det stilles vilkår om at man skal ha rutiner for å sikre kvalitet i registre. Man fant at man måtte vektlegge logisk del av sikring, men fysisk sikring måtte ikke neglisjeres. Man prioriterte administrasjon av adgang til registre, og administrasjon av passord-tildeling. Det er ikke gitt konkrete regler om hvordan autorisering skal skje.

4.2 Sverige

I Sverige møtte arbeidsgruppen representanter for Sårbarhetsberedningen - SÅRB, og Datainspektionen.

I Sverige ble det også lagt vekt på at man skulle stille standardkrav til sikring, men ikke detaljert utformet. Man hadde laget såkalte maler som ble nyttet når det skulle gis konsesjon til sosial-, politi-, helse-, og trygderegistere.

Noen sikringsregler fremgikk også av en egen brosjyre.

Særlig følsomme registre skulle ikke kjøres på eksternt servicebyrå, dette gjaldt f.eks. register over homo-seksuelle.

Man hadde ikke fokusert særlig på datakvalitet, men Sparebankenes revisjonsbyrå - Sparev, så for tiden på problem knyttet til datakvalitet i REX, infordringssystemet til Kronofogden.

Gjert Persson fra Datainspektionen tok utgangspunkt i opplysningstyper når man skulle bestemme sensitivitet for registeret. Det var en viss motstand mot detaljerte regler p.g.a. ridigitet og dårlig tilegnelse. Han understreket betydningen av "behørighetskontroll"-systemene.

5 GJELDENDE REGULERING I NORGE

Personregisterloven av 9. juni 1978, har hjemler til å gi regler om sikring av personopplysninger og anlegg. Konkrete sikringsregler er i noe omfang fastsatt i konsesjoner for personregistre etter § 9, og i konsesjoner for de enkelte typer virksomheter som personregisterloven regulerer.

De krav til sikring som hittil har vært stilt har vært relativt lite detaljerte og mer preget av å være generelle normer.

For de registre som er fritatt fra konsesjonsplikt i forskriftene til personregisterloven, er det stilt krav om at den registeransvarlige må sørge for forsvarlig sikring av de registrerte personopplysninger, slik at ikke noen får tilgang til opplysningene uten å ha rett til eller krav på det. Datatilsynet kan gi pålegg som anses nødvendig for å oppnå forsvarlig sikring. Fødselsnummer må ikke benyttes utenpå postsendiger. Og for organ i staten er det forøvrig vist til gjeldende sikkerhets- og databeskyttelsesinstruks, med utfyllende bestemmelser (datasikkerhetsdirektivet).

Det er videre fastsatt regler om sletting av opplysninger.

Av konkrete vilkår i konsesjoner kan nevnes krav til fysisk sikring av datamedier og krav til makulering av utskrifter m.v. Unntaksvis er det også stilt mer spesifikke krav, der hvor sensitiviteten av opplysningene har tilsagt at registrering ikke kan foretas uten at visse sikrings tiltak er truffet.

I et tilfelle er helsemyndigheter pålagt å anskaffe en separat datamaskin for et særlig sensitivt register fordi den aktuelle nettverkløsning ikke var akseptabel. Personregisterloven gjelder både offentlig og privat sektor, men reguleringen av sikring av opplysninger er mer omfattende på offentlig sektor, fordi sikkerhetsinstruksen, beskyttelsesinstruksen og datasikkerhetsdirektivet, som utfyller disse to instruksene, får anvendelse på offentlig sektor.

Disse instruksene nytter ulike beskyttelsesgrader alt etter hvilket innhold dokumenter har, og den angir vilkårene for de ulike graderinger. Det er også fastsatt nærmere regler for påføring av beskyttelsesgrader, spredning, journalisering, oppbevaring, forsendelse og tilintetgjørelse.

Det er forøvrig i forvaltningsloven og særlovgivning fastsatt taushetspliktreger, som også har betydning for sikring mot kompromittering av opplysninger.

Andre regler som regulerer adgangen til utlevering av data er straffeloven § 90, som gjelder hemmeligholdelse av hensyn til rikets sikkerhet. Straffeloven § 121 sanksjonerer brudd på taushetsplikt, og straffeloven § 294

nr. 2, som gjelder den som er ansatt eller har vært ansatt i en bedrift, og som uberettiget bruker eller åpenbarer forretnings- eller bedriftshemmeligheter. Tilsvarende regler finnes i § 294 nr. 3 for de som er knyttet til bedrifter som konsulenter eller har et annet oppdrag.

Lov om forsvarshemmeligheter av 24. juli 1914 § 3 fastsetter forbud mot nedtegning og mangfoldiggjøring av karter, skisser, beskrivelse m.v., som antas å være til nytte for rikets fiende i krigstilfelle. Det kan også følge utleveringsregler av avtaler, f.eks. i arbeidsavtaler.

Regler som retter seg mot ulovlig tilegnelse av data finnes i straffeloven § 145, straffeloven § 405 a, og regler mot uberettiget bruk, finnes blant annet i patentloven, åndsverksloven, og markedsføringsloven. Det er også nylig vedtatt endringer i Straffeloven som retter seg inn mot datakriminalitet; § 151b, § 261, § 270 og § 403.

Det er innenfor enkelte bedrifter og i regi av enkelte foreninger utarbeidet sikkerhetsinstrukser, og forsikringsselskaper har også stilt visse vilkår for sikring. Brannforskrifter gir også regler om fysisk sikring.

Sårbarhetsutvalget har tilrådd en regulering for å redusere samfunnets sårbarhet. Det foreligger ennå ikke konkret formulering av slikt regelverk. Forbruker- og administrasjonsdepartementet har et koordineringsansvar for en datasikkerhetskampanje høsten 1987.

Det har fra Personregisterloven trådt i kraft i 1980 vært et savn at det ikke har foreligget et bedre regelverk for sikring av personopplysninger og personregistre. Dette har blant annet kommet fram igjennom den kontrollvirksomhet som Datatilsynet har drevet siden 1980, og det er også uttrykt ønske fra ulikt hold om å få klarere regler. Dette har blant annet sammenheng med det faktum at etablering av akseptabelt sikkerhetsnivå kan medføre betydelige kostnader, og pålegg om konkrete sikringstiltak vil lettere gi gjennomslag for å få finansiert adekvate tiltak.

I Seip-utvalgets utredning NOU 1975:10 er det lagt opp til omfattende rutiner for fastsettesle av sikringsvilkår.

6. OMRÅDET FOR FORSKRIFTER OM SIKRING AV PERSONREGISTRE - FORHOLDET TIL ANNET REGELVERK.

Det er i mandatet fastsatt at utkastet til forskrifter primært skal regulere hvilke tiltak som skal iverksettes for å sikre mot tap og kompromittering av personopplysninger.

Det har i de senere år blitt en stadig sterkere bevissthet omkring betydningen av tilstrekkelig kvalitet i databehandlingen. Arbeidsgruppen har merket seg dette, og har også funnet at krav til tilstrekkelig datakvalitet og kvalitet i behandlingen av opplysninger, er av vesentlig betydning for personvernet.

Det er personverninteressene man har tatt som utgangspunkt for arbeidet med å lage sikringsforskriftene. En drøfting av personverninteressene er foretatt i rapporten fra den arbeidsgruppe som arbeidet regi av Institutt for rettsinformatikk i 1985.

Overordnet kan man si at personvern i vår sammenheng er den enkeltes interesse i å føre kontroll med de opplysninger som beskriver en selv, og hva disse opplysningene brukes til. Delinteresse er interesse i diskresjon, det vil si at man ikke ønsker unødig spredning og bruk av opplysninger om seg selv, og interesse i fullstendighet, som går ut på at de opplysninger som brukes om en selv er ajour og korrekt. Den enkelte ønsker også å vite hva andre vet om en og hva opplysningene brukes til. Dette kalles interesse i opplysthet.

Det bør også skaffes til veie en visshet for at de data som er registrert representerer den informasjon som bruker forventer at den skal representere.

Dette innebærer at det utkast til forskrifter arbeidsgruppen har valgt å fremme i hovedsak vil dreie seg om å hindre kompromittering av personopplysninger, sikre tilgjengeligheten til opplysninger og i et visst omfang også forsøke å sikre adekvat kvalitetsnivå.

I og med at forskriftene tar utgangspunkt i personregisterlovens område, og har personverninteressene for øyet, vil enkelte av de krav til sikring som blir stilt være spesielt motiverte ut i fra dette.

Mange av de tiltak som følger av forskriftene vil ofte være etablert delvis ut i fra registreiers eget ønske om god sikkerhet, delvis hensyn til diskresjon for de som måtte være registrert, dels ønske om å unngå industrispio-nasje, og dels ønske om å redusere kostnader ved sikkerhetsmessige problemer.

I noe omfang kan det tenkes at regler som er fastsatt i disse forskrifter eller med hjemmel i disse forskrifter, vil føre til andre krav enn det som følger ut i fra andre hensyn.

Arbeidsgruppen har funnet det vanskelig å utarbeide et felles regelverk ut i fra alle de ulike interesser som gir behov for sikringstiltak.

Arbeidsgruppen har funnet det nødvendig å reservere disse forskriftene for personverninteressene, men ser at det samtidig kan gi sikkerhetsmessige gevinster ut i fra andre interesser.

Gjennom det system man har lagt opp til i forskriften kan det også finnes individuelle løsninger der hvor eventuell motstrid mellom krav etter ulike regelsett kan skape problemer for registereierne. Det er med andre ord tilstrebet en viss fleksibilitet.

Arbeidsgruppen har hatt kontakt med Forvarets Overkommando / Sikkerhetsstaben under arbeidet, og mottatt verdifulle synspunkter derfra. Utvalget har også hatt uformelle kontakter med ulike personer fra fagmiljøer av sentral betydning. Det er i et visst omfang tatt hensyn til de merknader som har innkommet.

Forskriftene vil få konsekvenser ikke bare for registreiere og registeransvarlige, men også for databehandlingsforetak og foretak som forestår makulering og transport av opplysninger. Leverandører blir også i noe omfang berørt av forskriftene.

Forskriftene vil gjelde både offentlig og privat sektor, og antas å ville utgjøre et vesentlig bidrag til sikring på privat sektor hvor reguleringen har vært særlig mangelfull.

Forskriftene er som hovedregel foreslått gitt anvendelse for både eksisterende og fremtidige registre og foretak. Enkelte unntak kan imidlertid komme inn her.

7. FORSKRIFTENES SYSTEMATIKK

Arbeidsgruppen har tatt utgangspunkt i at nivået for sikringstiltak må tilpasses etter hvor store problemer trusler mot en opplysning antas å volde for den registrertes personlige integritet, helse, omdømme, rettigheter eller økonomi. Det er videre ønskelig å fastsette minimumskrav til sikring av registre mm. avhengig av registrets sensitivitetsgrader.

Personregisterlovens § 10 nytter begrepet "volde problem for den enkelte". Gruppen har gjennom opplistingen av begreper prøvd å dekke inn de områder som kan lide overlast ved krenkelse av personverninteresser, slik at brukeren av forskriftene får en oppfordring til å tenke igjennom hvert enkelt av disse områdene.

Det er således ikke en normal avveining mellom de kostnader en hendelse kan påføre registreier sammenholdt med kostnaden for å etablere tiltak for å hindre eller redusere den aktuelle trussel, som kommer inn i denne sammenheng. Krenkelse av personlig integritet kan ofte vanskelig kvantifiseres i kroner og ører.

Gruppen har funnet det hensiktsmessig å operere med sensitivitetsgrader knyttet til hvor store problemer trusler mot opplysningen antas å volde. Slik sensitivitetsfastsettelse skal foretas på fire nivå: ikke sensitiv, mindre sensitiv, sensitiv og særlig sensitiv. Sensitivitetsvurderingen skal gjøres både med hensyn til kompromittering av opplysninger, datakvalitet og tilgjengelighet.

Gruppen har funnet at slik sensitivitetsinnplassering gir den enkleste og den mest naturlige inngang til anvendelse av regelverket. Denne sensitivitetsinnplasseringen vil normalt bli foretatt av Datatilsynet etter forslag fra registreier.

Når det gjelder de registre som er fritatt fra konsesjonsplikt på visse vilkår i forskriftene til personregisterloven, forutsetter arbeidsgruppen at Justisdepartementet vil fastsette sensitivitetsnivå ved endring av disse forskrifter. Det er denne innplassering som gir anvisning på hvilke sikringsnivå registreier og registeransvarlig skal innrette seg på innen de ulike tiltaksområder.

Denne organiseringen av forskriftene fokuserer på personvern og er av utvalget ansett for å være mest hensiktsmessig.

Forskriftene introduserer deretter de tre sikkerhetsnivåer kalt A, B og C, som er knyttet opp til sensitivitetsgraden. I likhet med tidligere utkast vil det også her være slik at tiltak på nivå C også innbefatter de tiltak som er nevnt under A og B.

Innledningsvis er det inntatt en liste med definisjoner av

ord og uttrykk. Forskriftene regulerer et relativt nytt område med en terminologi som er tildels lite kjent og vanskelig for andre enn fagfolk. I et par tilfeller har det også vært nødvendig å introdusere helt nye begreper.

Deretter introduserer forskriftene de ulike ressurser og prosesser som er gjenstand for sikring, så som nettverk, kommunikasjoner, datamaskiner, lagringsmedia, periferutstyr og programmer.

Det er lagt stor vekt på å gi regler om (fysiske) adgangskontroll og (elektronisk) tilgangskontroll. Felles for adgangskontroll og tilgangskontroll er behovet for det som i forskriftene kalles operasjonsskontrollsystem.

Begrepet operasjonsskontroll er ikke særlig utbredt fra tidligere. Men arbeidsgruppen har funnet det hensiktsmessig å behandle samlet spørsmål som har med kontroll av hva forskjellige aktører kan få utføre av operasjoner på de ulike ressurser. Slike spørsmål omfatter sikkerhet vedrørende identifikasjon og autentisering av aktører, autorisasjoner, sikkerhet for det som i utkastet til forskrifter er kalt sperrer og de mekanismer som skal gi eller nekte tillatelse til operasjoner. Dette innebærer blant annet at man kan gi generelle regler for slike OK-systemer og ikke trenger å gjenta dem i de enkelte sammenhenger senere i forskriften.

Fysiske sikkerhetstiltak og tilgangskontroll behandles særskilt. Egne kapitler er viet sikkerhetstiltak i operativsystemer, sikkerhetstiltak for databaser og sikkerhetstiltak i maskinvare.

Det er videre stilt generelle krav til opplysnings- og registerkvalitet, og fastsatt nærmere tiltak for å styrke kvaliteten.

Det er foreslått regler for foretak som utfører oppdrag for andre, såkalte oppdragsforetak. Det er også foreslått krav til produsenter og importører som gjelder plikt til å opplyse til detaljister, kjøpere eller leiere i hvilken utstrekning produktene tilfredsstiller kravene i forskriften.

Videre er det foreslått krav til sikkerhetsorganisasjonen og administrasjonen av sikkerhetsarbeidet.

Gruppen har i løpet av den perioden det har jobbet med utkastet sett at forskrifter som skal gi tilstrekkelig materiell effekt, bør være såvidt presise som det nå foreliggende utkast. Det er klart at forskrifter som eventuelt bare angir tiltaksområder slik at man skal vurdere tiltak uten nærmere spesifisering, vil være enklere å lese og enklere å få forståelse av, men samtidig gir ikke dette noen garanti for et minimum av sikkerhet.

Med utgangspunkt i sensitivitetsinnplasseringen skal registreier eller registeransvarlig finne fram til de til-

tak som er pålagt i forskriften ut fra de aktuelle omgivelsene og den aktuelle løsning. F.eks. vil kapittelet om nettverks- og kommunikasjonssikkerhet ikke få anvendelse der hvor et register ligger på utstyr som ikke har kommunikasjon med omverden, og kapittelet om sikkerhetstiltak for databaser får rimeligvis bare anvendelse der hvor man har anvendt databaseløsning.

Således vil ikke alle paragrafer i forskriftene få relevans for alle registereiere. Dette vil i særdeleshet gjelde der hvor registre er manuelle.

8. GRUPPENS AVVEININGER HVA ANGÅR MÅTEN FORSKRIFTENE SKAL GJØRES GJELDENE PÅ.

Gruppen har funnet det nødvendig at Datatilsynet må ta en aktiv del i fastsettelsen av sikringsreglene for den enkelte registreier. Dette er fordi variasjonene i sensitivitet overfor kompromittering, tilgjengelighet og data-kvalitet varierer meget sterkt fra register til register, og fordi detaljeringsgraden i regelverket innebærer et visst behov for konkret vurdering av behov for tiltak.

Alle de registre som er fritatt fra konsesjonsplikt i kapittel 2 i forskrifter av 21. desember 1979 og 10. mars 1981 vil få fastsatt sensitivitet ved endring av disse forskriftene. Ut i fra denne fastsettelse må den enkelte registreier selv finne fram til de konkrete sikringstiltak som skal opprettes for registre.

Datatilsynet har ikke oversikt over disse registreierne, og det må derfor foretas alminnelig og tilstrekkelig kunngjøring av forskriftsendringene. Når det derimot gjelder de registre som er konsesjonspliktig, vil Datatilsynet tilskrive eiere av eksisterende registre, orientere om det nye regelverket, og be om å få forslag til sensitivitetsvurdering. Utfra dette vil Datatilsynet fastsette sensitivitet og ut i fra denne fastsettelsen skal registreier innrette seg på de riktige tiltaksnivå.

Dette systemet innebærer også at Datatilsynet kan gjøre unntak fra spesielle sikringskrav, eller eventuelt supplere de krav som følger av forskriftene. Dette systemet gir både god fleksibilitet og effektivitet, og gir åpning for tilpasninger.

Dette opplegget vil medføre økt arbeidsbyrde for Datatilsynet, blant annet ved at innplassering skal foretas, og at man på ny må ta kontakt med alle de som er meddelt konsesjoner. Men det må her foretas en prioritering slik at man tar fatt på de registre som man antar det er sterkeste behov for å få fastsatt vilkår for.

9. ALTERNATIVE REGULERINGSFORMER

Arbeidsgruppen har vurdert alternative, mindre kostnadskrevenne løsninger. Dette er vurdert og nedenstående alternativer kan drøftes:

9.1. En mulighet er å redusere forskriftene til å gjelde bare tiltak mot tap og kompromittering av opplysninger. Det vil medføre at flere bestemmelser kan forenkles eller sløyfes.

Det gjelder bl.a. kontroll ved registrering og overføring av data. Slik innskrenkning gir imidlertid liten gevinst ressursmessig, fordi de regler som er foreslått for å sikre kvalitet påfører registereierne relativt beskjedne byrder. Det samme gjelder for leverandører og Datatilsynet. De bestemmelsene som eventuelt sløyfes må anses som viktige for ivaretagelse av personvernet, fordi faren for bruk av uriktige opplysninger ellers vil øke.

9.2. Videre kan man opprettholde dagens ordning med vage krav til sikring, som inntatt i nåværende § 2-1 i forskriftene til personregisterloven, som lyder:

" Den registeransvarlige må sørge for forsvarlig sikring av de registrerte personopplysninger, slik at ikke noen får tilgang til opplysningene uten å ha rett til eller krav på dem. Datatilsynet kan gi pålegg som ansees nødvendige for å oppnå forsvarlig sikring."

Dette alternativet innebærer at sikringskrav formuleres individuelt i konsesjoner, eller som pålegg etter kontroll av registre som er fritatt fra konsesjonsplikt.

En slik ordning gir liten forutberegnelighet hva angår tiltakskrav. Datatilsynet har hittil ligget lavt hva angår å stille konkrete sikringskrav i påvente av forskrifter. Datatilsynets mangel på personalressurser har også bidratt til manglende bruk av hjemlene. Dersom denne ordningen blir valgt, vil det like fullt kreve ressurser såvel hos Datatilsynet som hos registereierne.

9.3. Kostnadmessige reduksjoner kan også oppnås enten ved lempelig innplassering av personregistre hva angår sensitivitet eller modifisering av kravene på de ulike nivåer. Arbeidsgruppen finner det vanskelig å lansere forslag til svekkelse av det sikringsnivå utkastet legger opp til.

Som en generell merknad til disse alternativer må nevnes at man står foran en periode der sensitive og særlig sensitive opplysninger som blir lagret ved større EDB-anlegg vil bli ønsket overført til andre anlegg. Dette kan gjelde pasientopplysninger, klientopplysninger o.l.

Videre er det slik at det allerede i dag er for lav sikkerhet rundt en rekke registre. En løsning som ikke fastsetter sikkerhetsnivået rundt registre avhengig av sensitivitetsgrader, kan ikke ventes å bedre den foreliggende situasjon vesentlig.

Det er også av betydning at sikkerhetsreglene gis i forskrifts form. Grunnen til dette er den virkning forskriften vil få i markedet for EDB- og sikkerhetsutstyr. De plikter utkastet legger på leverandører kan vanskelig pålegges ved enkeltvedtak.

10. MERKNADER TIL DE ENKELTE BESTEMMELSER I UTKASTET TIL SIKRINGSFORSKRIFTER

Del 1. OMFANG OG BRUK AV FORSKRIFTEN.

1. Omfang av, definisjoner i og administrasjon av forskriften.

Til § 1-1 Forskriftens omfang.

Forskriften gjelder sikring av personopplysninger, dvs. det området personregisterloven har. Det er samtidig gitt åpning for en fleksibilitet ved at Datatilsynet kan gjøre unntak fra bestemmelsene, og også i særlige tilfeller fastsette ytterligere regler.

Til § 1-2 Sensitivitetsgrader.

Det er foretatt drøfting av denne bestemmelsen foran, se under kap. 7.

Til § 1-3 Fastsettelse av sensitivitetsgrader for registre.

Det er lagt opp til at det hver for seg skal fastsettes sensitivitetsgrader for kompromittering, for datakvalitet for hver enkelt opplysningstype, for alle opplysnings-typene samlet og for hele registeret. Det skal også fastsettes sensitivitetsgrad for tilgjengelighet for hele registret. F.eks. er tilgjengelighet til blodtyper viktigere i journal enn i forskning. Sensitiviteten for kompromittering kan være like stor for en legejournal og et medisinsk forskningsregister. Men sensitiviteten for kvalitetsbrist er større for journaler enn forskningsregister.

Grunnen til at det skal fastsettes sensitivitet på såvel registernivå som opplysningstypenivå, er at sensitiviteten for opplysninger i et register kan variere sterkt fra de mer nøytrale opplysninger som navn og adresse til opplysninger om f.eks. helseforhold.

Det kan være grunn til å ha ulike sikringstiltak for ulike typer opplysninger i registeret. Hvis man lot nivået ene og alene bestemmes av de mest sensitive opplysningene og la de tiltakene gjelde alle opplysninger i registeret, så kan det medføre en overdimensjonering av tiltakene. Dette kan gi økte kostnader, og svekke respekten for kravene.

Datatilsynet er tillagt en aktiv rolle i fastsettelsen av sensitivitetsgrader, men registreiers forslag bør først være innhentet. Det innebærer bl.a. at registreier selv må tenke gjennom sensitiviteten til registeret og opplysningstypene og gir også et bedre grunnlag for Datatilsynet til å fastsette endelig sensitivitet.

Til § 1-4 Fastsetting av sensitivitetsgrader for lagringsmedia.

Bestemmelsen henleder den registeransvarliges oppmerksomhet på at også de media som nyttes til lagring av personopplysninger må vurderes med tanke på sensitivitet. Denne sensitiviteten må bygge på sensitivitetsgradene for de registre eller deler av registre som finnes på dem. Det er klart at lagringsmedia (magnetbånd, disketter etc.) som inneholder lite følsomme registre kan ha en lavere sikring mot kompromittering enn media med følsomme opplysninger. Krav til sikring med tanke på tilgjengelighet må også knyttes til hvor stor uløpse de registrerte vil bli påført ved manglende tilgjengelighet.

Til § 1-5 Om fastsettelse av sikkerhetsnivå.

Forslaget om fastsettelse av tre nivåer for sikkerhetstiltak: A, B, C, minner om det system forrige utvalg lanserte. Nivået er avhengig av den sensitivitetsgrad som er funnet etter systemet nevnt i § 1-2. Krav som ikke er knyttet til noe bestemt nivå gjelder også for de registre som ikke er sensitive.

Til § 1-6 Definisjon av ord og uttrykk. Forkortelser.

Utvalget har funnet det riktig å definere en del uttrykk som nyttes i forskriften for å redusere faren for misforståelser og lette tilgjengeligheten til reglene. Det er forsøkt å nytte anerkjente definisjoner, men det er likevel lagt vekt på å forklare uttrykkene slik de er lagt til grunn i denne forskrift.

Del 2. ADMINISTRATIV OG ORGANISATORISK SIKKERHET

2. Sikkerhetsorganisasjon og administrasjon.

Til § 2-1 Organisasjon og administrasjon internt.

Bestemmelsen presiserer at også ansvaret for sikkerheten påligger registeransvarlig. Registeransvarlig er utpekt i konsesjonen for registeret og denne har særlig ansvar for å sørge for at regelverket som gjelder for registeret blir etterlevd. Det er adgang til å delegerer ansvaret for og kontrollen med sikkerheten, og den daglige sikkerhetsmessige ledelse kan innehas av en sikkerhetsansvarlig som kan være en annen enn registeransvarlige. Dersom organisasjonen er såvidt stor at mer enn fem personer har ansvar for deler av drift og kontrollen av sikkerhetstiltak for registeret, bør det finnes en sikkerhetsorganisasjon. Dette er for å ha en bedre styring med sikkerheten. Det er også gitt anbefaling om at man skal utarbeide instruksjoner for de ulike funksjoner for sikkerhet.

Til § 2-2 Oppdrag som utføres ved andre foretak.

Bestemmelsen pålegger den registeransvarlige å se til at

kontrollen med sikkerheten til et register er i samsvar med dette regelverket selv om registeret blir overlatt til annet foretak, så som ved databehandling, service, vedlikeholdsoppdrag e.l.

Til § 2-3 Adgangs- og tilgangskontroll.

Bestemmelsen introduserer regler om fysisk adgangskontroll og tilgangskontroll som nevnt nedenfor under §§ 5-4 og 6-1. Det er verdt å merke seg at adgangs- og tilgangskontroll er eksempler på operasjonkontrollsystemer. Mens adgangskontroll kan få anvendelse for manuelle registre og EDB-registre så vil tilgangskontroll kun gjelde EDB-førte registre.

Til kap. 3. SIKKERHETSTILTAK FOR FORETAK SOM UTFØRER
OPPDRAG FOR ANDRE (OPPDRAGSFORETAK)

Til § 3-1 Generelt.

Bestemmelsen stiller på sikkerhetsnivå B krav til såkalte oppdragsforetak. Kravene gjelder da også nivå C. Oppdragsforetak vil kunne være databehandlingsforetak som utfører bearbeiding av personopplysninger for andre, det kan være vedlikeholdsforetak som står for vedlikehold av programvare og utstyr, det kan være foretak som forestår transport av lagringsmedia som f.eks. budtjenester og det kan gjelde foretak som står for makulering av utskrifter. Begrunnelsen for disse reglene er at enkelte registereiere i visse sammenhenger vil måtte overlate registeret til eksterne foretak. Ofte vil disse foretak ha konsesjon til å drive sin virksomhet fra Datatilsynet, men det vil ikke alltid være tilfelle. Det er derfor behov for en særskilt regel som sikrer visse minimumskrav til sikkerhet og gir registeransvarlig en rimelig mulighet til å kunne forvise seg om at de sikringsregler som gjelder for registeret blir etterlevet også når registeret befinner seg utenfor hans domene.

Til § 3-2 Krav til databehandlings- og vedlikeholdsforetak.

Kravet om at autorisasjoner for drifts- og vedlikeholds-personale skal godkjennes av registeransvarlig innebærer at den registeransvarlige faktisk har en vetorett hva angår omfanget av de autorisasjoner som gis. Bestemmelsen tar ikke sikte på å gi registeransvarlige en vetorett hva angår de personer i vedkommende foretak som skal kunne autoriseres til å utføre de aktuelle typer operasjoner. Bestemmelsen gir også den registeransvarlige rett til tilgang for å kunne kontrollere de avtalte tiltak. Bestemmelsen må brukes med fornuft og er ikke ment å innebære at den registeransvarlige til en hver tid skal kunne foreta omfattende kontroller av den virksomhet oppdragsforetaket driver.

Til § 3-3 Krav til produsenter og importører.

Bestemmelsen pålegger produsenter og importører av nettverk, datamaskiner, databasesystemer å vurdere i hvilken grad deres produkter tilfredsstiller de nærmere spesifiserte krav i disse forskrifter, og gi detaljister kjøpere, leiere og Datatilsynet nødvendige opplysninger om dette. Denne plikten er introdusert for å gi de registeransvarlige bedre mulighet til å kontrollere om de krav som blir stilt til sikring blir tilfredsstilt. Den enkelte utstyrskjøper vil vanskelig selv kunne vurdere dette. Det vil etter dette bli en plikt for, og en kostnad for produsenter og importører å foreta en nødvendig vurdering av produktene. Dersom Datatilsynet blir kjent med at produsenter og importører gir feilaktig opplysning om hvilke krav deres produkter tilfredsstiller, vil de berørte bli varslet om dette.

Til del 3. Tilgangskontroll og fysisk sikkerhet.

Kap. 4 OPERASJONSKONTROLLSYSTEMER.

Kapitlet gir hjelpebegreper til kapitlene om bl.a. fysisk adgangskontroll og tilgangskontroll, se nedenfor.

Til § 4-1 Operasjonskontrollsystemer.

Et operasjonskontrollsystem er et system for å kontrollere aktørers mulighet til å utføre operasjoner på bestemte ressurser. OK-systemet består av en sperre, autorisasjoner og en eller flere operasjonskontrollmekanismer. Et operasjonskontrollsystem kan legges utenpå et annet. F.eks. kan man ved inngang til en bygning ha en fysisk adgangskontroll, og videre ha en fysisk adgangskontroll inn til en etasje, maskinrom, etc. Endelig kan en ha tilgangskontroll ved hjelp av f.eks. passord for å komme inn i et nettverk, en maskin, et brukerområde, et program mm.

En sperre er et hinder for tilgang til operasjoner og ressurser. Sperren kan f.eks. være en vegg, vindu, dør eller en påloggingsmekanisme. Autorisasjon er en tillatelse til en aktør eller en gruppe aktører til å utføre bestemte operasjoner. En operasjonskontrollmekanisme (OK-mekanisme) er en innretning for å identifisere og autentisere aktører, slippe autoriserte aktører til og hindre uautoriserte i å slippe til sperrede operasjoner og objekter. Eksempel på dette er vakt, påloggingskontroll og kortlesersystem.

Til § 4-1, 3. ledd. Dette er en påpekning av at sikkerheten ikke er større enn det svakeste ledd i kjeden.

Til § 4-1, 4. ledd. Bestemmelsen gir en generell regel om utforming av OK-systemer og pålegger den registeransvarlige å følge opp etterlevelsen av reglene for operasjonskontrollen. Det er ikke stilt spesifikt krav til hyppigheten av slik kontroll, men det skal kontrolleres "jevnlig".

Til § 4-1, 5. ledd. Bestemmelsen stiller krav om faste rutiner for drift og vedlikehold av slike systemer, og legger vekt på å unngå uformelle autorisasjoner.

Til § 4-2 Sperrer.

Sperre er definert foran. Eksempel på krav til sperrer finnes i § 5-1 Innbruddssikkerhet.

Til § 4-3. Krav til aktører.

Bestemmelsen stiller krav til opplæring, instruks og arbeidsforhold for personer som autoriseres til å utføre operasjoner. Bestemmelsen stiller også krav til den enkelte aktør om at han ikke skal misbruke autorisasjoner til å utføre oppdrag det ikke er behov for å utføre. Det kan være at en aktør går inn og ser på registrerte opplysninger om en annen for egne private formål. Aktørene er også pålagt en plikt til å hindre at uvedkommende får tilgang til brukeridentifikasjon, passord, nøkler, terminaler, lokaler mm.

Det er på nivå B i tillegg stilt krav om at det skal gis sikkerhetsopplæring til aktører og at det bør foreligge en sikkerhetsinstruks for operatørene. Det er altså bare en anbefaling om at det skal foreligge sikkerhetsinstruks.

Det er på nivå A stilt krav om at automatiske prosesser skal være dokumenterte og dette gjelder jo derved også for nivåene B og C.

Til § 4-4 Krav til operasjoner.

Bestemmelsen stiller krav til tilretteleggelse, strukturering og kontroll med utførelse av operasjoner. Det kan være aktuelt med tiltak som videoovervåkning og logging av operasjoner, tiltak som i seg selv kan være personverntruende. Vi har her eksempel på mulighet for motstrid mellom sikringstiltak og personvern.

Til § 4-5 Autorisasjoner.

Ordet autorisasjon er definert foran. Bestemmelsen stiller visse generelle krav til autorisasjoner, registrering og beskyttelse av autorisasjonene. Det er videre stilt krav om autorisasjon for tilgang til maskinlesbare, formaterte registre. Det er også stilt krav for tilgang til dokumentbaserte og manuelle skjemabaserte registre.

På nivå A er det stilt krav om at autorisasjonene bare skal gis til den som har behov for det m.v. og regelen kan sies å knesette en "need to do"-regel.

For nivå B er det fastsatt at enhver som skal autorisere selv skal ha autorisasjon fra registeransvarlig. Kravet kan virke noe rigid ved store organinsasjoner, men Data-tilsynet har adgang til å dispensere. Det er videre stilt krav om at autorisasjonene skal registreres og at de skal beskyttes mot innsyn, endring og sletting. Dette er for å hindre misbruk ved at man skaffer rede på hvem som er autorisert til å gjøre hva.

Når det gjelder autorisasjon for tilgang til maskinlesbare formaterte registre, kan det på A-nivå gis tilgang til hele registeret under ett. Her kan imidlertid taushetsplikt komme inn og sette begrensninger som det må tas hensyn til.

På B-nivå skal det ikke gis tilgang til opplysninger om andre personer enn det er behov for. Det kan f.eks. innebære en geografisk begrensning slik at et distrikts-sosialkontor har tilgang til opplysninger om klienter innen sitt eget distrikt. Videre skal det bare gis tilgang til operasjoner av den type det er behov for. Dette kan innebære at en som bare har behov for å lese opplysninger i registeret ikke skal ha skrivetilgang.

For C-nivå skal det ikke gis tilgang til opplysningstyper det ikke er behov for tilgang til. Som eksempel på dette kan nevnes at alminnelige formidlere på arbeidsformidlingen ikke nødvendigvis skal ha tilgang til helseopplysninger om attføringsklienter.

Tilsvarende avgrensninger er også gitt for dokumentbaserte og manuelle skjemabaserte registre.

Til § 4-6 Operasjonskontrollmekanismer.

En operasjonskontrollmekanisme er som nevnt foran en innretning for å identifisere og autentisere aktører, slippe autoriserte aktører til og hindre uautoriserte i å slippe til sperrede operasjoner og objekter. Eksempler på OK-mekanismer er vakter, mekaniske og automatiske låser. På nivå A er det stilt krav om at mekanismen ikke på noe enkelt vis skal kunne omgås, endres eller settes ut av drift av uautoriserte. Identifikasjon kan skje gruppevis.

Dette kan f.eks. bety at alle sykepleiere på en avdeling kan benytte samme identifikasjon. For de som er registrert som aktører i følge listen, kan det tillates utført operasjoner som ikke er forbudt etter autorisasjonen. For de som ikke er registrert skal alt være forbudt. På B-nivå skal OK-mekanismen identifisere og autorisere alle aktører individuelt, f.eks. på navn. På nivå C er det stilt krav om logging av både nektet og gitt tilgang.se. Denne bestemmelsen kan i og for seg representere en trussel mot de ansattes personvern, men det må skje en avveining mot sikringshensyn. OK-mekanismen er anbefalt å være slik at de aktuelle operasjoner og ressurser blir sperret for tilgang dersom mekanismen settes ut av drift. Manuelle OK-mekanismer skal tilfredsstille krav i § 4-1. Dette er de krav som er fastsatt for personalet.

Til mekaniske OK-mekanismer er det i § 4-6 (3) stilt krav om at de skal være tilstrekkelig dimensjonert etter de ressurser de skal beskytte.

For automatiske OK-mekanismer er det i § 4-6 (4) på A-nivå stilles det krav om at funksjonsmåten til OK-mekanismen skal være dokumentert og at bare autorisert personale skal kunne sette igang, stoppe, endre og utføre andre lignende operasjoner på OK-mekanismer. På B-nivå er det stilt krav om at bare et lite antall gjentatte forøk på åpning fra en og samme aktør skal kunne godtas før den blokkeres. Det innebærer f.eks. at man lager en sperre dersom det er gjort mer enn 3 eller 5 forsøk på å komme inn med et uriktig passord. Det er videre stilt krav om logging av åpning eller forsøk på åpning av automatisk OK-mekanisme. Denne logg skal inneholde brukeridentifikasjon, tidspunkt og evt. mønster. Mønster er fysisk kjennetegn for en aktør eller nøkler, koder og passord som brukes ved autentisering.

På B-nivået er operasjoner som ikke er tillatt gjenstand for forbud fra OK-systemet.

Til § 4-7 Identifikasjon.

Identifikasjonen består i å fremskaffe identitet for en aktør, et program, en fil mm. Det er stilt krav om at identifikasjonen til aktører skal beskyttes mot uvedkommende og være korrekte og fullstendige før de godtas. Det er relativt vanlig at f.eks. lønnskarnummer eller navn brukes som brukeridentifikasjon, men dette bør unngås på dette nivå. Likeledes så bør man ikke godta deler av identifikasjon som tilstrekkelig identifikasjon. Dersom bruker heter Langfelt, så skal ikke L være tilstrekkelig identifikasjon selv om det i og for seg er entydig. Det skal videre nyttes entydige program- og maskinvareidentiteter for å unngå forvekslinger.

Til § 4-8 Autentisering.

Autentisering innebærer å vurdere om oppgitt identitet er riktig. Mønster er fysiske kjennetegn for en aktør eller nøkler, koder og passord som brukes ved autentisering. Det er stilt krav om et tilstrekkelig antall karakterer i f.eks. passord.

På nivå A er det stilt krav om at det skal fastsettes gyldighetsperiode for mønstre og mønstre skal endres etter at det må antas at det er kjent av andre. Gyldighetsperioden kan variere, men bør ikke være lengre enn 3 måneder. Passord skal bestå av minst 4 tegn. Passord skal også endres dersom personer med kjennskap til det slutter i sitt arbeide.

På B-nivået er det stilt krav om at mønsteret skal lagres envegskryptert. Det innebærer at det ikke skal være mulig å finne fram til innholdet selv om nøkkelen er kjent. Man skal ikke ved kjennskap til kryptert mønster og nøkkel for krypteringsmekanismen finne fram til ukryptert mønster. Mønster skal velges slik at de ikke er enkle å gjette seg til. Man bør ikke velge f.eks. fødselsdato eller andre karakteristika som lett forbindes med vedkommende person.

På C-nivå er det stilt krav om at det krypterte mønsteret varierer fra gang til gang. Passord skal bestå av minst 6 tegn. Arbeidsgruppen overveide å stille krav om flere tegn i passord som for mange ville skape problemer med å huske passordene og føre til nedtegning av disse, med de farer dette skaper. Det er på B-nivå stilt krav om at autentisering av maskinvare ved tvil om autenticitet til en enhet bør være maskinvarestyrt. På C-nivå er det stilt krav om at det bør foreligge en kommando for å kreve at en enhet identifiserer seg for en bruker eller for et program. Når det gjelder krav til autentisering av programmer er det ikke stilt krav på A- og B-nivå. Men et programs identitet bør kunne bekreftes ved en kontroll med at programmet er uendret.

Til kap. 5. FYSISK SIKKERHET.

Til § 5-1 Innbruddssikkerhet.

Bestemmelsen stiller krav til innbruddssikkerhet i bygg, rom og soner, arkiv- og dataskap. Når det gjelder sikring av bygg på A-nivå skal det være mulig å låse eller stenge dører, porter, vinduer, luker mm. forsvarlig. Kravet er relativt vagt og stiller svært beskjedne krav. Nivået må antas å ligge på det som er vanlig sikring av bolig. På B-nivå er det vist til låser godkjent av Forsikrings-selskapenes Godkjennelsesnevnd. Produsenter skal kunne opplyse om krav etter godkjennelsesvilkår er tilfreds-stilt. Det samme gjelder hvorvidt dører på C-nivå tilfredsstiller kravet til Norsk Standard 3159.

Tilsvarende er det under de krav som er stilt til fysisk sikring av rom og soner vist til krav stilt av Forsikringsselskapenes Godkjennelsesnevnd. Produsentene skal kunne opplyse hvorvidt disse vilkår er tilfredsstilt. Det er på nivå C stilt krav om at vinduer skal være fastmonterte, dvs. at de ikke skal være hengslet og ikke skal kunne åpnes. Det er på nivå C stilt krav om at innbruddsalarm skal være montert.

Hva angår arkiv- og dataskap er det på nivå A bare stilt krav om at skapet skal være låsbart. Og det skal selvsagt være låst utenom arbeidstid. På nivå B er det stilt krav om benyttelse av stålskap eller skap av tilsvarende styrke, og på nivå C er det stilt krav om at skapet skal være dirksikkert og ikke lett kunne fjernes. Det innebærer at det enten må være fastmontert eller at skapet skal ha en vekt eller størrelse som vanskeliggjør fjerning. Dersom annet enn nøkkel nyttes for å åpne skapet, skal det være slik konstruert at synlige spor viser innbruddsforsøket.

Til § 5-2 Sikkerhet mot brann- og vannskader.

Bestemmelsen fastsetter krav til brannsikring i rom og soner og av arkiv- og dataskap. Det er i bestemmelsen henvist til Norsk Standard og Nordtest standard. Nordtest er et organ under Nordisk Råd som arbeider for å etablere felles nordiske standardprøvningsmetoder for å redusere handelshindringer i Norden. Nordtest NT Fire 017 er en slik prøvningsmetode for arkiv- og dataskap. Produsenter og leverandører skal kunne opplyse hvorvidt kravene er tilfredsstilt.

Til § 5-3 Krav til fuktighet, temperatur og luftrenhet i rom og til sikring av strøm-, vanntilførsel og teletjenester.

Bestemmelsen kan sees som en påminnelse om de toleransegrenser som leverandører har fastsatt for utstyret. På nivå B er det lagt opp til at man bør vurdere sikkerhetstiltak for å unngå avbrudd i strøm-, vannforsyning og teletjenester. Det er altså ikke stilt spesifikke krav til slike tiltak her.

Til § 5-4 Fysisk adgangskontroll.

Bestemmelsen stiller generelle krav til fysisk adgangskontroll og særlige krav til slik kontroll til bygninger og lokaler. Bestemmelsen må ses i sammenheng med § 4-1 om operasjonssystem og § 5-1 om fysiske sperrer mot inntrenging. Det kan godt være flere adgangskontrollsystemer en person må passere for å kunne foreta en bestemt operasjon. Sikkerheten vil derfor være minst like høy som nivået på det beste adgangskontrolltiltaket. Det skal foretas separate sikkerhetsvurderinger hva angår utenforstående, for de ansatte (eller lignende) som ikke skal ha adgang til registeret, og for slike som skal ha

adgang. Rimeligvis vil de sterkeste tiltakene måtte settes inn mot utenforstående. Det er i § 5-4, nr. 2 for nivå A stilt krav om at det skal føres tilsyn med alle åpne innganger og adkomstveier til lokalene. Dette kan skje ved at personalet direkte har utsyn til disse områdene eller f.eks. via monitor. Det skal være en resepsjon som tar imot og henviser besøkende. For midlere sensitivitet og for svært sensitive opplysninger skal besøksliste føres og besøk skal hentes i resepsjonen. I større miljøer bør ID-kort brukes og bæres synlig og besøkende bør tildeles egne kort og ledsages av ansatte. Regelen om ID-kort og besøkskort og ledsaging av ansatte er å anse som anbefalinger.

Til § 5-5 Sikring av registerets tilgjengelighet.

Det er i forskriftsutkastet lagt opp til at forskriftene ikke bare skal dekke tiltak mot kompromittering av opplysninger, men også sikre tilgjengelighet og data-kvalitet. Paragraf 5-5 stiller krav om sikkerhetskopiering av registre (back-up). Bestemmelsen må ses i sammenheng med §§ 5-2 og 5-4, om sikkerhet mot brann og vannskader og fysisk adgangskontroll. Hvis et vanlig manuelt arkiv er særlig sensitivt mot manglende tilgjengelighet må det overveies sikkerhetskopiert f.eks. ved mikrofilming. Kravet er bare stilt der hvor særlig store problemer vil voldes for den enkelte om opplysninger blir borte.

Til kap. 6. TILGANGSKONTROLL.

Til § 6-1 Fastsettelse av sikkerhetsnivå for tilgangskontrollsystemer.

Bestemmelsen gjelder elektronisk tilgang til opplysninger, i motsetning til kap. 5 som gjelder fysisk adgang. Tilgangskontrollsystem er i denne sammenheng definert som en type operasjonskontrollsystem som kan regulere aktørers tilgang til EDB-ressurser som nettverk, datamaskiner, periferutstyr, maskinlesbare data og programmer mm. Det generelle kapitlet om operasjonskontrollsystemer kommer inn også her, og sikkerhetsnivået bestemmes etter § 4-1. Bestemmelsen er knyttet til § 6-2 nedenfor ved at de krav som er stilt etter denne også må tilfredsstilles. Tilsvarende som for fysisk adgangskontroll vil sikkerheten være minst like høy som den sterkeste tilgangskontroll en inntrenger må passere. Det kan være flere tilgangskontrollkontrollsystemer utenpå hverandre, evt. kombinert med fysiske adgangskontrollsystemer. Det er stilt krav om at de enkelte tilgangskontrollsystemene skal være under den registeransvarliges kontroll. Dette må imidlertid ses sammen med § 2-1, 2. ledd, som åpner adgang til å delegerer deler av kontrollen med sikkerheten.

Det skal foretas vurdering av sikkerheten overfor de samme grupper som fastsatt for fysisk adgangskontroll.

Til § 6-2 Tilknytningssikkerhet.

Bestemmelsen regulerer sikkerheten ved tilknytning av terminal eller datamaskin til en datamaskin eller et nettverk. Tilknytningssikkerheten for en enhet vil svare til den laveste for noen av de innganger som gir mulighet til operasjoner i enheten. Det er stilt krav til tilknytningssikkerhet på A, B og C-nivå. Ved A-nivå kan åpen tilknytning benyttes. Dette innebærer at det ikke kontrolleres hvor forespørsel om tilknytning kommer fra. Eksempler på åpen tilknytning er tilknytning via oppringt linje eller åpent nett.

På B-nivå kan åpen tilknytning nyttes hvis det med svært høy sikkerhet kan begrenses hvilke data og brukerområder, eller programmer det kan oppnås tilgang til. Det stiller krav til mulighet for å autorisere pr. inngang. Såkalt logisk lukket tilknytning kan benytte, dvs. anropende enhet må kunne identifiseres ved terminal-, linje-, telefon-, maskinnummer e.l. Om tilknytning begrenses ved tilbakeringing, lukket brukergruppe, terminalidentifikasjon e.l. vil det kunne betraktes som en logisk lukking.

På C-nivå er det gitt adgang til å benytte fast tilknytning, dvs. fast linje. Logisk lukking kan brukes dersom endring av lukkingen bare kan finne sted fra lokaler den registeransvarlige har fysisk adgangskontroll til på sikkerhetsnivå C. Dette er et eksempel på at god fysisk adgangskontroll kan kompensere noe svakere elektronisk tilgangskontroll. Bestemmelsen tar sikte på å hindre snokere i å manipulere listen over de som kan knytte seg til. Manuell tilknytning kan også nyttes om den som utfører tilknytningen gjenkjenner enhver som har tillatelse til å bli tilknyttet. En ytterligere begrensnings finnes i § 7-3, siste ledd.

Til del 4. SPESIELLE KRAV TIL EDB-UTSTYR OG BRUK AV EDB-UTSTYR.

For å lette tilgjengeligheten til forskriftene har en valgt å skille ut det som er spesifikt knyttet til EDB i en egen del.

Til kap. 7. NETTVERKS- OG KOMMUNIKASJONSSIKKERHET.

Kapitlet gir de regler som kommer til anvendelse dersom opplysninger lagres eller behandles i et nettverk. Det får ikke anvendelse for dem som har en frittstående datamaskin.

Til § 7-1. Kontroll med tilgang i nettverk.

Et nettverk er en samling datamaskiner og periferenheter som er knyttet sammen ved hjelp av kommunikasjonsutstyr for å utveksle data. Bestemmelsen fastsetter at ikke-sensitive eller mindre sensitive registre kan lagres i en åpen del av et nett. En enhet tilhører en åpen del av et nett om en åpent tilknyttet terminal kan få tilgang til den. Tilsvarende tilhører enheten en lukket del om bare lukket tilknyttede terminaler kan få tilgang. Sensitive registre kan lagres i lukket del av nett. Særlig sensitive registre kan lagres i såkalt fysisk lukket nett hvis den fysiske adgangskontrollen er god.

Til § 7-2 Lokalnett og andre nettverk av selvstendige EDB-erheter.

Bestemmelsen stiller krav til et nettverks operativsystem og kommunikasjonsgrensesnitt-enhet. Dette er en "boks" med maskin- og programvare som gjør en type EDB-utstyr i stand til å kommunisere med annet EDB-utstyr via en kommunikasjonskanal. Motivet er å gi sikkerhet for at enheten ikke misbrukes til lesing eller endring av data. Reglene for operativsystem i § 11-1 skal tilfredsstilles. Kravene til fysisk adgangskontroll og tilgangskontroll til en kommunikasjonsgrensesnittenhet må innrettes etter det mest sensitive register som skal kunne behandles i nettverket.

Dette kan medføre bl.a. at enkelte svært sensitive registre bør føres ved hjelp av en frittstående datamaskin, fordi sikringstiltakene kan bli for dyre ved sikring av nettverket.

Til § 7-3 Sikkerhet ved overføring av opplysninger.

Bestemmelsen stiller krav til sender om overføring av opplysninger der sender er initiativtaker til overføringen. Bestemmelsen tar sikte på å hindre tilgang for uvedkommende. Det skal bringes på det rene om mottaker har tillatelse til å motta opplysningene og hvorvidt det foreligger adgang til å utlevere opplysninger. Det stilles også krav til loggføring av utlevering og mottak av opplysninger. Det er videre stilt krav om kryptert overføring når det er særlig kompromitteringssensitive opplysninger som overføres eller hvor kompromitteringssensitive opplysninger skal overføres i stort omfang. Bestemmelsen tar sikte på å hindre tilgang for uvedkommende.

Til § 7-4 Distribuerte datamaskinsystemer.

Et transparent distribuert datamaskinsystem er et system av sammenkoblede datamaskiner og periferenheter som framstår for brukerne som ett datamaskinanlegg. Data kan derfor bli lagret hvor som helst i systemet. Brukeren har ikke kontroll med hvor i systemet data blir bearbeidet eller lagret, og det må derfor stilles samme krav til alle deler av systemet.

Til kap. 8. Sikkerhet for datamaskiner.

Kapitlet får anvendelse for alle datamaskiner som skal behandle registre. Presiseringen kan synes unødvendig siden forskriftene gjelder personopplysninger og personregistre, men er inntatt for å markere at den ikke gjelder datamaskiner som f.eks. ligger i nettverk og hvor den aktuelle datamaskin ikke skal behandle registre.

Til § 8-1 Sikkerhet for datamaskiner.

Bestemmelsen stiller krav til operativsystemsikkerhet og maskinwaresikkerhet for flerbrukermaskiner, og er knyttet opp til kapitlene 11 og 13. Videre er det stilt krav til fysisk adgangskontroll, tilgangskontroll og krav til adgangskontroll til maskinrom. Hvis et register er mindre sensitivt, kan fysisk adgangskontroll på nivå A medføre at kravene til tilgangskontroll etter § 6-1 kan sløyfes. For å oppnå tilstrekkelig sikkerhet for tilgjengelighet skal maskinen sikres etter § 5-2 (1) Sikkerhet mot brann- og vannskader.

Til kap. 9. SIKKERHET FOR LAGRINGSMEDIA OG PERIFERUTSTYR.

Kapitlet gjelder krav til sikkerhet for lagringsmedia og periferutstyr som brukes til lagring, lesing eller skriving av opplysninger. Lagringsmedia omfatter også papir og andre ikke maskinlesbare media.

Til § 9-1 Sikkerhet for lagringsmedia.

Bestemmelsen fastsetter krav til sikkerhet for lagringsmedia i lokaler og ved transport. Det er verdt å merke seg at bestemmelsen også gjelder manuelle lagringsmedia, se § 2-3.

Til § 9-2 Sikkerhet for datamaskiners periferutstyr.

Bestemmelsen fastsetter krav til fysisk adgangskontroll til periferutstyr som brukes til å lagre, lese eller skrive opplysninger. Bestemmelsen gjelder eksternlagerenheter og terminaler. Periferutstyr er eksternlagerenheter, lesere, skrivere og terminaler. Eksternlager er en lagerenhet ved en datamaskin som bare er tilgjengelig gjennom kanal for innmating og utmating. § 9-2, nr. 1, 3. ledd er et unntak fra krav til tilknytningssikkerhet i § 6-2.

Til kap. 10. SIKKERHET I PROGRAMMER.

Til § 10-1 Sikkerhet i programmer som skal behandle registre.

Bestemmelsen stiller krav til utvikling, godkjenning, innlegging og klargjøring av programmer for drift. Det er også stilt krav til tilgangskontroll til programmer, og til at testing og feilsøking i størst mulig grad bør skje uavhengig av registre. Dette har bl.a. betydning for tilgjengelighet til data. Det kan være en risiko for ødeleggelse av og kompromittering av reelle data.

Til § 10-2 Sikkerhet i systemprogrammer.

Bestemmelsen stiller krav til sikring mot endring i kompilatorer, interpretere, lenkeredigerer og laste-moduler og programmer som skal bidra med tilgangskontroll på nivå B eller C.

Kap. 11. OPERATIVSYSTEMSIKKERHET

Et operativsystem er et system av manuelle og automatiske rutiner for administrasjonen av et datamaskinanlegg.

Det vil være nødvendig for registereier å kontakte leverandør for å få vite hvorvidt operativsystemet tilfredsstiller de krav som er stilt i denne forskrift.

Til § 11-1. Operativsystemer.

Operativsystemet skal sørge for tilgangskontroll etter de krav som er stilt i § 6-1.

På nivå A er det stilt krav om at operativsystemet skal ha kontroll med tildeling av ressurser, så som f.eks. magnetbåndstasjon til ulike aktører, tilgang til lagerområder og operativsystemfunksjoner som lesing, skriving og sletting i lagre. Det skal også kunne ha kontrollen med skifte mellom modi for utførelse, dvs. kontrollen med det privilegienivå et program kan utføre under.

På nivå B er det stilt krav om at det bare skal være mulig å få direkte tilgang til operativsystemets lagerområder for administrasjon av ressurser gjennom operativsystemet. For spesielt autorisert personale kan direkte tilgang gis ved feilsøking og retting. Andre brukere og programmer skal bare kunne ha tilgang gjennom operativsystemet. Det skal heller ikke være mulig for et program å referere utenfor sitt eget lagerområde. Det skal være mulig å autorisere en brukers tilgang til de ulike operativsystemfunksjoner. Det skal foretas logging av mislykkete forsøk på tilgang til filer og operativsystemfunksjoner. Det er videre stilt krav om opprettelse av sikkerhetslogg med logging av viktige hendelser vedrørende bruk av operativsystemet.

På nivå C skal operativsystemet ha verktøy for å kunne analysere sikkerhetsloggen. Systemfeil, uforutsette og planlagte stans skal håndteres på en slik måte av systemet at sikkerheten opprettholdes, slik at det ikke skal være åpent for inntrenger selv om det oppstår feil i systemet.

Til § 11-2 Krav til filsystemer i flerbrukermiljø.

Et filsystem er et programsystem for organisering og katalogisering av filer på eksternlager og for regulering av tilgang til filer. En fil er en navngitt samling data som består av et varierende antall poster av en bestemt posttype. Det er på nivå B stilt krav om at filsystemet skal kontrollere at det logiske lagerområde til en fil ligger innenfor eierens logiske lagerområde. Kravet er stilt for å sikre dataenes integritet og å hindre uvedkommende tilgang.

På nivå C er det stilt krav om at filsystemet skal foreta en fysisk sletting av opplysninger i frigitte lager-områder. Dette innebærer at når en aktør sletter opplysninger så skal ikke området bare frigis for senere registrering, men det skal automatisk foretas en fysisk sletting av dataene.

Til § 11-3 Brukerlagete operativsystemrutiner.

Bestemmelsen gjelder operativsystemrutiner som ikke er installert av leverandør før leveranse, men som er iverksatt ved den aktuelle EDB-installasjon. De spesielle kravene som er stilt til brukerlagete operativsystemrutiner er laget for at ikke slike systemer skal svekke den sikkerhet som det opprinnelige operativsystem har. Det er bare på nivå C at det er stilt spesifikke krav. Slike brukerlagete operativsystemrutiner må godkjennes av vedkommende sikkerhetsansvarlig før de iverksettes.

Det skal ikke være mulig for brukerlagete operativsystemrutiner å endre modus for utførelse for kallende program eller endre programmets autorisasjoner. Det skal heller ikke overlate kontroll til rutiner man ikke kjenner sikkerheten til unntatt det kallende programmet. Bestemmelsen er inntatt for å redusere muligheten til å svekke sikkerhetssystemene.

Kap. 12. Databasesikkerhet.

Kapitlet får bare anvendelse for registre som er etablert som database og for registre som er en del av en database. En database er en samling filer som er tilgjengelig via et eget programsystem kalt database-administrasjonssystem (DBAS).

Til § 12-1 Administrasjon og tilgangskontroll.

Kravene til sikkerhet i systemprogrammer som nevnt i § 10-2 skal være fulgt hva angår kontroll med tilgang til database administrasjonssystemet.

En brukers buffere skal bare være tilgjengelig for brukeren via DBAS. Denne bestemmelsen er inntatt fordi en bruker ikke nødvendigvis har tilgang til alle data-elementer i buffer. Buffer er et lagerområde for mellom-lagring av data ved kommunikasjon med eksterne lager, terminaler og datamaskiner mm.

På nivå C er det stilt krav om at DBAS må kunne begrense tilgang til bestemte felttyper i en fil. Dette innebærer at det skal være mulig å sørge for at ulike brukere av opplysninger skal kunne få tilgang til ulike delmengder av opplysningene. Det skal også være mulig å begrense tilgang til postforekomster avhengig av verdier for felter. F.eks. slik at man bare skal kunne søke på inntekter over et bestemt beløp.

Til § 12-2 Databaseintegritet og tilgjengelighet.

Databaseintegritet er graden av samsvar mellom det som er representert i databasen og det som skal representeres. På nivå B er det stilt krav om at DBAS skal sørge for entydig identifikasjon av poster. For relasjonsdatabase-systemer bør det sørges for at et hvert referansefelt i en post enten refererer en eksisterende post eller til ingen post (dvs. at det ikke finnes noen aktuell post å referere til).

På nivå C er det stilt visse krav til datadefinisjonsspråket. I et slikt språk defineres posttyper, sammenhenger mellom posttyper og indekser, nøkler osv. Databasedefinisjonsspråket bør ha muligheter for spesifisering av integritetsrestriksjoner på og mellom felter som ikke nødvendigvis er i samme post. Integritetsrestriksjonen kan f.eks. være rimelighetskontroller, prøver på om en verdi er større enn en annen. Formatrestriksjoner, domene- og verdirestriksjoner bør kunne gis. Dette er restriksjoner hva angår utforming, områder og verdi. Det siste kan f.eks. være at det skal være oddetall i fødselsnummer på menn og partall på kvinner. Videre skal det være mulig å beskrive prosedyrer for håndtering av unntakssituasjoner. Endelig bør databaseadministrasjonssystemet ha mulighet for forsøksvis oppdatering.

Kap. 13. MASKINVARESIKKERHET.

Til § 13-1 Generelt.

Maskinvaren skal være slik laget at det er god sikkerhet mot uautoriserte endringer i forhold til spesifikasjonene. Formålet er å unngå at sikkerheten svekkes gjennom endringer av maskinvaren. Videre skal maskinvaren være godt dokumentert og sikkert identifisert. Den skal tilfredsstille leverandørens dokumenterte testkrav.

Til § 13-2 Sikkerhet i datamaskiners maskinvare.

På nivå B er det stilt krav om at maskinvaren skal kunne sperre programmer mot å skrive, lese og utføre i ulike deler av internlager og det skal være kontroll med tilgangen til maskininstruksjoner som påvirker sikkerheten. Det skal ikke være direkte tilgang for program i brukermodus til maskininstruksjoner for å lese fra eller skrive til eksternt lager eller kommunikasjon. Det skal være avbruddsrutiner som kontrollerer system- og operatørfeil. Maskinvaren skal ha kjente reaksjoner på alle instruksjoner med alle mulige operander og koder mv. Operand er den ressurs det blir operert på.

På C-nivå er det stilt krav om at det skal finne sted en feilkontroll ved henting av instruksjoner og operander for utførelse av operasjoner.

Kap. 14. DRIFTSSIKKERHET

Til § 14-1 Generelt.

På nivå A er det stilt krav til tilretteleggelse av data-behandlingen. Trusler skal søkes avdekket og avverget så effektivt som mulig. Det bør være etablert rutiner for rapportering av trusler, f.eks. til sikkerhetsansvarlig, og det bør være dokumentasjon av denne.

På nivå B skal det i tillegg jevnlig kontrolleres at deler som har betydning for sikkerheten virker som forutsatt.

Til § 14-2 Service og vedlikehold.

På nivå A er det stilt krav om at endringer skal registreres og bare kunne foretas av de som er autorisert til å foreta endringene. Dette er for å lette feilsøking og begrense faren for forvanskninger og tap av data. Videre kan det lettere finnes fram til den som er ansvarlig for handlingen.

På nivå B skal i tillegg de som skal foreta feilsøking mot registret ha undertegnet taushetserklæring. Dette er en taushetserklæring som er utarbeidet av Datatilsynet. Der hvor det nyttes fjerndiagnose, dvs. feilsøking via linje utenfra, skal tilknytning skje manuelt. Det skal også foretas en registrering av foretatt fjerndiagnose. Videre skal de kopier som måtte oppstå i forbindelse med feilsøking sikres på lik linje med de originale registre.

Til § 14-3 Drift av datamaskiner.

På nivå B er det stilt krav om retningslinjer for å opprette, autorisere, kontrollere og fjerne brukere i en datamaskin. Videre behandles krav til ansvar for rutiner og hvem som skal kunne utføre de. Dersom det er mulig å låse maskiner, så skal de være låst unntatt ved oppstartning og stopping. Før et register etableres som en database, samling av filer e.l., skal dette være godkjent av registeransvarlig. Det kan i tillegg tenkes at Datatilsynets samtykke må være innhentet dersom samlingen er i strid med vilkår i forskrifter for registret eller konsesjon.

Til § 14-4 Sikkerhetskopiering.

Bestemmelsen stiller krav for nivåene A, B og C hva angår sikkerhetskopiering av register og registreringer. Bestemmelsen tar primært sikte på å sikre tilgjengelighet til data.

Til § 14-5 Registrering og etterbehandling.

Det er stilt krav om at det skal være fysisk adgangskontroll til de lokaler hvor registrering mv. finner sted. Sikkerhetsnivået i § 5-4 blir som vanlig bestemt av sensitiviteten av opplysningene. Det er stilt krav om at sensitive opplysninger skal oppbevares innelåst etter arbeidstid. Dette er krav som allerede i dag f.eks. er stilt til oppbevaring av dokumenter på sosialkontor.

Til § 14-6 Makulering og sletting.

Bestemmelsen tar sikte på å sikre at riktige medier blir slettet og at det foreligger tillatelse til makulering. Dette bidrar til å sikre tilgjengelighet. Krav til foretak som utfører oppdrag for andre, i § 3-1 gjelder ved transport og oppbevaring.

På nivå B er det stilt krav om at materialet ikke skal være rekonstruerbart etter makulering. Dette stiller krav til tilstrekkelig brenning eller finhet i makulatur. Når det gjelder datamedia er det krav til tilstrekkelig grundig sletting, f.eks. ved gjentatt overskriving med 1 og 0.

På nivå C er det i tillegg stilt krav om at en representant for registeransvarlig eller evt. databehandlingsforetak e.l. skal følge med og kontrollere at makulering blir foretatt på riktig måte.

Del 5. SPESIELLE KRAV TIL REGISTERKVALITET

Kap. 15 Registerkvalitet mm.

Kapitlet inneholder spesielle krav til registerkvalitet, men flere av de andre reglene i forskriftene gir også bidrag til å sikre kvaliteten. Sikkerhetsnivået bestemmes av sensitivitetsgraden for datakvalitet for hver enkelt type opplysning i registeret, for alle opplysningstypene samlet og for hele registret.

Til § 15-1 Generelle krav til opplysnings- og registerkvalitet.

På nivå A er det stilt krav om at registret må være utformet slik at dataelementene er velegnet til uttrykke de relevante opplysninger. Formater og koder skal være slik at opplysningene enkelt lar seg beskrive.

På nivå B skal det i tillegg foreligge dokumentasjon av vilkårene for at poster og opplysninger skal forekomme i registret, og rutinene skal være tilrettelagt slik at registret til enhver tid er fullstendig. Dersom registret bare nyttes med visse mellomrom er det tilstrekkelig at det er oppdatert før ny bruk.

På nivå C er kravene skjerpet slik at det skal foreligge informasjons-, meldings- eller kontrollrutiner slik at registret er fullstendig og uten irrelevante opplysninger. Relevansen kan variere fra person til person. Det skal videre innføres gyldighetsperiode for opplysninger som varierer over tid, for å sikre at de til enhver tid blir holdt ajour.

Til § 15-2 Datainnsamling, koding, registrering og kontroll.

Der det er aktuelt skal det angis hvilken nøyaktighetsgrad og presisjonsgrad opplysningstypene har.

Det er ikke tilstrekkelig at man kontrollerer om opplysningene er korrekte i forhold til grunnlagsmaterialet ved registrering, det må også stilles krav til selve tilblivelsen av opplysningene. De måle-, observasjons- og andre innsamlingsmetoder som nyttes må være gode nok til å skaffe tilveie et godt datagrunnlag. Dette må sees i forhold til det formål de skal brukes til. Det er fra et personvernssynspunkt gjerne viktigere at opplysningene har en god kvalitet i administrative registre enn i forskningsregistre.

I tillegg til disse generelle kravene til innsamling mv. er det stilt krav for nivåene A, B og C. På nivå C er det stilt krav om at de registrerte bør tilbys mulighet til å kontrollere opplysningene etter registrering såfremt det foreligger innsynsrett i registret. Innsynsretten er regulert av personregisterlovens § 7, og forskriftene til denne, kap. 1. Enkelte registre kan være unntatt fra innsynsretten.

Til § 15-3 Tolkning av opplysninger.

Det er for nivå B stilt krav om at brukeren av opplysningene skal gis opplæring i tolkning av opplysningstypene og i bruk av det utstyr og informasjon som trengs for tolkningen.

Til § 15-4 Søking.

Bestemmelsen stiller krav til opplæring i utforming av søkekriterier mv. På nivå B er det stilt krav om tilstrekkelig identifikasjon av de personer det søkes opplysninger om, og på nivå C bør det i tillegg forsikres at søk gir fullstendige og relevante resultater. Dette for å unngå at informasjoner ikke blir fremhentet.

Til § 15-5 Dataoverføring.

Det er her bare stilt krav for nivå C. Dersom opplysningene skal overføres i telenett, åpent nettverk eller andre åpne transmisjonsmåter så skal opplysningene forsegles forsvarlig. Forsegling vil si påføring av segl eller kontrollsiffer bl.a. for å hindre uvedkommende i å manipulere data uoppdaget. Videre skal både mottaker og sender loggføre sending og mottaker skal kvittere for godkjent mottak til avsender.

Til § 15-6 Endring og sletting.

På nivå A er det stilt krav om at opplysninger skal slettes i henhold til fastsatte slettefrister. Dette kan være eksplisitte slettefrister i konsesjoner, men også de generelle slettingsregler i personregisterlovens § 8 kan her komme inn.

På nivå B er det stilt krav om at opplysninger som kan antas å være foreldet eller uriktig skal innhentes på nytt før opplysninger fra registret brukes til å fatte beslutning. Der hvor opplysninger ikke lenger skal være i registret skal den fjernes eller merkes som ugyldig. Alle endringer skal logges med angivelse av situasjonen før og etter endring, hvem som foretok denne og tidspunktet. Det kan i visse tilfeller være aktuelt å kreve sletting av situasjonen før endringen, se også personregisterlovens § 8.

Til § 15-7 Dokumentasjon av register.

På nivå A skal det foreligge dokumentasjon for formål med registret, beskrivelse av opplysningstypene, sammenhenger mellom opplysningstyper, vilkår for at poster og opplysninger skal foreligge samt kodeskjema som skal nyttes.

På B-nivå er det stilt krav om at det skal fremgå hvilken aktør som har forestått registreringen mv. Det bør også registreres fra hvilket tidspunkt en opplysning gjøres tilgjengelig. Dette kan f.eks. ha betydning i forbindelse med kredittopplysningsvirksomhet.

Til § 15-8 Utskrifter.

På nivå A er det stilt krav til at utskrifter til den registrerte bør være enkle å forstå og kontrollere riktigheten av. Om nødvendig skal det legges ved informasjon eller henvises til informasjonstjeneste. Dette for at de registrerte på en meningsfylt måte skal kunne utøve sin rett til innsyn og kunne ha oversikt over hvilke registreringer som foretas og hva opplysninger brukes til.

På B-nivå skal det i tillegg etter egne retningslinjer foretas kontroller f.eks. ved stikkprøver.

Til § 15-9 Resultatkontroll.

Det er på nivå B stilt krav om at man rutinemessig skal foreta resultatkontroll, noe som kan skje ved rimelighetskontroll. Slik kontroll vil gjerne bli utført manuelt.

11. Administrative og økonomiske konsekvenser av forskriften

Økonomiske og administrative konsekvenser er drøftet for registreiere, Justisdepartementet og Datatilsynet.

Kostnadene er inndelt i fire kategorier: investeringer, driftskostnader, tilpasningskostnader og effektivitetstap.

Når det gjelder tilpasning og effektivitetstap har det vist seg svært vanskelig å kvantifisere kostnadene. Disse kostnader inngår ikke i de overslag som er gjort. Tilpasninger kan imidlertid antas å bli en betydelig kostnad. Særlig gjelder dette kostnader ved endring av databaser og programmer og ettersikring mot brann.

Med hensyn til effektivitetstap er det tiltak i forbindelse med sikring av datakvalitet som er viktigst. Her er det antatt at kontrollordninger kan redusere effektiviteten fram til data er registrert med så mye som opptil 20-30%. Likedan vil krav til kryptering redusere overføringshastigheter med opp mot 40%.

Kostnader for registreiere er anslått for 5 hovedtyper behandlingsmiljøer: manuelt, enbrukermaskin, minimaskin (1-16 terminaler tilknyttet), mellomstor maskin (17-128 terminaler) og stormaskin (mer enn 129 terminaler). Det er for sikkerhetsnivåene A, B og C anslått en kostnad som følger av forskriften utover et antatt minimums-nivå. Det er antatt at registreier allerede har gjennomført tiltak for 4/5-del av kostnaden, slik at bare 1/5 av kostnaden følger av forskriften. Det er gjort antakelser om hvilket sikkerhetsnivå behandlingsmiljøene må klareres for.

Resultatene av utvalgets anslag kan presenteres i følgende tabell:

	A	B	C	
Manuelle registre	70 000	35 000	17 500	
Kostnad	40.0 Mkr	52.5 Mkr	4.6 Mkr	97.1 Mkr
Enbrukermaskiner	5 160	2 580	860	
Kostnad	11.9 Mkr	24.8 Mkr	20.6 Mkr	57.3 Mkr
Minimaskiner	11 200	3 200	1 600	
Kostnad	25.8 Mkr	47.7 Mkr	42.7 Mkr	116.2 Mkr
Midimaskiner	1 260	360	180	
Kostnad	11.6 Mkr	19.0 Mkr	14.3 Mkr	44.9 Mkr
Stormaskiner	6	96	18	
Kostnad	0.3 Mkr	16.2 Mkr	9.0 Mkr	25.5 Mkr
Total sum				341.0 Mkr

Det er meget stor usikkerhet forbundet med de foreliggende anslag og antakelser. Særlig gjelder dette antallet registre, typiske kostnader for sikring av ulike behandlingsmiljøer, hvor stor andel av datamaskinene som fører personregistre og fordeling av sikkerhetsbehov for maskinene. Likedan har forenkende antakelser introdusert betydelig usikkerhet. F eks er sensitivitetsgradene satt like for et register. En har ikke tatt med nettverkssikkerheten i anslaget.

Anslaget på ca 300 - 500 millioner kroner i investeringer er regnet ut fra dagens priser.

Et anslag mellom 300 og 500 millioner kroner synes som et rimelig anslag for de totale investeringskostnader som følger av forskriften. Dette svarer til ca 1 250 kroner pr register eller ca kr. 5 000 pr registreier i gjennomsnitt.

Driftskostnadene som følger av forskriften er anslått til ca 50 millioner kroner årlig. Det er to hovedkilder til dette beløp: fysisk sikring og kvalitetskontroll med de registrerte opplysninger.

Investeringskostnadene kan virke noe høye i forhold til de ca. 1 mrd. kroner som man antar årlig investeres i fysiske sikringstiltak i Norge.

Nå vil sikringstiltakene etter utkastet ikke bare sikre personregistre, men også andre verdier som registreier oppbevarer og bruker i nærheten av personregistrene. Ved gjennomføring av tiltak i medhold av denne forskrift vil registreierne få reduserte utgifter til sikkerhetstiltak som er begrunnet i andre hensyn.

Slike hensyn kan være industrimessige hensyn, behov for å redusere samfunnets sårbarhet, militære hensyn, m fl. Her vil investeringene i forbindelse med sikring ut fra personvernperspektiv delvis dekke tiltaksbehov ut fra andre perspektiver.

Såtidig må det nevnes at en eventuell forskrift i tråd med utkastet vil kunne tillate løsninger som nå ikke er tillatt, og dermed være økonomisk besparende. Dette kan skje ved å dele datamaskiner, overføringer over telenettet, nettverksintegrering av maskiner, m.m. Følgelig kan investeringer i sikkerhetstiltak redusere investerings- og driftskostnader for EDB-utstyr forøvrig. På lengre sikt er det sannsynlig at innsparingene vil være større enn investeringene, gitt det "samme" krav til sikkerhet. Eller med andre ord: Den langsiktige totalkostnad som følger av forskriften antas å være lavere enn de innsparinger som følger ved at nye ordninger vil kunne tillates. Forskriften antas derfor også å være "samfunnsøkonomisk lønnsom".

De vesentligste kostnader for Datatilsynet vil være forbundet med sensitivitetsinnplassering av registre etter forskriften. Her må det skilles mellom registre som allerede har konsesjon, §41-registre og forskriftsunntatte registre. Ytterligere er det nødvendig å skille mellom allerede opprettede registre og de som ikke er opprettet.

Innplassering av de forskriftsunntatte registre er et engangsarbeide, der sensitivitetsgradene oppgis i de generelle forskrifter i tilknytning til hver enkelt registretype. Dette vil legge beslag på lite ressurser.

For de andre to registerkategorier må en foreta en innplassering for et meget stort antall typer registre. Antallet typer er anslått til ca 2000.

Det er vanlig å operere med et antall opplysningstyper i registerkonsesjoner som sjelden overstiger 50. Det burde derfor etter noen tid være mulig å foreta en innplassering av 4-5 register pr dag pr. ansatt. Oppgaven kan derfor anslås til i størrelsesorden ett årsverk pr. 1000 registre, noe som skulle svare til 2 årsverk for dette arbeid i Datatilsynet. 1 årsverk regnes i tillegg på kontorsiden.

Det må ellers antas at Datatilsynet vil få en rekke henvendelser fra registeransvarlige m.m. som ønsker presiseringer eller tolkninger av forskriften. Denne belastning må antas å nå en topp rundt ikrafttredelsesdato og forøvrig i forbindelse med saker som er aktuelle i media. Det er selvsagt vanskelig å anslå omfanget av slike forespørsler. Denne aktivitet antas å kreve 1/2 stilling.

Forskriften vil nok lede til en omfattende etterspørsel etter foredrag fra Datatilsynet. Dette er en type oppdrag som Datatilsynet normalt stiller seg velvillig til, og som ventelig vil legge beslag på en del av Tilsynets ressurser de første par årene. Det regnes med 1/4 stilling til dette.

I tillegg til sensitivitetsinnplassering og informasjon, må man regne med at Datatilsynet vil få et antall dispensasjonssøknader. Det er vanskelig å si noe om omfang og art. Det vil ikke overraske om en hovedtyngde kommer til å dreie seg om dispensasjon for gamle systemer, der planer foreligger for å ta i bruk nye. 1/4 stilling er regnet for denne funksjon.

Det vil også bli nødvendig å utforme nye søknads-blanketter for konsesjonsppliktige registre. Dette er ikke særlig fordyrende, siden dette under alle omstendigheter står for tur.

Gruppen har ikke foreslått at Datatilsynet skal godkjenne utstyr m.m. til bruk i behandling av personregistre også av økonomiske og administrative grunner. I stedet foreslår utvalget at leverandører m.m. gjør egne vurderinger i forhold til forskriften og

oversender disse til Datatilsynet. Selv om Datatilsynet etter forslaget ikke skal godkjenne utstyr, bør man opprette et eget arkiv for dokumentasjonen og vurderingene, og ta sikte på å gå gjennom hver enkelt sak i detalj, slik at ikke produkter i markedet sikkerhetsvurderes for høyt av produsentene. En stilling trengs for å betjene denne oppgave.

I forbindelse med fastsettelse av sensitivitetsgrader vil det være nødvendig å sende ca 20 000 skriftlige meldinger til registreiere. Datatilsynet vil få tilleggsutgifter til porto på ca 100 000 kr. Det vil også bli nødvendig å rykke inn annonser og formidle informasjon på annen måte, slik at ca 100 000 kr. ekstra bør bevilges til informasjon i forbindelse med innplasseringen.

Det kan være ønskelig å utgi forenklede retningslinjer for enkelte typer forskriftsunntatte registre som pasientregistre, advokatregistre, mfl. Dette vil være mulig der behandlingsmiljøene rundt registrene er likeartede. Og det kan være ønskelig siden forskriften er relativt komplisert i sin oppbygning. Et arbeid med forenklede regler bør evt. finne sted i samarbeid med bransjeorganisasjonene. Det må antas å ville legge beslag på betydelige ressurser (1/2 stilling).

Når så mange arbeidskrevende momenter er nevnt, bør det også nevnes et tilfelle hvor forskriften må antas å bli arbeidsbesparende. Det er ved sikkerhetskontroller. Pr i dag er dette en omfattende oppgave, siden en ofte mangler krav/kriterier å kontrollere mot. En forsvarlig gjennomført kontroll stiller i dag store krav til forberedelser, der både sensitivitetsvurderinger og vurdering av sikkerhetsbehov er vanskelige vurderinger. Disse vurderinger vil bli vesentlig enklere som følge av forskriften.

Den ekstra arbeidsmengde Datatilsynet vil påføres etter forskriften vil gjøre det nødvendig med en tilføring av 3 årsverk og ca 200 000 kr i forbindelse med sensitivitetsinnplassering av eksisterende registre. I tillegg må Datatilsynet skaffes hjemler til å ansette 2 1/2 saksbehandlere på permanent basis. Minst to av disse bør ha betydelig teknisk kompetanse.

Ved vurdering av stillingsbehovet må det tas hensyn til at Datatilsynet allerede i dag er underbemannet på den tekniske side. I budsjettet for 1988 var det således søkt om en teknisk stilling i tillegg til spesialrådgiverstillingen. Det ekstra stillingsbehov for Datatilsynet som følger av forskriften er således bare anslått til 1 1/2 stilling.

Det kan være passende å vise til at både i Danmark og Sverige er det 3 personer ved tilsynene som har teknisk kompetanse. Når man i tillegg foreslår regler som i større grad enn i disse land vil regulere sikkerhetsnivået rundt personregistre, burde det være tydelig at utvalgets forslag er meget beskjedent.

Justisdepartementet kan vente seg to oppgaver som vil kreve ressurser hvis forskriften gjøres gjeldende. Utover den normale bekjentgjøring, vil det antakelig være klagesaker som blir belastningen for Departementet. Dette antas å gjelde både klage på sensitivitetsfastsettelse og avslag på dispensasjoner. Arbeidsgruppa anslår dette til å innebære et ressurskrav på 4-5 ukeverk/år.

VEDLEGG

Utkast til

FORSKRIFT FOR SIKRING AV PERSONREGISTRE

Innholdsfortegnelse:

Del 1 OMFANG OG BRUK AV FORSKRIFTEN

1 OMFANG AV, DEFINISJONER I OG ADMINISTRASJON
AV FORSKRIFTEN 4

- § 1-1 Forskriftens omfang
- § 1-2 Sensitivitetsgrader
- § 1-3 Fastsettelse av sensitivitetsgrader for registre
- § 1-4 Fastsettelse av sensitivitetsgrader for lagringsmedia
- § 1-5 Om fastsettelse av sikkerhetsnivå
- § 1-6 Definisjon av ord og uttrykk. Forkortelser

Del 2 ADMINISTRATIV OG ORGANISATORISK SIKKERHET

2 SIKKERHETSORGANISASJON OG ADMINISTRASJON 8

- § 2-1 Organisasjon og administrasjon internt
- § 2-2 Oppdrag som utføres ved andre foretak
- § 2-3 Adgangs og tilgangskontroll

3 SIKRINGSTILTAK FOR FORETAK SOM UTFØRER
OPPDAG FOR ANDRE 9

- § 3-1 Generelt
- § 3-2 Krav til databehandlings- og vedlikeholdsforetak
- § 3-3 Krav til produsenter og importører

Del 3 TILGANGSKONTROLL OG FYSISK SIKKERHET

4 OPERASJONSKONTROLLSYSTEMER 10

- § 4-1 Operasjonskontrollsystemer
- § 4-2 Sperrer
- § 4-3 Krav til aktører
- § 4-4 Krav til operasjoner
- § 4-5 Autorisasjoner
- § 4-6 Operasjonskontrollmekanismer

- § 4-7 Identifikasjon
- § 4-8 Autentisering

5 FYSISK SIKKERHET 13

- § 5-1 Innbruddssikkerhet
- § 5-2 Sikkerhet mot brann- og vannskader
- § 5-3 Krav til fuktighet, temperatur og luftrenhet i rom og til sikring av strøm-, vanntilførsel og teletjenester
- § 5-4 Fysisk adgangskontroll
- § 5-5 Sikring av registres tilgjengelighet

6 TILGANGSKONTROLL 15

- § 6-1 Fastsettelse av sikkerhetsnivå for tilgangskontrollsystemer
- § 6-2 Tilknytningssikkerhet

Del 4 SPESIELLE KRAV TIL EDB-UTSTYR OG BRUK AV EDB-UTSTYR

7 NETTVERKS OG KOMMUNIKASJONSSIKKERHET 15

- § 7-1 Kontroll med tilgang i nettverk
- § 7-2 Lokalnett og andre nettverk av selvstendige EDB-enheter
- § 7-3 Sikkerhet ved overføring av opplysninger
- § 7-4 Distribuerte datamaskinsystemer

8 SIKKERHET FOR DATAMASKINER 16

- § 8-1 Sikkerhet for datamaskiner

9 SIKKERHET FOR LAGRINGSMEDIA OG PERIFERUTSTYR 17

- § 9-1 Sikkerhet for lagringsmedia
- § 9-2 Sikkerhet for datamaskiners periferutstyr

10 SIKKERHET I PROGRAMMER 18

- § 10-1 Sikkerhet i programmer som skal behandle registre
- § 10-2 Sikkerhet i systemprogrammer

11 OPERATIVSYSTEMSIKKERHET 18

- § 11-1 Operativsystemer
- § 11-2 Krav til filsystemer i flerbrukermiljø
- § 11-3 Brukerlagete operativsystem-rutiner

12 DATABASESIKKERHET	20
§ 12-1 Administrasjon og tilgangskontroll	
§ 12-2 Database-integritet og tilgjengelighet	
13 MASKINVARESIKKERHET	20
§ 13-1 Generelt	
§ 13-2 Sikkerhet i datamaskiners maskinvare	
14 DRIFTSSIKKERHET	21
§ 14-1 Generelt	
§ 14-2 Service og vedlikehold	
§ 14-3 Drift av datamaskiner	
§ 14-4 Sikkerhetskopiering	
§ 14-5 Registrering og etterbehandling	
§ 14-6 Makulering	
Del 5 SPESIELLE KRAV TIL REGISTERKVALITET	
15 REGISTERKVALITET	22
§ 15-1 Generelle krav til opplysnings- og registerkvalitet	
§ 15-2 Datainnsamling, koding, registrering og kontroll	
§ 15-3 Tolking av opplysninger	
§ 15-4 Søking	
§ 15-5 Dataoverføring	
§ 15-6 Endring og sletting	
§ 15-7 Dokumentasjon av register	
§ 15-8 Utskrifter	
§ 15-9 Resultatkontroll	

Del 1 OMFANG OG BRUK AV FORSKRIFTEN

1 OMFANG AV-, DEFINISJONER I OG ADMINISTRASJON AV FORSKRIFTEN

§ 1-1 Forskriftens omfang

Denne forskrift gir regler om sikring av personopplysninger, jfr. personregisterloven § 1.

Datatilsynet kan ved enkeltvedtak gjøre unntak fra bestemmelsene. Datatilsynet kan også i særlige tilfeller pålegge ytterligere sikringstiltak og treffe vedtak til utfylling og gjennomføring av forskriften.

§ 1-2 Sensitivitetsgrader

Ved fastsettelse av sensitivitetsgrader for en type opplysning, skal det skilles mellom gradene IKKE SENSITIV, MINDRE SENSITIV, SENSITIV og SÆRLIG SENSITIV opplysning avhengig av hvor store problemer trusler mot opplysningen antas å volde for den registrertes personlige integritet, helse, omdømme, rettigheter eller økonomi.

§ 1-3 Fastsettelse av sensitivitetsgrader for registre

Det skal hver for seg fastsettes sensitivitetsgrader for kompromittering og for datakvalitet for hver enkelt type opplysning i et register, for alle opplysnings-typene samlet og for hele registeret. Det skal også fastsettes sensitivitetsgrader for tilgjengelighet av et register.

Det kan fastsettes sensitivitetsgrader for deler av registre.

Ved fastsettelse av sensitivitetsgrader for registre eller deler av registre skal det legges vekt på antallet registrerte personer og opplysningenes sensitivitet.

For konsesjonspliktige registre etter PRL § 9 og for registre som er unntatt fra konsesjonsplikt etter PRL § 41 fastsetter Datatilsynet sensitivitetsgrader. Registereiers forslag bør først være innhentet.

For registre som er unntatt fra konsesjonsplikt etter forskrifter til PRL, gjelder de sensitivitetsgrader som der er gitt.

Registeransvarlig kan for delregistre som lagres fysisk adskilt selv fastsette sensitivitetsgrader for kompromittering og datakvalitet. Ved fastsettelsen skal det tas hensyn til de sensitivitetsgrader som ellers gjelder slik at delregistre alltid gis minst like høye sensitivitetsgrader som noen av de opplysningstyper som forekommer i delregistret.

§ 1-4 Fastsettelse av sensitivitetsgrader for lagringsmedia

Registeransvarlig skal besørge at det fastsettes K-, D- og T-sensitivitetsgrader for lagringsmedia eller at

media klareres med hensyn på hvor sensitive opplysninger som kan lagres der.

Et lagringsmedium har minst like høge sensitiviteter som sensitiviten til de registre eller deler av registre som fins på mediet.

Det bør fastsettes K-sensitivitet for rutinemessige utskrifter.

§ 1-5 Om fastsettelse av sikkerhetsnivå

Ved fastsettelse av sikringstiltak nyttes det tre sikkerhetsnivåer, kalt A, B og C, avhengig av sensitivitetsgrad, jfr. § 1-2.

For mindre sensitive registre skal iverksettes sikringstiltak som beskrevet under A, for sensitive registre som beskrevet under A og B og for særlig sensitive registre som beskrevet under A, B og C dersom ikke annet er fastsatt.

Krav som verken er knyttet til nivå A, B eller C gjelder også registre som er ikke sensitive.

Denne paragraf gjelder tilsvarende for opplysningstyper.

§ 1-6 Definisjon av ord og uttrykk. Forkortelser

I denne forskrift menes med

A: forkortelse for sikkerhetsnivå A skrevet foran de krav som stilles til sikkerhetsnivået.

aktør: en felles betegnelse for en person eller en automatisk prosess som utfører en operasjon.

autentisere: å vurdere om oppgitt identitet er riktig.

autorisere: å gi en aktør, eller en gruppe av aktører, tillatelse til å utføre bestemte operasjoner på bestemte ressurser, eventuelt på nærmere vilkår.

B: forkortelse for sikkerhetsnivå B benyttet foran de krav som stilles til nivået.

buffer: et lagerområde for mellomlagring av data ved kommunikasjon med eksternt lager, terminaler og datamaskiner, m.m.

C: forkortelse for sikkerhetsnivå C skrevet foran de krav som stilles til nivået.

D-sensitiv: forkortelse for sensitiv med hensyn til datakvalitet.

database: en samling filer som er tilgjengelig via et eget programsystem (kalt database-administrasjonssystem, eller kortere: DBAS).

database-integritet: graden av samsvar mellom det som er representert i databasen og det som skal representeres.

datamaskin (maskin): en programmerbar maskin med sentralprosessorer, internlagre og inn-ut-enhet for kommunikasjon med periferutstyr.

datamaskinanlegg: en eller flere sammenkoblede datamaskiner med periferutstyr og eventuelt med utstyr for kommunikasjon med andre anlegg.

dataskap: skap for oppbevaring av maskinlesbare lagringsmedia.

eksternlager: et lager ved en datamaskin som bare er tilgjengelig gjennom kanal for innmating og utmating.

felttype: en ikke sammensatt datatype.

fil: en navngitt samling data som består av et varierende antall poster av en bestemt posttype.

filsystem: et programsystem for organisering og katalogisering av filer på eksternlager og for regulering av tilgang til filer, m.m.

forsegling: påføring av segl eller kontrollsiffer blant annet for å hindre uvedkommende i å manipulere data uoppdaget.

fysisk adgangskontrollsystem: en type operasjonskontrollsystem. Fysisk adgangskontroll kan legges på flere nivåer som nevnt utenfra og innover: område rundt bygninger, bygning, seksjon av bygning, rom, arkivskap, m.m.

identifisere: å framskaffe identitet for en aktør, et program, en fil, m.m.

internlager: et lager i en datamaskin som er tilgjengelig uten bruk av kanal for innmating og utmating.

K-sensitiv: forkortelse for sensitiv med hensyn til kompromittering.

kommunikasjons-grensesnitt-enhet: en enhet som knytter en datamaskin eller en periferenhet til et nettverks kommunikasjons-kanal.

kryptere: å omforme data for å beskytte meningsinnholdet overfor uvedkommende. For å få tilgang til de opprinnelige data må de krypterte data dekrypteres.

lagringsmedium: maskinlesbart lagringsmedium og også papir m.m. for lagring og påfølgende manuell lesing og skrijving.

maskinlesbart lagringsmedium: et medium for automatisk lagring, lesing og skrijving av tekst og data som internlager, bånd, kassetter, plater og disketter.

modus for utførelse: det privilegienivå et program kan utføre under. Tilgang til å utføre maskininstruksjoner kan for eksempel begrenses til bestemte privilegie-nivåer.

mønster: fysiske kjennetegn for en aktør eller nøkler, koder og passord som brukes ved autentisering.

nettverk (nett): en samling datamaskiner og periferenheter knyttet sammen ved hjelp av kommunikasjonsutstyr for å utveksle data.

nettverk av datamaskiner: nettverk som knytter sammen datamaskiner og der periferenheter er knyttet til datamaskinene.

nettverk av selvstendige EDB-ressurser: nettverk som knytter datamaskiner, periferenheter og øvrige enheter direkte til nettverket. En enhet tilhører en åpen del av et nett om en åpent tilknyttet terminal kan få tilgang til den. Tilsvarende tilhører enheten en lukket del om bare lukket tilknyttede terminaler kan få tilgang.

operasjonskontrollmekanisme (OK-mekanisme): en innretning for å identifisere og autentisere aktører, slippe autoriserte aktører til og hindre uautoriserte i å slippe til sperrede operasjoner og objekter.

operasjonskontrollsystem (OK-system): et system for å kontrollere aktørers mulighet til å utføre operasjoner på bestemte ressurser. Et OK-system består av en sperre, autorisasjoner og en eller flere operasjonskontroll-mekanismer. Et OK-system kan legges utenpå et annet, jfr. definisjonene av fysisk adgangskontroll og tilgangskontroll.

operativsystem: et system av manuelle og automatiske rutiner for administrasjon av et datamaskin-anlegg.

operatør: en person som utfører operasjoner av betydning for databehandling.

oppdragsforetak: et foretak som utfører oppdrag for andre.

opplysning: personopplysning som definert i PRL § 1.

periferutstyr: eksternt lagerenheter, lesere, skrivere og terminaler.

posttype: en navngitt samling av en eller flere feltyper.

PRL: personregisterloven av 9.6.1978 nr. 48.

register: personregister etter PRL § 1.

ressurs: felles betegnelse for både aktører, prosesser og objekter.

sensitiv: en opplysning, et sett av opplysninger eller et register som enten er K-, D- eller T-sensitiv

sperre: et hinder for tilgang til operasjoner og ressurser.

T-sensitiv: forkortelse for sensitiv med hensyn til tilgjengelighet.

terminal: skjerm og tastatur og andre innretninger med tilstrekkelig utstyr for å kommunisere med en datamaskin.

tilgangskontrollsystem: en type operasjonskontroll-system. Et slikt system kan regulere aktørers tilgang til EDB-ressurser som nettverk, datamaskiner, periferutstyr, maskinlesbare data og programmer, m.m.

tilknytning, åpen: en tilknytning av terminal eller datamaskin til en datamaskin, eller et nettverk, der det ikke kontrolleres hvor forespørselen om tilknytning kommer fra. Tilknytning via oppringt linje eller åpent nett er eksempler på åpen tilknytning.

tilknytning, lukket: en tilknytning som bare kan oppnås fra en positivt bestemt gruppe terminaler eller datamaskiner. Lukkingen kan være logisk eller fysisk. En anropende enhet identifiseres ved terminal-, linje-, telefon-, maskinnummer, e.l. Begrenses tilknytning ved tilbakeringing, lukket brukergruppe, terminalidentifikasjoner e.l., vil den etter denne forskrift betraktes som logisk lukket.

transparent, distribuert datamaskinsystem: et system av sammenkoblede datamaskiner og periferenheter som framstår for brukerne som et datamaskinanlegg.

vedlikeholdsforetak: foretak som utfører vedlikehold på EDB-utstyr eller programmer som benyttes for lagring eller behandling av registre.

Del 2 ADMINISTRATIV OG ORGANISATORISK SIKKERHET

2 SIKKERHETSORGANISASJON OG ADMINISTRASJON

§ 2-1 Organisasjon og administrasjon internt

Ansvar for sikkerheten til et register etter denne forskrift påligger registeransvarlig.

Er det ellers tillatt, kan registeransvarlig overlate kontrollen med deler av sikkerheten til overordnet, sideordnet eller underordnet ledd i sin organisasjon. Delegering av dette ansvar skal foretas formelt.

Den daglige sikkerhetsmessige ledelse innehas av sikkerhetsansvarlig for registeret, som kan være en annen enn registeransvarlig. Til en slik funksjon hører ansvar for planlegging, etablering, organisasjon, vurderinger og kontroll av sikringstiltak for registeret og behandling av registeret. Ansvar for sikkerhetsopplæring og motivasjon av personalet bør også tilligge sikkerhetsansvarlig.

Om mer enn 5 personer har ansvar for deler av drift og kontroll av sikringstiltak for registeret, bør det finnes en sikkerhetsorganisasjon for dette.

Instruksér bør benyttes for ulike funksjoner av betydning for sikkerhet som vakt-, resepsjons- og arkivtjeneste, EDB-drift, registrering, etterbehandling, m.m. Instruksene bør også dekke irregulære hendelser, tilkalling av ekstra personell ved behov, m.m.

§ 2-2 Oppdrag som utføres ved andre foretak

Registeransvarlig som, helt eller delvis, overlater til annet foretak kontrollen med sikkerheten til registeret eller en del av det, som ved databehandlings- transport-, service- og vedlikeholds- eller lignende oppdrag, plikter å forsikre seg om at oppdraget skjer med den sikkerhet som er fastsatt i denne forskrift. Dette skal om nødvendig skje ved egen kontroll.

Registeransvarlig skal opplyse registerets sensitivitetsgrader til oppdragsforetaket.

§ 2-3 Adgangs og tilgangskontroll

Det skal være fysisk adgangskontroll til et register som fastsatt i § 5-4. Lagres registeret i fysisk adskilte deler skal det for hver del være slik adgangskontroll.

Det skal være tilgangskontroll til et maskinlesbart register som er tilgjengelig for flere brukere samtidig som fastsatt i § 6-1, jfr. § 8-1, 2. - 4. ledd. Det samme gjelder for en separat lagret del.

Også for lagringsmedia som ikke er maskinlesbare gjelder §§ 9-1 og 14-6.

3 SIKRINGSTILTAK FOR FORETAK SOM UTFØRER OPPDRAG FOR ANDRE (OPPDRAGSFORETAK)

§ 3-1 Generelt

B) Et foretak som utfører oppdrag for registeransvarlig skal på forespørsel kunne opplyse hvem i foretaket som har tilgang og adgang til registeret. Disse skal ha underskrevet taushetserklæring som har gyldighet for registeret. Ved faste oppdrag skal foretaket skriftlig bekrefte at sikkerheten for registeret tilfredsstilles for de tiltak oppdragsforetaket er ansvarlig.

§ 3-2 Krav til databehandlings og vedlikeholdsforetak
Databehandlings- og vedlikeholdsforetak plikter å sikre registre etter denne forskrift.

B) Autorisasjoner til et register for drifts- og vedlikeholdspersonale i foretak skal godkjennes av registeransvarlig.

Oppdragsforetaket er ansvarlig for kontroll av fastsatte sikringstiltak. Registeransvarlig skal ha anledning til å kontrollere de avtalte tiltak.

§ 3-3 Krav til produsenter og importører

Foretak som produserer eller importerer nettverk, § 7-2, datamaskiner, §§ 11-1 og 11-2 og § 13, databasesystemer, § 12, som brukes til behandling av registre skal opplyse til detaljister, kjøpere eller leiere og til Datatilsynet om i hvilken utstrekning produktet tilfredsstiller kravene i nevnte paragrafer. Produsenter og importører av tilgangskontrollsystemer, eller programmer som har innebygd tilgangskontrollsystem, skal vurdere disse etter § 6-1. Dokumentasjon og egen vurdering av produktet i forhold til forskriften skal sendes til Datatilsynet.

Del 3 TILGANGSKONTROLL OG FYSISK SIKKERHET

4 OPERASJONSKONTROLLSYSTEMER

§ 4-1 Operasjonskontrollsystemer

Et OK-system består av en sperre, autorisasjoner og en eller flere operasjonskontroll-mekanismer.

Der det er åpning i en sperre som skal beskytte operasjoner og ressurser, skal det etableres en OK-mekanisme.

Et OK-system har sikkerhetsnivå lik det laveste nivå for sperrer, autorisasjoner og OK-mekanismer det består av, jfr. §§ 4-2, 4-5 og 4-6. Sikkerhetsnivået er heller ikke høyere enn det høyeste nivå som tilfredsstilles under §§ 4-3 og 4-4.

Systemet skal utformes slik at operasjoner og ressurser beskyttes på en hensiktsmessig måte. OK-systemet skal jevnlig kontrolleres og vedlikeholdes av

autorisert personale.

Det skal etableres faste rutiner for administrasjon og drift av ethvert OK-system, dvs. for å innlemme og fjerne aktører, operasjoner og ressurser, for autorisasjon og for å drive OK-mekanismer.

§ 4-2 Sperrer

En sperre kan bestå av flere deler. Sikkerheten mot gjennomtrenging er da som den laveste sikkerhet for noen av delene.

Sperrer må ikke enkelt kunne trenge gjennom eller settes ut av funksjon.

En sperre kan legges utenpå en annen for å danne et mer effektivt hinder. Sikkerheten mot gjennomtrenging er da minst like høy som for den beste av sperrere.

§ 4-3 Krav til aktører

(1) Personell

A) Personer som autoriseres til å utføre operasjoner som er regulert av denne forskrift må gis opplæring, instruks og arbeidsforhold slik at arbeidet kan få god kvalitet.

Den enkelte må ikke misbruke autorisasjoner til å utføre oppdrag det ikke er behov for å utføre.

Aktører må påse at brukeridentifikasjon, passord, nøkler, terminaler, lokaler, m.m, beskyttes slik at ikke uvedkommende får tilgang til disse.

B) Det skal gis sikkerhetsopplæring.

Sikkerhetsinstruks for operatører bør foreligge.

(2) Automatiske prosesser

A) Automatiske prosesser skal være dokumenterte.

§ 4-4 Krav til operasjoner

A) Operasjonene bør tilrettelegges slik at de ikke kan brukes til å svekke OK-systemet.

B) Operasjoner og ressurser må struktureres på en slik måte at presise autorisasjoner kan gis.

C) Det bør føres kontroll med hvordan manuelle operasjoner utføres.

§ 4-5 Autorisasjoner

(1) Generelt

A) Autorisasjon skal bare gis til den som har behov for det, rettmessig adgang til det, og bare for den tid det er behov for det. Ved stillingsendringer skal autorisasjoner revurderes.

B) Enhver som skal autorisere skal selv ha autorisasjon fra registeransvarlig. Aktører skal autoriseres individuelt.

Alle autorisasjoner skal registreres. Autorisasjonene skal beskyttes mot innsyn, endring og sletting ved adgangskontroll, jfr. § 5-4, og tilgangskontroll der det er aktuelt, jfr. § 6-1, på

sikkerhetsnivå B.

C) Autorisasjonene skal sikres på sikkerhetsnivå C mot uautorisert innsyn, endring og sletting.

(2) Autorisasjon for tilgang til maskinlesbare, formaterte registre

A) Det kan gis tilgang til hele registeret under ett.

B) Det skal ikke gis tilgang til opplysninger om andre personer enn det er behov for.

Det skal bare gis tilgang til operasjoner av den type det er behov for.

C) Det skal ikke gis tilgang til opplysningstyper det ikke er behov for tilgang til.

(3) Autorisasjon for tilgang til dokumentbaserte og manuelle skjemabaserte registre

Et register der opplysningene i hovedsak ikke er formaterte, og manuelle skjemabaserte registre der opplysningene i hovedsak er formaterte, bør i størst mulig grad ordnes med person som hovednøkkel, og etter sak der det er høvelig.

A) Det kan gis tilgang til hele registeret under ett.

B) Det kan gis tilgang til de saker det er behov for.

C) Det skal bare gis tilgang til de dokumenter det er behov for.

§ 4-6 Operasjonskontrollmekanismer

(1) Generelle krav

En OK-mekanisme skal identifisere og autentisere alle aktører. Sikkerhetsnivået til en OK-mekanisme fastsettes som det laveste nivået som tilfredsstilles etter denne paragraf og etter §§ 4-7 og 4-8.

A) OK-mekanismen bør ikke på noe enkelt vis kunne omgås, endres eller settes ut av drift av uautoriserte. Identifikasjon kan skje gruppevis.

Aktører som ikke kan identifisere seg på foreskrevne måte må ikke gis tillatelse til å passere.

Operasjoner for godkjente aktører som ikke er forbudt etter autorisasjonene, kan tillates.

B) OK-mekanismen skal identifisere og autentisere alle aktører individuelt.

Forsøk på gjennomtrenging, misbruk, endring eller ødeleggelse av OK-mekanismen bør forhindres og skal varsles til sikkerhetspersonale så snart det oppdages.

C) Bruk av OK-mekanismen skal dokumenteres fortløpende. Dokumentasjonen oppbevares i minst 3 måneder. OK-mekanismen bør fortrinnsvis være innrettet slik at den sperrer de operasjoner og ressurser den beskytter om den settes ut av drift.

(2) Manuelle OK-mekanismer

Kravene i § 4-3(1) skal tilfredsstilles.

(3) Mekaniske OK-mekanismer

Mekaniske låser skal være tilstrekkelig dimensjonert etter de ressurser de skal beskytte, jfr. § 5-1.

(4) Automatiske OK-mekanismer

En OK-mekanisme i en datamaskin kan benytte identiteten for en aktør godkjent av en OK-mekanisme i et utenforliggende OK-system i datamaskinen. Identifikasjonssikkerheten er da ikke høyere enn sikkerhetsnivået i dette utenforliggende OK-systemet.

A) OK-mekanismens funksjonsmåte skal være dokumentert. Bare autorisert personale skal kunne sette igang, stoppe, endre og utføre lignende operasjoner på OK-mekanismen.

B) En automatisk OK-mekanisme skal bare godta et lite antall, gjentatte forsøk på åpning fra samme aktør før den blokkeres.

Åpning, eller forsøk på åpning, av automatisk OK-mekanisme skal logges med brukeridentifikasjon, tidspunkt og eventuelt med forsøkt mønster.

Alle operasjoner som ikke er tillatt etter autorisasjonene skal forbys av OK-mekanismen.

§ 4-7 Identifikasjon

(1) Identifikasjon av aktører

B) Identifikasjonsnummer og navn til godkjente aktører skal beskyttes mot uvedkommende og være korrekte og fullstendige før de godtas.

(2) Identifikasjon av program- og maskinvareenheter

B) Entydige program- og maskinvareidentiteter skal benyttes.

§ 4-8 Autentisering

(1) Valgbare mønstre

Antallet forskjellige mønstre i et autentiserings-system bør være så stort at automatisk generering og utprøving av mønster ikke vil lykkes før mønstrene er endret.

A) Det skal fastsettes en gyldighetsperiode for mønstre. Mønstre skal endres etter at de må antas kjent av andre.

Passord skal bestå av minst 4 tegn.

B) Mønstre skal lagres envegskryptert.

Mønstre som overføres over eksterne linjer eller nett bør krypteres.

Mønstre bør velges av den enkelte aktør slik at de ikke er enkle å gjette seg til.

C) Ved overføring bør kryptert mønster variere fra gang til gang.

Passord skal bestå av minst 6 tegn.

(2) Krav til autentisering av maskinvare

B) Autentisering av maskinvare bør være maskinvarestyrt.

C) Det bør finnes en kommando for å kreve at en enhet identifiserer seg for en bruker eller for et program.

(3) Krav til autentisering av programmer

C) Et programs identitet bør kunne bekreftes ved en kontroll med at programmet er uendret.

5 FYSISK SIKKERHET

§ 5-1 Innbruddssikkerhet

(1) Bygg og lokaler

Disse kravene til dører, vinduer, porter og luker gjelder enheter plassert i utvendige vegger.

A) Det skal være mulig å låse eller stenge dører, porter, vinduer, luker, m.m. forsvarlig.

B) Dører, porter, luker, hengslende vinduer ol skal ha låser godkjent av Forsikringsselskapenes Godkjennelsesnevnd eller låser av tilsvarende styrke. Utadslående dører, porter, luker ol skal ha hengsler som er sikret mot demontering eller ha bakkantbeslag. Dører, porter, luker ol som ikke vender mot beferdet område skal tilfredsstille kravene etter Norsk Standard 3159.

Innbruddsalarm bør være montert.

C) Dører skal tilfredsstille Norsk Standard 3159. Dørkarmers innfestning skal tilfredsstille Norsk Standard 3157. Innbruddsalarm skal være montert og varsle vaktsentral. Alternativt kan mobil vakt nyttes.

(2) Rom og soner

A) Rommet eller sonen må være mulig å avlåse.

C) Innvendige dører til rommet eller sonen bør ha låser godkjent av Forsikringsselskapenes Godkjennelsesnevnd eller ha tilsvarende innbruddsstyrke.

Sikkerhetsglass godkjent av Forsikringsselskapenes Godkjennelsesnevnd eller glass av tilsvarende styrke skal nyttes i vinduer på utvendige vegger. Disse vinduer skal være fastmonterte.

Dør til rommet bør ikke finnes i utvendige vegger.

Innbruddsalarm skal være montert.

(3) Arkiv- og dataskap

A) Skapet skal være låsbart.

B) Stålskap, eller skap av tilsvarende styrke, skal benyttes.

C) Skapet må ha en dirksikker lås og må ikke lett kunne fjernes. Skapet må bare kunne åpnes med nøkkel uten at synlige spor settes.

§ 5-2 Sikkerhet mot brann- og vannskader

(1) Rom og soner

A) Brannslukningsutstyr skal alle steder være

tilgjengelig innen 15 meters avstand. Opplæring i bruk skal gis ansatte.

B) Rommet eller sonen skal være beskyttet i minst brannklasse A60, jfr. Norsk Standard 3919. Brannøvelse bør gjennomføres minst hvert andre år. Brennbart inventar bør begrenses til et minimum.

C) Rommet eller sonen beskyttes i brannklasse A90, jfr. Norsk Standard 3919. Ligger rommet eller sonen i kjeller skal det være særlig sikret mot vannskade. Brann og vanddetektorer skal være installert og varsle vaksentral. Et rom eller en sone som normalt er ubemannet bør ha automatisk brannsløkkingsanlegg.

(2) Arkiv- og dataskap

Arkiv- og dataskap må plasseres med tanke på at de raskt kan berges ut i tilfelle brann.

Arkiv- og dataskap skal tilfredsstille Nordtest standard, NT Fire 017 slik:

- B) 1 times motstand
- C) 2 timers motstand

§ 5-3 Krav til fuktighet, temperatur og luftrenhet i rom og til sikring av strøm-, vanntilførsel og teletjenester

Fuktighet, temperatur, og renhet i luft bør ligge innenfor toleransegrenser fastsatt av leverandører for utstyret.

B) Sikringstiltak for å unngå avbrudd i strøm-, vannforsyning og teletjenester bør vurderes.

§ 5-4 Fysisk adgangskontroll

(1) Generelt

Sikkerhetsnivået til fysiske adgangskontrollsystemer bestemmes av krav etter denne paragraf, §§ 4-1 og 5-1.

Sikkerheten i adgangskontrollen til en bestemt ressurs mot en inntrenger er minst like høy som den beste sikkerhet i noe adgangskontrollsystem som registeransvarlig har kontroll med og som inntrengereren må passere for å få adgang til ressursen.

Sikkerheten overfor utenforstående, overfor ansatte e.l. som ikke skal ha adgang til registeret og overfor slike som skal ha adgang skal vurderes hver for seg.

(2) Fysisk adgangskontroll til bygninger og lokaler

A) Det skal føres tilsyn med alle åpne innganger og adkomstveier til lokalene. Resepsjonen skal ta imot og henvise besøkende.

C) Besøksliste skal føres og besøk hentes i resepsjonen. Der ansatte ikke kan forventes å kjenne hverandre bør identitetskort brukes og bæres synlig. Besøkende bør tildeles egne kort og ledsages av ansatte.

§ 5-5 Sikring av registres tilgjengelighet

Et maskinlesbart register skal ha en sikkerhetskopi sikret etter §§ 5-2 og 5-4 på et sikkerhetsnivå bestemt av registrets T-sensitivitet. Sikkerhetskopi skal

oppbevares i betryggende avstand fra originalen.

Et manuelt register skal sikres etter §§ 5-2 og 5-4 på et sikkerhetsnivå bestemt av T-sensitiviteten.

Et manuelt, særlig T-sensitivt register skal overveies sikkerhetskopiert ved mikrofilming e.l.

6 TILGANGSKONTROLL

§ 6-1 Fastsettelse av sikkerhetsnivå for tilgangskontrollsystemer

Sikkerhetsnivået til et tilgangskontrollsystem bestemmes etter § 4-1. Ved fastsettelse av sikkerhetsnivået for tilgangskontrollsystemer til nettverk, datamaskiner og periferutstyr skal også kravet til tilknytningssikkerhet i § 6-2 benyttes.

Sikkerheten i tilgangskontrollen til en bestemt ressurs mot en inntrenger er minst like høy som den beste sikkerhet i noe tilgangskontrollsystem som registeransvarlig har kontroll med og som inntrengerer må passere for å få tilgang til ressursen.

Registeransvarlig skal vurdere sikkerheten overfor utenforstående, overfor ansatte som ikke skal ha tilgang og overfor ansatte som skal ha tilgang hver for seg.

§ 6-2 Tilknytningssikkerhet

En datamaskin, et nettverk eller en annen EDB-enhet har tilknytningssikkerhet som den laveste for noen inngang bestemt etter denne paragraf.

Sikkerhetsnivået for tilknytning til en inngang bestemmes slik:

A) Åpen tilknytning kan benyttes.

B) Åpen tilknytning kan nyttes for en inngang om det med meget høy sikkerhet kan begrenses hvilke data og brukere eller programmer inngangen kan gi tilgang til. Logisk lukket tilknytning kan benyttes.

C) Fast (fysisk lukket) tilknytning kan benyttes.

Logisk lukking kan benyttes om endring av lukking bare kan finne sted fra lokaler registeransvarlig har fysisk adgangskontroll til på sikkerhetsnivå C.

Manuell tilknytning kan nyttes om den som utfører tilknytningen gjenkjenner enhver som har tillatelse til å bli tilknyttet.

Del 4 SPESIELLE KRAV TIL EDB-UTSTYR OG BRUK AV EDB-UTSTYR

7 NETTVERKS- OG KOMMUNIKASJONSSIKKERHET

Om et register lagres eller behandles i nettverk skal krav fastsatt i dette kapittel tilfredsstilles.

§ 7-1 Kontroll med tilgang i nettverk

I en åpen del av et nett skal verken sensitive eller

særlig sensitive registre lagres. I en lukket del kan sensitive registre lagres.

Et særlig sensitivt register kan lagres i et fysisk lukket nett, hvis det er fysisk adgangskontroll, jfr. § 5-4, til nettets ressurser på sikkerhetsnivå C.

§ 7-2 Lokalnett og andre nettverk av selvstendige EDB-enheter

Et nettverks operativsystem skal tilfredsstillе krav fastsatt i § 11-1.

En kommunikasjons-grensesnitt-enhet må ha fysisk adgangskontroll og tilgangskontroll på sikkerhetsnivå med det mest sensitive register som skal kunne behandles i nettverket.

§ 7-3 Sikkerhet ved overføring av opplysninger

Ved overføring av opplysninger skal det kontrolleres at mottaker har tillatelse til å motta opplysningene, at tillatelse foreligger til å utlevere og at mottaker er riktig identifisert. Utlevering og mottak av opplysninger skal logg-føres.

Særlig K-sensitive opplysninger som overføres, eller K-sensitive opplysninger som overføres i stort omfang, i åpne eller offentlige nett, skal overføres kryptert.

Ved overføring av særlig sensitive opplysninger til annet anlegg kan logisk lukket tilknytning benyttes, jfr. § 6-2, ved de aktuelle innganger til mottaker-anlegget dersom det verken er mulig å lese, endre eller slette tidligere overførte opplysninger via disse tilknytninger.

§ 7-4 Distribuerte datamaskinsystemer

I et transparent, distribuert datamaskinsystem gjelder krav som fastsatt i § 8-1 for alle datamaskiner som er del av systemet. Alle eksternlagerenheter i et slikt system skal tilfredsstillе § 5-4.

Kravene i kapittel 11 og 13 gjelder tilsvarende for distribuerte operativ- og databasesystemer.

8 SIKKERHET FOR DATAMASKINER

Dette kapittel gjelder for datamaskiner som skal behandle registre.

§ 8-1 Sikkerhet for datamaskiner

Om et register lagres ved eller behandles av en flerbrukermaskin, skal denne ha operativsystemsikkerhet og maskinwaresikkerhet som fastsatt i kapitlene 11 og 13.

Er det fysisk adgangskontroll på sikkerhetsnivå A til terminaler som gir tilgang til et mindre sensitivt register, kan kravene til tilgangskontroll for datamaskinen etter § 6-1 sløyfes.

Det skal være tilgangskontroll til en enbrukermaskin på sikkerhetsnivå B om et særlig sensitivt register lagres ved denne.

Det skal være fysisk adgangskontroll, jfr. § 5-4, til en datamaskin som behandler registre.

Maskinen må sikres etter § 5-2(1) på et sikkerhetsnivå bestemt av T-sensitivitet for registre som behandles.

Maskinrom skal tilfredsstille krav til klima m.m. som fastsatt i § 5-3.

Drift av datamaskiner skal tilfredsstille krav fastsatt i kapittel 14.

9 SIKKERHET FOR LAGRINGSMEDIA OG PERIFERUTSTYR

Media og periferutstyr som brukes til lagring, lesing eller skriving av opplysninger, skal ha sikkerhet som fastsatt i dette kapittel.

§ 9-1 Sikkerhet for lagringsmedia

(1) I lokalene

Det skal være fysisk adgangskontroll som fastsatt i § 5-4 til et lagringsmedium.

Maskinlesbare lagringsmedia skal være sikret mot brann- og vannskader etter § 5-2 på et sikkerhetsnivå bestemt av T-sensitivitetene for lagringsmediene.

B) Før lagringsmedia utleveres, skal det kontrolleres at utlevering kan foretas. Utlevering og mottak av lagringsmedia skal logg-føres.

(2) Ved transport

Hvis et lagringsmedium under transport ikke er under transportørs oppsyn eller kontroll forøvrig, skal det være godt sikret mot tyveri, ødeleggelse og skade.

A) Forsendelse kan skje i lukket sending eller med bud.

B) Forsendelse skal skje rekommandert eller forseglet.

C) Transport av lagringsmedia skal skje forseglet eller med særskilt godkjent bud. Mottaker skal kvittere for mottatt sending.

§ 9-2 Sikkerhet for datamaskiners periferutstyr

Det skal være fysisk adgangskontroll som fastsatt i § 5-4 til periferutstyr som brukes til å lagre, lese eller skrive opplysninger.

(1) Eksternlagerenheter

Det skal være tilgangskontroll til eksternlagerenheter som fastsatt i kapittel 6. Enhetene må sikres etter § 5-2(1) på et sikkerhetsnivå bestemt av T-sensitivitet.

Sikkerhetsnivået skal minst være så høgt som for det mest sensitive lagringsmedium som skal kunne behandles.

Lagerenheter som brukes til lagring av særlig K-sensitive eller særlig D-sensitive opplysninger, kan ha logisk lukket tilknytning, jfr. § 6-2, om opplysningene lagres henholdsvis kryptert eller forseglet. Dekryptering eller bryting av segl må skje i en datamaskin med tilgangskontroll på sikkerhetsnivå C.

(2) Sikkerhet for terminaler

Det skal være fysisk adgangskontroll som fastsatt i § 5-4 til terminaler som kan gi tilgang til et register.

B) En terminal som kan gi tilgang til register bør logges ut etter høyst 15 minutter uten aktivitet.

Hvis rommet forlates av terminal-operatøren i løpet av arbeidsdagen skal utlogging, låsing av terminal eller rom finne sted. Ved arbeidsdagens slutt skal brukeren logges ut.

C) Terminalen bør være mulig å låse.

10 SIKKERHET I PROGRAMMER

§ 10-1 Sikkerhet i programmer som skal behandle registre
Ethvert program skal være godkjent til bruk av registeransvarlig.

Et program skal bare kunne legges inn i maskinen og klargjøres for drift av autorisert personale.

Det skal være tilgangskontroll til programmer som fastsatt for register i § 6-1, jfr. § 8-1, 3. ledd.

Ved utvikling av programmer bør en nytte faste metoder og standarder, som "DND og NFK's Standard for kvalitetssikring av programvare". En skal dokumentere programmene slik at feil kan unngås og raskt rettes om de oppstår.

Testing og feilsøking i programmer bør i størst mulig grad skje uavhengig av register.

§ 10-2 Sikkerhet i systemprogrammer

Oversetterprogrammer (kompilatorer og interpretere), lenkeredigerer og lastemodul og programmer som skal bidra med tilgangskontroll eller annen sikkerhet på sikkerhetsnivå B eller C for et register, skal sikres mot endring som fastsatt for register etter §§ 5-4 og 6-1.

11 OPERATIVSYSTEMSIKKERHET

§ 11-1 Operativsystemer

Et operativsystem skal sørge for tilgangskontroll

til de ressursene det administrerer, jfr. § 6-1.

Krav som ikke tilfredsstilles av et operativsystem etter denne paragraf kan tilfredsstilles av supplerende sikkerhetssystemer.

A) Operativsystemet skal ha kontroll med tildeling av ressurser til ulike aktører, tilgang til lagerområder og operativsystem-funksjoner og kontroll med skifte mellom modi for utførelse.

B) Operativsystemets dataområder for administrasjon av ressurser skal bare være direkte tilgjengelig for operativsystemet og for spesielt autorisert personale for feilsøking og retting. For øvrige brukere og programmer skal tilgang bare gis via operativsystemet.

Operativsystemet må hindre et program i å referere utenfor lagerområde programmet skal ha tilgang til.

Det skal være mulig å autorisere en brukers tilgang til de ulike operativsystem-funksjoner.

Forsøk på å skaffe seg tilgang til filer og funksjoner en bruker ikke er autorisert for, skal logges av operativsystemet.

Operativsystemet skal ha en sikkerhets-logg med registrering av tidspunkt for på- og avlogging og fra hvilken terminal dette skjer. Likedan skal manuell oppstarting av programmer registreres. Bruk av operativsystem-funksjoner skal også kunne logges.

C) Operativsystemet skal ha verktøy for å analysere operativsystemets sikkerhets-logg.

Operativsystemet bør håndtere systemfeil, uforutsette og planlagte stans av systemet slik at sikkerheten opprettholdes.

§ 11-2 Krav til filsystemer i flerbrukermiljø

B) Et filsystem må kontrollere at en fils logiske lagerområde ligger innenfor brukerens logiske lagerområde.

Filsystemet skal ha mulighet for å kontrollere tilgang på minst tre nivåer til filer tilsvarende brukerens, en gruppes og andres autorisasjoner. Det skal kunne autoriseres til operasjonene lese, skrive, føye til, endre navn, endre autorisasjon og slette, for alle filer og utføre for programfiler.

Standard autorisasjon til genererte filer skal være 'ingen tilgang' for andre enn brukeren selv.

C) Filsystemet skal ved frigivelse av lagerområder kunne foreta fysisk sletting av opplysninger.

§ 11-3 Brukerlagete operativsystemrutiner

C) Brukerlagete operativsystemrutiner må godkjennes av sikkerhetsansvarlig før implementering.

Brukerlagete operativsystemrutiner må ikke endre modus for utførelse for et kallende program eller endre programmets autorisasjoner forøvrig. Slike rutiner må heller ikke overlate kontroll til en rutine med uvis sikkerhet, unntatt det kallende program. Rutinene må kontrollere om det kallende program har skrivetilgang for et angitt lagerområde ved returnering av data, og de må bare bruke godkjente moduler for lasting fra eksternlager.

12 DATABASESIKKERHET

Et register etablert som en database, eller del av en database, skal tilfredsstille de krav som er fastsatt i dette kapittel.

§ 12-1 Administrasjon og tilgangskontroll

Kontroll med tilgang til database-administrasjonssystemet (DBAS), skal være som fastsatt i § 10-2.

B) Registeransvarlig skal kunne autorisere til operasjoner på databasen eller sin del av en database. DBAS må kunne kontrollere tilgang til filer og postforekomster for de ulike brukere.

For enhver database som inneholder flere registre bør det være en databaseadministrator med ansvar for utforming, opprettelse, redefinerings, vedlikehold og sikkerhet for databasen.

Databasefilene skal bare være tilgjengelig via DBAS og andre spesielt autoriserte programmer.

En brukers buffere for databasefiler skal bare være tilgjengelig for brukeren via DBAS.

C) DBAS må kunne begrense tilgang til bestemte felttyper i en fil. DBAS bør kunne begrense tilgang til postforekomster avhengig av verdier for felter.

§ 12-2 Database-integritet og tilgjengelighet.

B) DBAS skal sørge for entydig identifikasjon av poster.

Relasjonsdatabasesystemer bør sørge for at ethvert referansefelt i en post enten refererer en eksisterende eller ingen post.

C) Datadefinisjonsspråket bør ha muligheter for spesifikasjon av integritetsrestriksjoner på og mellom felter, som ikke nødvendigvis er i samme post. Formatrestriksjoner, domene- og verdirestriksjoner bør kunne gis. Tilsvarende bør prosedyrer for håndtering av unntakssituasjoner kunne beskrives. DBAS skal påtvinge restriksjonene.

DBAS bør ha mulighet for forsøksvis oppdatering.

13 MASKINVARESIKKERHET

§ 13-1 Generelt

Maskinvaren må være utviklet og produsert med høy sikkerhet mot uautoriserte endringer i forhold til spesifikasjonene.

Maskinvaren skal være godt dokumentert og sikkert identifisert, jfr. også § 4-7(2).

Maskinvaren skal tilfredsstille leverandørens dokumenterte testkrav.

§ 13-2 Sikkerhet i datamaskiners maskinvare

B) Maskinvaren skal kunne sperre programmer mot å skrive, lese og utføre i ulike deler av internlager.

Tilgangen til maskininstruksjoner som påvirker sikkerheten skal kontrolleres for ulike brukere og programmer.

Maskininstruksjoner for å lese fra og skrive til eksternlager eller kommunikasjon skal ikke være direkte tilgjengelige for et program i brukermodus.

Avbruddsrutiner i maskinvaren bør kontrollere system- og operatørfeil.

Feilkontroll bør finne sted ved overføring til og fra eksternlager og ved kommunikasjon.

Alle instruksjoner med alle mulige operander, koder mv bør lede til kjente reaksjoner fra maskinvaren.

C) Feilkontroll bør finne sted ved henting av instruksjoner og operander for utførelse.

14 DRIFTSSIKKERHET

§ 14-1 Generelt

A) Databehandling av registre skal tilrettelegges slik at den blir mest mulig robust mot uønskete hendelser. Uhell, misbruk, feil og øvrige trusler skal søkes avdekket og avverget så effektivt som mulig. Rutiner for trusselrapportering og dokumentasjon bør finnes.

B) Det skal jevnlig kontrolleres at komponenter av betydning for sikkerheten virker som forutsatt.

§ 14-2 Service og vedlikehold

A) Endringer av programmer, databaser, operativsystemer og maskinvare skal logges og bare kunne utføres av dertil autorisert personale.

B) Personer som skal foreta feilsøking mot registre skal ha undertegnet taushetserklæring.

Ved fjerndiagnose skal tilknytning skje manuelt. All fjerndiagnose skal logges.

Eventuelle kopier av opplysninger som tas i forbindelse med feilsøking skal sikres etter denne forskrift.

§ 14-3 Drift av datamaskiner

B) Det skal finnes retningslinjer for å opprette, autorisere, kontrollere og fjerne brukere i en datamaskin. Ansvar for disse rutinene skal være klart plassert. Rutinene skal bare kunne utføres av autoriserte personer fra autoriserte terminaler eller av programmer.

Låsbare maskiner skal være låst unntatt ved oppstart og stopping. Det skal foreligge retningslinjer for stopping og start.

Bare autorisert personale skal kunne starte

maskinen.

Før et register etableres som en database, samling av filer, e.l., skal dette være godkjent av registeransvarlig.

Satsvise databehandlingsoppdrag skal være dokumenterte og de skal logg-føres. Dokumentasjonen bør omfatte hvilke programmer, registre og eventuelle lagringsmedia som skal benyttes.

§ 14-4 Sikkerhetskopiering

A) Det skal finnes rutiner for å sikkerhetskopierte maskinlesbare registre og programmer.

B) Sikkerhetskopiering av registre bør foretas høyst en uke etter endring. Kopi av endringer av registeret bør tas fortløpende og oppbevares til to nye sikkerhetskopier av registeret er tatt. Sikkerhetskopier skal lagres på annet medium enn det registeret ligger på.

C) Tilstanden før eller etter oppdatering bør kopieres.

§ 14-5 Registrering og etterbehandling

Det skal være fysisk adgangskontroll til lokaler der registrering, utskrift og etterbehandling finner sted, jfr. § 5-4, på et sikkerhetsnivå bestemt av opplysningenes sensitivitet.

Sensitive opplysninger skal oppbevares innelåst etter arbeidstid.

§ 14-6 Makulering og sletting

Før makulering av lagringsmedia foretas må det forsikres at identiteten til mediene er riktig og at tillatelse til makulering foreligger.

Ved transport og oppbevaring før makulatur gjelder krav etter § 3-1.

B) Det må sørges for at materialet ikke er rekonstruerbart etter makulering.

C) Transport og makulering skal foretas under oppsyn av en representant for registeransvarlig eller oppdragsforetak.

Del 5 SPESIELLE KRAV TIL REGISTERKVALITET

15 REGISTERKVALITET M.M.

Et register skal tilfredsstillende de krav til kvalitet som er fastsatt i dette kapittel. Sikkerhetsnivået bestemmes av D-sensitiviteten for registeret.

§ 15-1 Generelle krav til opplysnings- og registerkvalitet

A) Registeret må ha en egnet representasjon av opplysningstypene. Formater og koder må være slik at opplysningene enkelt lar seg beskrive.

B) Vilkår for at poster og opplysninger skal forekomme i register skal være dokumenterte. Det må innføres passende rutiner slik at registeret til enhver tid er fullstendig.

C) Det skal etableres informasjons-, meldings- eller kontrollrutiner slik at registeret er fullstendig og uten irrelevante opplysninger.

Det skal innføres gyldighetsperiode for opplysninger som varierer over tid.

§ 15-2 Datainnsamling, koding, registrering og kontroll
Nøyaktighet og presisjon bør angis for opplysningstypene i registeret der det er aktuelt.

Ved måling, observasjon og annen innsamling av data må det påsees at dataene er tilstrekkelig nøyaktige og presise for det formål de skal anvendes.

A) Det bør gis opplæring i å kode og registrere, og forstå de forhold som registreres, om sammenhenger som gjelder mellom opplysninger i registeret og om bruk av det utstyr og de programmer som trengs for å kode og registrere. Opplysninger som inntas i register bør kvalitetskontrolleres etter registrering.

B) De som skal kode, registrere eller kontrollere opplysninger skal autoriseres for dette.

Koding, registrering og oppdatering i register skal kontrolleres. Andre personer enn de som utførte arbeidet bør fortrinnsvis foreta kontrollen.

Sammenhenger som skal gjelde i et register skal automatisk eller manuelt kontrolleres ved innsetting av nye opplysninger eller poster. Opplysninger bør kontrolleres for rimelighet der detaljerte kontroller ikke er mulig.

Kontroll av gyldighet for sammenhenger mellom opplysninger, forekomst av opplysninger og poster som med rimelighet kan automatiseres, bør automatiseres.

C) Opplysninger bør tilbys til kontroll for den registrerte etter registrering såfremt det er innsynsrett i registeret.

§ 15-3 Tolking av opplysninger

B) Det skal gis opplæring i tolking av registerets opplysningstyper og i bruk av det utstyr og den informasjon som trengs for tolkinga.

§ 15-4 Søking

A) Brukere som skal søke i et register må gis opplæring i utforming av søkekriterier, om søkemekanismene og vurdering av resultatene av søk.

B) Det skal kontrolleres at personidentiteten for framsøkte opplysninger er entydig og korrekt før opplysningene brukes om personen.

C) Det bør forsikres at søk gir fullstendige og relevante resultater.

§ 15-5 Dataoverføring

C) Ved overføring av opplysninger i telenettet, i åpne nettverk eller ved andre åpne transmisjonsmåter skal opplysningene forsegles forsvarlig. Både mottaker og sender skal logg-føre sending. Mottaker skal kvittere for godkjent mottak til avsender.

§ 15-6 Endring og sletting

A) Opplysninger skal slettes i henhold til fastsatte slettefrister.

B) Opplysning som kan antas å være foreldet eller uriktig skal innhentes på nytt før den brukes i noen beslutning. Der vilkår for forekomst av opplysning ikke lenger er oppfylt skal opplysninga fjernes, eller merkes ugyldig.

I den utstrekning det ikke strider med PRL § 8 skal alle endringer logges med angivelse av situasjonen før og etter endringa, hvem som foretok denne og tidspunkt. De personer som skal ha anledning til å endre eller slette opplysninger skal være autorisert for dette.

§ 15-7 Dokumentasjon av register

A) Følgende dokumentasjon skal finnes: formål med registeret, beskrivelse av opplysningstypene, sammenhenger mellom opplysningstyper, vilkår for at poster og opplysninger skal foreligge, samt kodeskjema.

B) Det bør for alle opplysninger i et register framgå hvilken aktør som har produsert, kodet, registrert og kontrollert eller avgitt opplysningene.

Det bør registreres fra hvilket tidspunkt en opplysning gjøres tilgjengelig.

§ 15-8 Utskrifter

A) Utskrifter til den registrerte bør være enkle å forstå og kontrollere riktigheten av. Om nødvendig skal det legges ved informasjon eller henvises til informasjonstjeneste.

B) Det bør etter egne retningslinjer foretas kontroller av kvaliteten av utskrifter, f eks ved stikkprøver.

§ 15-9 Resultatkontroll

B) Rutinemessig resultatkontroll bør foretas, f eks ved rimelighetskontroll.

Indeksliste

adkomstveier	14
aktør	5, 6, 7, 10, 11, 12, 18, 24
arkiv	8
arkivskap	6
autentisere	5, 6, 11
autorisere	5, 10, 19, 20, 21, 23
avbruddsrutiner	21
besøkende	14
besøksliste	14
brann	
-slokking	
-sanlegg, automatisk	14
-sutstyr	13
-øvelse	14
bruker	7, 15, 17, 19, 20, 21
	23
brukeridentifikasjon	10, 12
brukergruppe	7
bud	17
særskilt godkjent -	17
buffer	
D-sensitiv	5, 18, 22
database	5, 20, 21
- administrasjonssystem (DBAS)	5, 20
-integritet	5
-system	9, 16
distribuert -	2, 7, 16
databehandling	1, 7, 21
-soppdrag	22
satsvise -	22
-sforetak	9
datadefinisjonsspråk	20
datakvalitet	4, 5
datamaskin	5, 6, 7, 12, 15, 16, 17
	18, 20, 21
-anlegg	5, 7
enbruker -	17
drift av -	17
flerbruker -	3, 16, 19
-system	7, 16
distribuert -	7, 16
transparent -	7, 16
dataskap	5, 13, 14
datatype	6
detektor	
brann-	14
vann-	14
dokument	10, 11, 12, 13, 19
eksternlager	5, 6, 19, 21
overføring til -/ fra -	19, 21
enheter	7, 16, 17
etterbehandle	8, 22

feilkontroll	21
feilsøking	18, 19, 21
felt	20
-type	6, 7, 20
referanse-	20
fil	5, 6, 19, 20, 21
generert -	19
-system	6, 19
formater	22
forsegle	17, 18, 23
forsendelse	17
fysisk adgangskontroll (evt. bare adgangskontroll)	6, 8, 10, 14, 15, 16, 17, 18, 22
-system	6, 7, 8, 14, 15, 16, 17, 18 22
gyldighetsperiode	12, 23
identifikasjons-	
nummer	12
navn	12
identifisere	6, 7, 11, 12
identitet	5, 6, 12, 13, 22
inn-ut-enhet	5
innbruddsalarm	13
innganger	14, 16
inntrenger	14, 15
interpretere	18
internlager	6, 20
instruks	8, 10
K-sensitiv	5, 6, 16, 17
klarere	5
kode	6, 21, 22, 23
kompiletor	18
kompromittering	4, 6
kommando	12
kommunikasjon	5, 21
-sutstyr	6
-skanal	6
-s-grensesnitt-enhet	6, 16
kryptere	6, 12
de-	6
envegs-	12
lagerområde	5, 19
logisk -	19
lagringsmedium	4, 5, 17, 22
makulering av -	22
maskinlesbart -	5, 6
mottak av -	17
utlevering av -	17
transport av -	17, 22
lastemodul	18, 19
lenkeredigerer	18
leser	7
linje	7

ekstern -	12
oppringt -	7
logg-	12, 16, 17, 18, 19, 21, 22, 23, 24
lukket sending	17
lås	
dirksikker -	13
manuell oppstartning	19
maskinlesbare data	7
maskinrom	17
mellomlagring	5
mikrofilming	15
mobil vakt	13
modus for utførelse	6, 19
moduler	19
mønster	6, 12
overføre -	
måling	23
nettverk (nett)	6, 7, 12, 19, 20
- av datamaskiner	
- av selvstendige EDB- ressurser	
lukket -	6, 7
lukket del av -	6, 15
offentlig -	16
åpen del av -	6, 15
åpent -	6, 7
nøkkel	13
nøyaktighet	23
objekter	6, 7
observasjon	23
operand	21
operasjon	5, 6, 7, 12, 19, 20
operasjonskontroll	5, 10, 11
-mekanisme (OK-mekanisme)	6, 11
automatisk -	12
manuell -	11
mekanisk -	12
-system (OK-system)	6, 9
operativsystem	7, 16, 18, 19, 21
distribuert -	8
nettverks -	16
-rutine	20
brukerlagete -	19
-funksjon	19
operatør	7, 10, 18, 21
oppdrag	
databehandlings-	8, 9, 22
service-	8, 21
-sforetak	7, 8, 9, 22
transport-	8, 17, 22
vedlikeholds-	7, 8, 9
opplysning	7
mottak av -	16
overføring av -	8, 16, 23

slette -	16, 24
utlevering av -	16
passord	6, 10, 12
periferutstyr	5, 7, 17
personopplysning	4
personregister	4
post	6, 20, 22, 23, 24
posttype	6, 7
presisjon	23
program	6, 7, 9, 12, 13, 15, 18, 19, 20, 21, 22, 23
kallende -	19
system-	18
prosedyre	20
prosess	7
automatisk -	5, 10
register	4, 5, 7, 9, 11, 14, 18, 20, 24
-ansvarlig	4, 8, 9, 10, 14, 18, 20, 21, 22
-eier	4
formatert -	11
maskinlesbart -	12, 14
manuelt -	12, 14
dokumentbasert -	11
skjemabasert -	11
registrere	10, 23, 24
registrert (registrert person)	4, 23, 24
rekommandert	17
resepsjon	8, 14
ressurs	5, 6, 7, 9, 10, 11, 14, 15, 16, 18, 19
retningslinje	21, 24
rom	6, 13, 14, 18
rutine	9, 19, 21, 22
automatisk -	7
manuell -	7, 10, 19
kontroll-	23
meldings-	23
segl	6
bryting av -	18
sensitiv	
sensitivitetsgrad	4, 8
sentralprossessor	5
sikkerhets	
-ansvarlig	8, 19
-glass	13
-kopi	14, 15, 22
-logg	19
-nivå	5, 9, 10, 11, 12, 14, 15, 16, 17, 22
-opplæring	8, 10, 13, 23
-personale	11
-systemer	18
sikringstiltak	5, 8, 9, 14
fastsettelse av -	

skade	13, 14, 17
skjerm	7
skriver	7
slette	16, 19, 24
sone	13, 14
sperre	6, 7, 9, 10, 20
stålskap	13
søker	23
T-sensitiv	7, 14, 17
tastatur	7
terminal	5, 6, 7, 10, 16, 18, 19, 21
testing	18
tilbakeringing	7
tilgangskontroll	7: 10, 15: 18, 20
-system	7, 9, 15
tilgjengelighet	4
tilknytning	7, 15, 16, 21
lukket -	7, 15, 16, 18
fysisk -	15
logisk -	18
manuell	11
åpen -	7, 15
-ssikkerhet	15
tilstanden	22
transmisjonsmåte	23
åpen -	23
transportør	17
tyveri	17
utlogging	18
utskrift	22, 24
rutinemessig -	5
vakt	8, 13
mobil -	13
-sentral	13, 14
vedlikehold	7: 9, 20, 21
-sforetak	7, 9
ødeleggelse	11, 17



Tidligere utgitt i skriftserien CompLex

Alle heftene i skriftserien CompLex kan kjøpes hos, eventuelt bestilles fra Akademika (se kupongen bakerst). De kan også kjøpes fra Norsk forening for jus og edb, Postboks 7557 Skillebekk, 0205 OSLO 2. Her kan man også tegne abonnement eller abonnere på «vaskesedler» som gir en kort omtale av hver rapport etterhvert som de kommer ut, og som inneholder bestillingsseddel. Abonnement på «vaskesedler» er gratis.

CompLex 1/81

Johs Hansen

Et edb-system for analyse av rettslige avgjørelser

64 kr

CompLex 2/81

Johs Hansen (red)

Notater om deontiske systemer

47 kr

CompLex 3/81

Vidar Sørensen

Informasjonssystem mm for Norges Geotekniske Institutt

83 kr

CompLex 4/81

Kjetil Johnsen

Systemtekniske konsekvenser av persondatalovgivningen

111 kr

CompLex 5/81

Marit Thorvaldsen

Teledata og rettsinformasjon

65 kr

CompLex 6/81

Anne Kirsti Brække

Postmonopolet

27 kr

CompLex 7/81

Knut S Selmer (ed)

The LAWDATA Papers

28 kr

- CompLex 1/82
 Norsk forening for jus og edb & Svenska föreningen för adb och juridik
Nordiske personregisterlover,
Council of Europe Convention og OECD Guidelines 31,50 kr
- CompLex 2/82
 Harald Brænd og Vidar Sørensen
Oljevern: Brukerbehov og kildemateriale 55 kr
- CompLex 3/82
 Jon Bing og Dag Frøystad
Rettskildebruk 90 kr
- CompLex 4/82
 Thomas Prebensen Steen
Post- og televerkets regulerte ansvar 77 kr
- CompLex 5/82
 Datatilsynet
Årsmelding 1981 44 kr
- CompLex 6/82
 Birger Eckhoff
 in cooperation with Jon Bing, Dag Frøystad and Anja Oskamp
CATTS: Computerized program for teaching text retrieval systems 61 kr
- CompLex 7/82
 Jon Bing
Informasjonssystemer for Trygderettens kjennelser 126 kr
- CompLex 8/82
 de Mulder, Oskamp, van der Heyden and Gubby
Sentencing by Computer: An Experiment 123 kr
- CompLex 9/82
 Colin Tapper
An Experiment in the Use of Citation Vectors in the Area of Legal Data 56 kr
- CompLex 1/83
 Arve Føyen
Utredning om endringer i pensjonregisterloven 70 kr

CompLex 2/83 Stein Schjølberg <i>Computers and Penal Legislation</i>	140 kr
CompLex 3/83 John S Gulbrandsen og Terje Hoffmann <i>Rettigheter i idrettsarrangementer</i>	64 kr
CompLex 4/83 Sally Moon and Anja Oskamp <i>The Law of Legal Information Systems: Two Essays</i>	95 kr
CompLex 5/83 Datatilsynet <i>Årsmelding 1982</i>	utsolgt
CompLex 6/83 Olav Torvund <i>Betalingsformidling</i>	146 kr
CompLex 7/83 Else Ryen <i>Lov og lovmottaker</i>	103 kr
CompLex 8/83 Daniel Stripinis <i>Probability Theory and Circumsantial Evidence</i>	23 kr
CompLex 9/83 Frede Cappelen <i>Edb-basert informasjonssystem for forvaltningens praksis</i>	36 kr
CompLex 10/83 NORDIPRO <i>Legal Acceptance of international Trade Data</i>	utsolgt
CompLex 11/83 Jørgen Hafstad og Thomas Prebensen Steen <i>Teleksrett og merverdiavgift på programvare</i>	42 kr
CompLex 12/83 Kristin Kjelland-Mørdre <i>Om forenkling av regler</i>	utsolgt

CompLex 13/83 Jon Bing <i>Edb: Mulighet og problem ved forenkling av regelverk</i>	92 kr
CompLex 14/83 Tarjei Stensaasen <i>Utvalgte emner i jus og edb (3. utgave)</i>	190 kr
CompLex 15/83 Anette Klafstad og Ulf Alex Samer <i>Plan for et forsikringsrettslig informasjonssystem</i>	60 kr
CompLex 1/84 Jon Erling Skjørshammer <i>Kabelnett: Bygnings- og ekspropriasjonslov</i>	utsolgt
CompLex 2/84 Tore Andreas Hauglie og Dag Wiese Schartum <i>Forslag til et helserettslig informasjonssystem</i>	120 kr
CompLex 3/84 Justisdepartementet <i>Den elektroniske grunnbok</i>	utsolgt
CompLex 4/84 Datatilsynet <i>Årsmelding 1983</i>	utsolgt
CompLex 5/84 Tove Fjeldvig <i>Tekstsøking: Teori, metoder og systemer</i>	90 kr
CompLex 6/84 Jon Bing <i>Offentlighetsloven og edb</i>	94 kr
CompLex 7/84 Gunnar Bach, Beate Jacobsen and Vidar Stensland <i>The National Social Insurance System of Norway</i>	51 kr
CompLex 8/84 Dag Frøystad <i>Data Protection in Practice I: Identifying and Matching Elements</i>	80 kr

CompLex 9/84 Tove Fjeldvig og Anne Golden <i>Automatisk rotlematisering - et lingvistisk hjelpemiddel for tekstsøking</i>	90 kr
CompLex 10/84 Elling Øyehaug Ose <i>Retstidene som informasjonssystem</i>	120 kr
CompLex 1/85 Jon Bing <i>Data Protection in Practise II: International Service Bueraux and Transnational Data Flow</i>	47 kr
CompLex 2/85 Jon Bing <i>Opphavsrett og edb</i>	176 kr
CompLex 3/85 Dag Wiese Schartum <i>Codex, Calculation and Computers</i>	utsolgt
CompLex 4/85 Olav Torvund <i>To informasjonsrettslige arbeider</i>	52 kr
CompLex 5/85 Datatilsynet <i>Årsmelding 1984</i>	utsolgt
CompLex 6/85 Hans Chr Aakre (red) <i>Utvalgte artikler i rettsinformatikk</i>	utsolgt
CompLex 7/85 Johannes Hansen <i>SARA: Brukerveiledning og programdokumentasjon</i>	150 kr
CompLex 8/85 Johannes Hansen <i>Modelling Knowledge, Action, Logic and Norms</i>	90 kr

CompLex 9/85 Thomas Prebensen Steen (red) <i>Kompendium i informasjonsrett</i>	utsolgt
CompLex 10/85 Tarjei Stensaasen <i>Opphavsrettslovens § 43 («katalogregelen»)</i>	97 kr
CompLex 11/85 Jon Bing <i>Straffelovens definisjon av «trykt skrift» anvendt på datamaskinbaserte informasjonssystemer</i>	65 kr
CompLex 12/85 Magnus Stray Vyrje <i>Vanhjemmel, opphavsrett og datamaskinprogrammer</i>	161 kr
CompLex 1/86 Anne Kirsti Brække <i>Formidlingsplikt for kabeleier</i>	80 kr
CompLex 2/86 Dag Wiese Schartum <i>Stans av edb-tjenester i krigs- og krisesituasjoner</i>	80 kr
CompLex 3/86 Ingvild Mestad <i>«Elektroniske spor» - nye perspektiv på personvernet</i>	100 kr
CompLex 4/86 Jon Skjørshammer <i>Opphavsrett, databaser og datamaskinprogrammer: Kontraktrettslige aspekter</i>	205 kr
CompLex 5/86 Datatilsynet <i>Årsmelding 1985</i>	73 kr
CompLex 6/86 Johannes Hansen <i>Simulation and automation of legal decisions</i>	132 kr

- CompLex 7/86
Stein Schjølberg
Datakriminalitet og forsikring 54 kr
- CompLex 8/86
Thomas Prebensen Steen (red)
Kompendium i informasjonsrett (2.utg) 70 kr
- CompLex 9/86
Peter Blume
Edb-retlige foredrag 77 kr
- CompLex 1/87
Joseph A Cannataci
*Privacy and data protection law:
International Development and Maltese Perspectives* 170 kr
- CompLex 2/87
Jon Bing og Jon Bonnevie Høyer
Publisering av rettsavgjørelser 170 kr
- CompLex 3/87
Hagen Kuehn
*The Social Security System in the
Federal Republic of Germany* 77 kr
- CompLex 4/87
Hanne Plathe Maartmann
Personvern i sykepengerutinen 70 kr
- CompLex 6/87
Jon Bing
*Electronic Publishing:
Data Bases and Computer Programs* 55 kr
- CompLex 7/87
Ånde Somby
*Selektiv gjenfinning av bestemmelser i
bygningslovgivningen* 119 kr

- CompLex 8/87
Jon Bing
FOKUS:
Knowledge based systems for public administration 125 kr
- CompLex 9/87
Dag Wiese Schartum
The introduction of computers in the Norwegian local insurance offices 230 kr
- CompLex 10/87
Knut Kaspersen
Kredittopplysning 75 kr
- CompLex 11/87
Ernst Buchberger, Bo Göranzon and Kristen Nygaard (ed)
Artificial Intelligence: Perspectives and Implications 120 kr
- CompLex 12/87
Jon Bing, Kristine M Madsen og Kjell Myrland
Strafferettslig vern av materielle goder 118 kr
- CompLex 13/87
Tove Fjeldvig
Effektivisering av tekstsøkesystemer: Utvikling av språkbaserte metoder 175 kr
- CompLex 14/87
Jon Bing
Journalister, aviser og databaser 66 kr
- CompLex 15/87
Andreas Galtung
Skatterettslig ekspertsystem: Et eksempel basert på skattelovens § 77 82 kr
- CompLex 1/88
Robin Thrapp-Meyer
Uvalgte emner i rettsinformatikk (4. utgave) 228 kr

CompLex 2/88 Ernst Buchberger, Bo Göranson and Kristen Nygaard (ed) <i>Artificial Intelligence: Perspectives of AI as a social technology</i>	178 kr
CompLex 3/88 Jon Bing og Anne Kirsti Brække <i>Satellittfjernsyn</i>	128 kr
CompLex 4/88 Jon Bing <i>Journalists, Databases and Newspapers</i>	68 kr
CompLex 5/88 Joseph Cannataci <i>Liability and responsibility for expert systems</i>	108 kr
CompLex 6/88 Datatilsynet <i>Årsmelding 1987</i>	58 kr
CompLex 7/88 Henrik Sinding-Larsen (ed) <i>Artificial Intelligence and Language</i> Old questions in a new key	295 kr
CompLex 8/88 Jon Bing Database for offentlige publikasjoner (DOP): Fremtidig organisering NORIS (87)	178 kr
CompLex 9/88 Jon Bing Conceptual Text Retrieval NORIS (77)	98 kr
CompLex 11/88 Ingvild Mestad L' Informatique, la Liberté Individuelle et la Recherche Epidémiologique Data Protection and Epideminologic Research	98 kr

Fremtidige utgivelser i skriftserien CompLex

Nedenfor følger omtale av CompLex-utgivelser som vil foreligge i nærmeste fremtid. De kjøpes/bestilles på samme måte som for tidligere utgitte nummer i serien – se foran og kupongen bakerst.

CompLex 13/88

Henning Herrestad & Dag Syvert Mæsel (eds)

**FIVE ARTICLES ON ARTIFICIAL INTELLIGENCE AND LEGAL EXPERT SYSTEMS
NORIS (83) F KUS**

This compendium comprises five articles on legal expert systems and artificial intelligence.

The first three articles present three different legal expert systems, demonstrating the wide range of different motives, research interests and approaches to making legal expert systems.

The fourth article focuses on the question of how to make formal representations of law.

The fifth article presents more visionary ideas concerning how artificial intelligence research could be used as an instrument in reducing international tension.

The compendium originates from a roundtrip made by the editors to six different institutes situated in the Netherlands, West-Germany and Austria. Three of the institutes are doing research especially on legal expert systems, the other three on various aspects within the field of artificial intelligence. In their introduction the editors have summed up their impressions and thoughts after these visits.

100 sider. Pris kr 108,-.



COMPLEX

Bestillingskupong

Ja takk, vi bestiller herved følgende eks.
av COMPLEX:

.....eks. av nr..... à kr

.....eks. av nr..... à kr

.....eks. av nr..... à kr

.....eks. av nr..... à kr

Av fremtidige COMPLEX utgivelser (se omtale foregående sider)
bestilles herved:

.....eks. av nr..... à kr

.....eks. av nr..... à kr

Navn:.....

Firma:.....

Adresse:.....

Postnr./sted:.....

Kupongen sendes til:

Akademika
INTERNASJONAL FAGBOKHANDEL

Karl Johansgt. 47
0162 Oslo 1







Bull



GRENSELØS DATAKOMMUNIKASJON

Honeywell Bull A/S,
Tollbugata 32, Postboks 470 Sentrum, 0105 Oslo 1,
Telefon (02) 41 80 30.

SIKRING AV PERSONREGISTRE

Personvern karakteriseres gjerne som den interesse den enkelte har i å kontrollere bruk og lagring av opplysninger som angår vedkommende selv. Et ledd i en slik kontroll, vil være sikkerhet med uautorisert aksess, tilfeldig sletting eller forvanskning av data, ukontrollert spredning av data osv – elementer som gjerne samles under betegnelsen «datasikkerhet».

Personregisterloven har i § 8b en generell hjemmel for utferdigelse av «regler for sikring av personopplysninger». I april 1986 nedsatte Justisdepartementet en arbeidsgruppe for å utforme sikkerhetsforskrifter. Forut for dette arbeidet hadde imidlertid Institutt for rettsinformatikk – under ledelse av Datatilsynets spesialrådgiver i edb, Johs Hansen – trukket i gang et prosjekt som tok sikte på å utforme prinsipper for sikring av personverninteresser, foretak og edb-anlegg. Den foreløbige rapporten ble lagt til grunn for arbeidsgruppens vurderinger, og danner på mange måter et forarbeid til det utkast til forskrifter som nå foreligger.

Rapporten har en analytisk innfallsvinkel. Den omfatter bl a en diskusjon av risikoanalyse av anlegg og foretak som behandler personregistre, en sikkerhetsmodell bygd på ressursbegrepet, en vurdering av sensitivitet og sårbarhet som fører frem til en sensitivitetsmodell, og en diskusjon av hva som ligger i «informasjons-sikkerhet». I oppsummeringen drøftes sentrale spørsmål for utforming og administrasjon av sikkerhetsforskriften.

Rapporten fra Justisdepartementets arbeidsgruppe med utkast til forskrift for sikring av personregistre følger som vedlegg.

ISBN 82-518-2596-2



ISBN 82-518-2596-2

