Datatilsynet

Endelig kontrollrapport		
Saksnummer: 07/01455 Dato for kontroll: 13. november 2007 Rapportdato: 25. januar 2008	Kontrollobjekt: Justis- og politidepartementet, Kriminalomsorgsavdelingen Sted: Ila Landsfengsel	Utarbeidet av: Helge Veum, senioringeniør Cecilie L. B. Rønnevik, seniorrådgiver

1 Innledning og kort oppsummering

Datatilsynet gjennomførte kontroll hos Justis- og politidepartementets Kriminalomsorgsavdeling (Kriminalomsorgens sentralforvaltning - KSF) den 13. november 2007. Kontrollen ble gjennomført i medhold av personopplysningslovens § 44, jf. § 42, 3. ledd nr 3.

Temaet for kontrollen var behandling av personopplysninger om innsatte ved norske fengsler, særlig i det elektroniske informasjonssystemet Kompis. Kontrollen ble gjennomført ved Ila Landsfengsel og sikringsanstalt.

I foreliggende rapport vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Datatilsynets funn kan kort oppsummeres slik:

- Det foreligger et *uoffisielt og ukontrollert personregister* ved Ila (”innsatt pr nummer”), inneholdende svært sensitive personopplysninger, jf pkt 5 og 6.1

- Den behandling av personopplysninger som skjer i fagsystemet Kompis *mangler et rettslig grunnlag*, i form av en lovhjemmel, pkt 6.3

- Etter Datatilsynets vurdering *ivaretar ikke KSF de registrerte grunnleggende rettigheter* etter personopplysningsloven, med hensyn til innsyn, retting og sletting, pkt 6.5

- KSF har *ikke etablert et internkontrollsystem* for å sikre at behandlingen av personopplysninger skjer i henhold til lovgivningen, pkt 6.6

- KSF har *ikke foretatt relevante risikovurderinger* av behandlingen, pkt 6.9

- KSF har *ikke sørget for tilfredsstillende informasjonssikkerhet*, særlig med tanke på konfidensialitet, pkt 6.8

- KSF har etter Datatilsynets vurdering *gitt tilsynet mangelfull og feilaktig informasjon* på vesentlige punkter pkt 6.10

- *Justisdepartementets Kriminalomsorgsavdeling anbefales å delegere bort ansvaret* for etterlevelsen av personopplysningsloven

Datatilsynet vurderer at de funnene som blir beskrevet i denne rapporten er alvorlige. Den behandlingen av sensitive personopplysninger som skjer innen Kriminalomsorgen ivaretar på ingen måte de grunnleggende lovkrav til beskyttelse av den enkeltes personlige integritet.

Datatilsynet er av den oppfatning at det er spesielt utilfredsstillende at denne type alvorlige mangler foreligger i tilknytning til myndighetenes gjennomføring av frihetsberøvelse og tvangstiltak ovenfor enkeltpersoner. Tilsynet vil presisere at en dom på frihetsberøvelse ikke innebærer at man samtidig fradømmes andre grunnleggende menneskerettigheter, som retten til et privatliv under og etter soning. Tvert imot tilsier den registrertes situasjon som innsatt at myndighetenes behandling av vedkommende bør være underlagt en god og demokratisk kontroll.

Datatilsynet finner det særlig bekymringsfullt at ansvaret for de manglene som er avdekket, kan tilbakeføres til Justis- og politidepartementet. Det vises her både til at det er Justis- og politidepartement som er tillagt oppgaven med å sikre den enkelte borgers rettsikkerhet i justissektoren, og at vedkommende departement også er fagdepartement med forvaltningsansvaret for nettopp personopplysningsloven.

2 Tilstede under kontrollen

2.1 Fra behandlingsansvarlig:

- Unni Gunnes, fungerende ekspedisjonssjef, Justis- og politidepartementet
- Per E. Schwab, seniorrådgiver, Kriminalomsorgens sentralforvaltning
- Bjørn Holstad, direktør, Kriminalomsorgens it-tjeneste (KITT)
- Karin Kristiansen, seniorrådgiver, Kriminalomsorgens it-tjeneste
- Stein Nilsen, fungerende assisterende regionsdirektør
- John Juklerød, fengselsinspektør, Ila fengsel
- Ola Seeberg, it-driftsansvarlig, Ila fengsel
- Per Næss, avdelingsleder, Ila fengsel
- Vidar Elvsaas, rådgiver, Ila fengsel
- Trine Nordseth, konsulent, Ila fengsel
- Kine Traa, konsulent, Ila fengsel

Deltagerne var tilstede på ulike deler av kontrollen.

2.2 Fra Datatilsynet:

- Helge Veum, senioringeniør, Tilsyns- og sikkerhetsavdelingen
- Cecilie L. B. Rønnevik, seniorrådgiver, Juridisk avdeling

3 Kort om bakgrunnen for Datatilsynets kontroll

Kompis er et elektronisk informasjonssystem som ble innført ved alle landets fengsler i 1992. Systemet ble gitt konsesjon fra Datatilsynet i henhold til personregisterloven

av 1978. Da personopplysningsloven erstattet personregisterloven i 2001 falt denne konsesjonen bort. I brev av 2. desember 2002 og 20. desember 2002 ble det søkt om nye konsesjoner for behandlingen i henhold til personopplysningslovens bestemmelser (Dt 2002/2186-1 og 2003/49-1). Datatilsynet fant at behandlingen var unntatt fra konsesjonsplikt etter personopplysningslovens § 33 fjerde ledd, men presiserte at personopplysningslovens øvrige bestemmelser uansett fikk anvendelse ved den aktuelle behandlingen (Dt 2002/2186-9 og 2003/49-5).

I brev av 24. juni 2005 ba KSF om at Datatilsynet vurderte hvorvidt registreringen i Kompis kunne utvides, uten at det derved oppstod konsesjonsplikt. Det ble i den forbindelse avholdt et møte mellom Datatilsynet og KSF. I brev av 9. november 2005 redegjorde Datatilsynet for de grunnkrav som personopplysningsloven oppstiller, og ba om at KSF vurderte sin behandling i forhold til lovens krav. Herunder ble det pekt spesielt på lovens krav til behandlingsgrunnlag, og bestemmelser om sletteplikt og informasjonsplikt.

Datatilsynet har mottatt flere klager fra innsatte ved Ila fengsel. Mer konkret er det klaget på at den tilgangen som de ansatte har til personopplysningene om de innsatte, både ved denne konkrete anstalten og ved andre anstalter, er for vid. I brev av 13. november 2006 ba Datatilsynet derfor om en redegjørelse fra KSF, for den behandling av personopplysninger som finner sted i fengselsvesenet, særlig i Kompis (Dt 06/01209-3). Den 15. desember 2006 oversendt KSF sin redegjørelse.

I brev av 21. september 2007 varslet Datatilsynet KSF om at behandlingen ville bli gjenstand for en stedlig kontroll (Dt 07/01455-1).

4 Kort om bruk av personopplysninger i Kompis, samt formålet med behandlingene

I informasjonssystemet Kompis behandles en rekke personopplysninger. Formålet med behandlingen er ”gjennom en god saksbehandling å oppfylle straffegjennomføringslovens formål om å motvirke nye straffbare forhold og for å være betryggende for samfunnet”, jf KSF sitt brev av 24. juni 2005.

4.1 Opplysninger om innsatte

I informasjonssystemet Kompis behandles følgende opplysninger om de innsatte:

- Navn
- Alias/tidligere navn
- Fødselsnummer
- Kjønn
- Folkeregistrert adresse
- Utenlands adresse/poste restante adresse
- Fødested/land

- Statsborgerskap
- Innsattnummer
- Innsattkategori (varetekt, sikring, forvaring, bøtesoning med mer)
- Yrkessituasjon
- Sivilstatus
- Bidragsplikt
- Språk
- Plassering i anstalten
- Status for soningen (sykehus, lukket avdeling, åpen avdeling, behandlingsinstitusjon)
- Utdrag fra dom
- Opplysninger om "hendelser", for eksempel
  - at det er skrevet en miljørapport,
  - at det er søkt om permisjon,
  - at det er gitt disiplinærreaksjon,
  - at det er tatt blod- eller urinprøver, og hvilket resultat prøven ga,
  - at vedkommende har hatt permisjon,
  - at vedkommende har hatt besøk,
  - osv.

Listen er ikke uttømmende. Det vises blant annet til at det finnes fritekstområder, uten at det er implementert rutiner for hvilke opplysninger som kan registreres der.

Saksdokumentene, fra for eksempel permisjonssøknader og lignende, ligger ikke tilgjengelig i Kompis, men legges i den manuelle/papirbaserte saksmappen for den enkelte innsatte.

Under intervju med ansatte ved Ila fengsel fremkom det at man også leverte ut opplysninger til politiet, i forbindelse med etterforskning av straffbare forhold. Som eksempel ble det nevnt at den lokale politimyndighet ringer og ber om å få opplysninger om hvilke innsatte som har hatt permisjon på et bestemt tidspunkt, i forbindelse med at det er begått et lovbrudd i området.

4.2 Opplysninger om pårørende og besøkende

For samme formål behandles følgende opplysninger:

- Om pårørende
  - navn og kontaktopplysninger

- Om besøkende
  - navn på personer som kan komme på besøk, iflg vedtak

Navn på tredjepersoner er ikke søkbare.

5 Kort om personregisteret ”Innsatt pr nummer”

Under tilsynets samtaler med de ansatte ved Ila fremkom det at de saksdokumentene som produseres i programmet Word, på den enkelte ansattes hjemmeområde, også lagres elektronisk i en mappe på fellesområdet (F:/innsatt pr nummer).

Her lagres alle saksdokumentene som produseres om den enkelte innsatte, så som psykiatriske vurderinger, miljørapporter, vedtak om for eksempel permisjon, besøk osv. Opplysningene som fremkommer her er således mer detaljerte og av mer sensitiv karakter enn de opplysningene som ligger i Kompis. Det vises til at man her legger fulltekstutgaver av blant annet psykiatriske vurderinger.

Selve det formelle saksdokumentet, i form av en signert utskrift, legges i den enkelte innsattes manuelle saksmappe i anstaltens arkiv.

De ansatte ved anstalten forklarte at det var ”innsatt pr nummer” som ble brukt i den daglige saksbehandlingen rundt de innsatte. Kompis gir ikke tilgang på selve saksdokumentene, og det ble ansett å være for tungvint å hente frem den manuelle saksmappen hver gang man skulle fatte et vedtak. Registeret fungerer med andre ord som et saksbehandlingssystem, slik at man også la til grunn opplysningene i de dokumentene som allerede lå der i den videre saksbehandlingen av den enkelte innsatte. Dette til tross for at opplysningene ikke var sikret integritet.

Registeret ligger plassert på det øverste mappenivået på fellesområdet. Det innebærer at alle med tilgang til felleområdet har ubegrenset tilgang til de opplysningene som ligger der.

6 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

6.1 Spesielt om ”Innsatt per nummer”

Etter det Datatilsynet erfarte er ikke registeret forankret i den behandlingsansvarliges ledelse, men har ”vokst frem” ved institusjonen. Registeret er således å anse både som uoffisielt og ukontrollert.

At det ikke finnes noen dokumentasjon knyttet til behandlingen av opplysningene i registeret vanskeliggjorde også Datatilsynets kontroll av behandlingen, i henhold til de konkrete krav som personopplysningslovens oppstiller. Tilsynet kan ikke annet enn å konkludere med at hele registeret som sådan er ulovlig. Tilsynet vil peke spesielt på det alvorlige i at hensynet til konfidensialitet og integritet ikke er ivaretatt på en tilfredsstillende måte.

Datatilsynet reagerer sterkt på at registeret har blitt etablert og eksistert i en årrekke, tilsynelatende uten at det har blitt oppdaget av KSF. Etter tilsynets vurdering vitner dette om mangel på kontroll på den behandling av personopplysninger som finner sted ved anstalten.

Ettersom registeret "innsatt pr nummer" har vokst frem som følge av manglende saksbehandlingsfunksjonalitet i Kompis, er det tvingende nødvendig at KSF straks foretar undersøkelser ved de andre anstaltene hvor manglende saksbehandlingssystem kan ha ført til fremveksten av lignende registre, og eventuelt sørger for å ta kontroll på disse registrene.

Datatilsynet ser også alvorlig på at registeret fremstod uten informasjonssikkerhet med hensyn til integritet, samtidig som opplysningene i registeret blir benyttet som beslutningsgrunnlag når det fattes vedtak rettet mot de innsatte.

Praksisen med registeret "innsatt per nummer" ses som et brudd på personopplysningslovens § 13 om informasjonssikkerhet og § 14 om internkontroll.

6.2 Behandlingsansvar

I henhold til personopplysningslovens § 2 nr 4 ligger behandlingsansvaret hos "den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes".

Behandlingsansvaret for behandling av personopplysninger om innsatte i fengselsvesenet er i dag plassert i Justisdepartementets Kriminalomsorgsavdeling (KSF). Det vises i den forbindelse til KSF sine konsesjonssøknader av 2. og 20. desember 2002.

Datatilsynet vil generelt bemerke at behandlingsansvaret erfaringsvis ivaretas best når ansvaret plasseres i relativt nær tilknytning til selve behandlingen av personopplysningene. Når behandlingsansvaret plasseres fjernt fra selve behandlingen vil det måtte gjøres omfattende delegeringer. Det vil derfor lett oppstå uklare ansvars- og myndighetsforhold. I tillegg blir den behandlingsansvarliges løpende kontroll med at behandlingen skjer i henhold til lovens bestemmelser vanskeliggjort.

Datatilsynet vil bemerke at det å legge behandlingsansvaret på departements- eller direktoratsnivå, for den behandling som skjer lokalt ved det enkelte fengsel, ikke er å anbefale. Datatilsynet pekte på dagens plassering av behandlingsansvaret som et mulig problem allerede i sitt brev av 16. februar 2004 (Dt 2003/49-4 og 2002/2186-9), men kan ikke se at dette ble fulgt opp fra departementets side.

Foreliggende kontrollrapport viser alvorlige mangler knyttet til departementets ivaretakelse av behandlingsansvaret. Tilsynet vil derfor anbefale at plasseringen av behandlingsansvaret snarest revurderes.

Datatilsynet vil i den forbindelse peke på straffegjennomføringslovens § 6, hvoretter beslutninger etter straffegjennomføringsloven som hovedregel skal treffes på lokalt eller regionalt nivå.

6.3 Behandlingsgrunnlag

I henhold til personopplysningslovens § 11 litra a plikter den behandlingsansvarlige å sørge for at det behandles personopplysninger bare når det er tillatt etter §§ 8 og 9. Da det i dette tilfellet behandles sensitive personopplysninger kommer de skjerpede kravene i personopplysningslovens § 9 til anvendelse.

6.3.1 Nærmere om lovens krav til behandlingsgrunnlag - legalitetsprinsippet

Datatilsynet anser at den registreringen som skjer i Kompis er svært inngripende. Det vises både til at det registreres opplysninger som er klart sensitive i personopplysningslovens forstand, og at registreringen er av et slikt omfang at den innebærer en omfattende kartlegging av den enkelte innsattes liv ved anstalten.

Tilsynet vil i tillegg peke på at den registrerte i dette tilfellet befinner seg i en tvangssituasjon, og at det derfor er særlig viktig å sikre at vedkommendes integritet ivaretas under oppholdet.

Med bakgrunn i legalitetsprinsippet må det etter dette stilles svært strenge krav til behandlingsgrunnlaget. Etter Datatilsynets vurdering vil det derfor være helt nødvendig med en klar lovhjemmel, jf § 9 litra b, for den behandling av personopplysninger som finner sted i Kompis. Ettersom Kompis i tillegg er et nasjonalt register, er Datatilsynet av den oppfatning av det er påkrevd med egen lovregulering, en såkalt registerlov.

6.3.2 Nærmere om straffegjennomføringsloven som behandlingsgrunnlag

I forbindelse med konsesjonssøknadene fra KSF er det anført at behandlingen er hjemlet i straffegjennomføringsloven med forskrifter.

Etter Datatilsynets vurdering gir ikke straffegjennomføringsloven tilstrekkelig klar hjemmel for den behandlingen av opplysninger som finner sted i Kompis, utover den behandling av personopplysninger som skjer i forbindelse med KSFs saksbehandling. Tilsynet kan ikke se at hjemlene gir tilstrekkelig klarhet i forhold til hvilke opplysninger som kan behandles, til hvilket formål og hvordan behandlingen for øvrig skal skje.

Det at behandlingen av opplysningene er en nødvendig forutsetning for at kriminalomsorgen skal gjennomføre sine øvrige plikter, tilfredsstiller etter Datatilsynets vurdering ikke kravet til lovhjemlet behandling etter personopplysningslovens § 9 litra b.

Det vises for øvrig til Datatilsynets vurderinger vedrørende konsesjonsplikten, pkt 6.4.

6.3.3 Kort om Datatilsynets brev av 9. november 2005

I Datatilsynets brev av 9. november 2005 er behandlingsgrunnlaget vurdert, i forhold til spørsmålet om utvidet registrering i Kompis. Tilsynet konkluderte med at utvidelsene ikke vil kunne hjemles i straffegjennomføringsloven, og ba om at departementet vurderte alternative behandlingsgrunnlag.

Datatilsynet vil bemerke at det er den behandlingsansvarlige som etter personopplysningsloven bærer det endelige ansvaret for å påse at man har et gyldig behandlingsgrunnlag for den behandlingen man forestår. Det er den behandlingsansvarige selv som presumptivt har størst kunnskap både om eget regelverk og om egne behandlinger, og som derfor er nærmest til å foreta denne vurderingen.

Uansett er spørsmålet om KSFs eventuelle gode tro vedrørende dette helt uten betydning ved vurderingen av om det pr i dag foreligger et behandlingsgrunnlag eller ikke.

6.3.4 Konklusjon

Datatilsynet kan ikke se at det foreligger et gyldig behandlingsgrunnlag for den behandling av personopplysninger som finner sted i Kompis. Dette er å anse som et brudd på personopplysningslovens § 11 litra a.

6.4 Konsesjonsplikt

I henhold til personopplysningslovens § 33 foreligger det som hovedregel konsesjonsplikt for elektronisk behandling av sensitive personopplysninger.

Det ble søkt om konsesjon for Kompis i henhold til personopplysningsloven den 20. desember 2002 (Dt. 2003/49). Datatilsynet vurderte at behandlingen var unntatt fra konsesjonsplikt etter § 33 fjerde ledd, hvoretter konsesjonsplikten ikke gjelder for behandling i organ for stat eller kommune når behandlingen har hjemmel i egen lov. Det vises til Datatilsynets vedtak av 16. februar 2004.

Datatilsynet har foretatt en ny vurdering, og finner at unntakshjemmelen i § 33 fjerde ledd ikke kommer til anvendelse på behandlingen. Datatilsynet kan ikke se at straffegjennomføringsloven i tilstrekkelig grad regulerer den behandlingen som finner sted. Det at behandlingen følger forutsetningsvis vil ikke være tilstrekkelig til å unnta behandlingen fra konsesjonsplikt. Det vises i den forbindelse til Ot prp nr 92, side 129:

"For at et personregister skal være fritatt fra konsesjon i medhold av denne bestemmelsen, kreves det at det eksplisitt fremgår av loven at det skal eller kan føres et register. Det er ikke tilstrekkelig at en særlov hjemler en aktivitet som gjør opprettelsen av et personregister nødvendig."

Bakgrunnen for nevnte unntak er at lovgivende myndigheter, i forbindelse med lovarbeidet, allerede har foretatt de vurderingene som Datatilsynet ville ha gjort i forbindelse med en konsesjonsbehandling.

I henhold til legalitetsprinsippet vil hjemmelskravet være avhengig av behandlingens inngripende karakter. Når behandlingen har en så inngripende karakter som i foreliggende tilfelle må det, etter tilsynets vurdering, være klart at straffegjennomføringsloven ikke i tilstrekkelig grad regulerer behandlingen, slik at den derfor skal unntas fra Datatilsynets konsesjonsbehandling. Det vises her til at loven ikke uttrykkelig gir anvisning på verken at det skal eller kan opprettes et register, hvilket formål et slikt register skal ha, hvilke opplysninger som skal behandles, med mer.

Med bakgrunn i det ovennevnte finner Datatilsynet at det er grunnlag for å gjøre om tilsynets vedtak av 16. februar 2004. Datatilsynet viser i den forbindelse til forvaltningslovens § 35 siste ledd, jf alminnelige forvaltningsrettslige regler, hvoretter et gyldig vedtak kan omgjøres etter en avveining mellom partens interesser i at vedtaket ikke omgjøres og samfunnets interesse i at vedtaket omgjøres. Datatilsynet vurderer i dette tilfellet at samfunnets interesse i at Datatilsynet konsesjonsbehandler KSFs behandling klart overstiger KSFs interesse i å unngå en konsesjonsbehandling.

Datatilsynets finner at det foreligger konsesjonsplikt etter personopplysningslovens § 33.

Det bemerkes imidlertid at Datatilsynet prinsipalt anser at behandlingen må lovhjemles, jf pkt 6.3. Dersom en lovhjemmel etableres vil konsesjonsplikten falle bort.

6.5 Ivaretakelse av de registrertes rettigheter

6.5.1 Informasjonsplikt

I henhold til personopplysningslovens §§ 19 og 20 plikter den behandlingsansvarlige å gi den registrerte informasjon som setter vedkommende i stand til å ivareta egne rettigheter som registrert. I de tilfeller hvor opplysningene hentes fra den registrerte selv, skal informasjonen gis før behandlingen tar til.

De klagene som tilsynet har fått fra innsatte viser at det faktisk finnes kunnskap blant de innsatte om at Kompis eksisterer. Datatilsynets kontroll avdekket imidlertid at det ikke systematisk gis informasjon, verken til de innsatte eller til andre registrerte (herunder barn, pårørende og besøkende) om den registreringen som finner sted i Kompis og hvilke rettigheter vedkommende har i den forbindelse. Hvilken kunnskap som finnes hos de registrerte synes derfor å bero på tilfeldigheter.

Tilsynet kan forøvrig ikke se at KSF har vurdert hvilke unntaksbestemmelser som eventuelt kommer til anvendelse i dette tilfellet, jf personopplysningslovens § 23.

Datatilsynets anser at dette representerer et brudd på opplysningsplikten i personopplysningslovens § 19 og 20.

6.5.2 Rett til innsyn

I henhold til personopplysningslovens § 18 annet ledd har den registrerte rett til innsyn i hvilke opplysningene om den registrete som behandles, og sikkerhetstiltakene rundt disse.

Det er utarbeidet retningslinjer for innsynsretten, både i departementets rundskriv av 2000 (G-111/2000) om journalføring og registrering i Kompis § 6 og i Kriminalomsorgens "Retningslinjer for innsattes rett til innsyn i anstaltens saksdokumenter".

Datatilsynet vil bemerke at disse retningslinjene tar utgangspunkt i den innsynsretten som en part har i henhold til forvaltningslovens §§ 18 og 19. Den innsynsretten som følger av personopplysningsloven er imidlertid ikke regulert. Det skal i den forbindelse bemerke at den innsynsretten som følger av forvaltningsloven er langt snevrere enn den som følger av personopplysningsloven. Det vises her til at innsynsretten etter forvaltningsloven kun regulerer den adgangen en "part" har til å få innsyn i (forvaltnings)"sakens dokumenter".

Datatilsynet anser at nevnte begrensninger i innsynsretten innebærer et brudd på personopplysningslovens § 18, både i forhold til personopplysninger som ikke er å anse som saksdokumenter, og for personer som ikke er å anse som en part - herunder pårørende, barn og besøkende.

6.5.3 Sletting

I henhold til personopplysningslovens § 28 skal personopplysninger ikke lagres lenger enn det som er nødvendig for formålet med behandlingen. Opplysningene skal da slettes, med mindre det foreligger lovpålagt lagringsplikt etter for eksempel arkivloven.

Under kontrollen fremkom det at det ikke på noe tidspunkt slettes opplysninger i Kompis. KSF viste til at riksarkivaren har uttalt at opplysningene i Kompis er å anse som arkivverdige, og således skal oppbevares i henhold til arkivlovens bestemmelser.

Datatilsynet vil bemerke at oppbevaring i henhold til arkivloven er et eget behandlingsformål. Tilsynet kan ikke se at arkivering har vært fremme i forbindelse med KSFs redegjørelse for formålet med Kompis. For eksempel er ikke arkivloven nevnt som et behandlingsgrunnlag i forbindelse med konsesjonssøknadene. Tilsynet kan derfor vanskelig se at Kompis er ment å være virksomhetens arkivsystem. Etter hva Datatilsynet erfarer vil dette filsystemet heller ikke være egnet til å ivareta de krav som arkivloven oppstiller.

Det skal uansett bemerkes at arkivplikten, etter det Datatilsynet forstår, vil kunne ivaretas tilfredsstillende gjennom oppbevaring av den papirbaserte journalen.

Arkivplikten vil etter dette ikke kunne anføres som et grunnlag for ikke å slette opplysninger i Kompissystemet. Det vises for øvrig til pkt 6.8 i rapporten, om tilgangsstyring.

Det ligger utenfor Datatilsynets faktiske og formelle kompetanse å vurdere hvorvidt opplysninger er arkivverdige etter arkivloven. Tilsynet tillater seg allikevel å bemerke at man vanskelig kan se at alle de opplysningene som behandles er arkivverdige. Dette gjelder for eksempel opplysninger om hvem som har vært på besøk hos en innsatt. Tilsynet anbefaler derfor at departementet utber en redegjørelse fra Riksarkivaren, hvor arkivverdigheten vurderes konkret, på opplysningsnivå.

6.6 Internkontroll

Personopplysningslovens § 14 oppstiller krav om at den behandlingsansvarlige skal etablere planlagte og systematiske tiltak for å sikre at personopplysningslovens bestemmelser etterleves ved behandlingen (internkontroll). Utfyllede bestemmelser er gitt i personopplysningsforskriftens § 3-1.

Kravet til internkontroll i forbindelse med informasjonssikkerhet (personopplysningslovens § 13) er behandlet i rapportens pkt 6.7. I det følgende behandles virksomhetens internkontroll knyttet til ivaretakelse av lovens øvrige krav.

6.6.1 Om Kvalitetssystem for informasjonssikkerhet - KIS

Datatilsynet vurderer KIS til å være begrenset til å gjelde informasjonssikkerhet etter personopplysningslovens § 13, og er derfor nærmere behandlet i pkt 6.8.

6.6.2 Om Rundskriv G-111/2000 Om journalføring og registrering i Kompis

Enkelte rutiner for behandlingen av personopplysninger i Kompis er beskrevet i eget rundskriv fra Justis- og politidepartementet[1].

Rundskrivet er, etter det Datatilsynet kan se, utarbeidet med bakgrunn i personregisterloven av 1978, og har ikke blitt revidert i forbindelse med innføring av personopplysningsloven i 2001.

Dokumentet kan etter tilsynets vurdering uansett ikke sies å være dekkende for rutinebehovet etter personopplysningslovens § 14. Det pekes blant annet på forhold beskrevet andre steder i denne rapporten:

- Rutiner for utlevering til politiet.
  Hva gjelder rutiner for utlevering av opplysninger til politiet viser KSF til rundskriv G-3/2005. Datatilsynet registrerer at det foreligger et rundskriv, men vil bemerke at rundskrivet ikke i seg selv er å anse som en implementert rutine. Det vises forøvrig til at de ansatte som Datatilsynet

[1] Justis- og politidepartementet, "Om journalføring og registrering i Kompis KIA", rundskriv G-111/2000 Jnr.98/12110 D 006.1.H-GS/

intervjuet under kontrollen ikke kjente til hvilke bestemmelser som gjaldt for slik utlevering. Det forligger ingen dokumenterte rutiner for å sikre at det foreligger et behandlingsgrunnlag for utleveringen i det konkrete tilfellet, og for å sikre at opplysningene i så fall leveres ut til rette vedkommende.

- Rutiner for innsyn, retting og sletting.
  Det foreligger ingen dokumenterte rutiner for å sikre at de registretes rettigheter vedrørende innsyn, retting og sletting blir ivaretatt.

- Kontrollerende rutiner.
  Med bakgrunn i de funn som er gjort under kontrollen ved Ila, herunder fremvekst av registeret "innsatt per nummer" og manglende informasjonssikkerhet, anser Datatilsynet at lovpålagte rutiner for å kontrollere ivaretakelsen av personopplysningslovens bestemmelser ikke kan være implementert. Mangelen består enten i at rutinene ikke eksisterer eller ikke fungerer.

Datatilsynet vil presisere at tilsynet tidligere har påpekt lovens krav om internkontrollrutiner overfor KSF. Konkret var dette knyttet til sletting av personopplysninger, jf Datatilsynets brev av 13. november 2006. I brev til Datatilsynet, av 15. desember 2006, uttaler KSF om dette at:

"Når det gjelder forbudet mot å lagre unødvendige personopplysninger etter personopplysningslovens § 28 har kriminalomsorgen i dag ikke rutiner for hvilke personopplysninger som skal slettes. Kriminalomsorgen har derfor igangsatt et arbeide med å utarbeide og implementere en rutine for sletting av personopplysninger".

Slike rutiner var allikevel ikke etablert på tidspunktet for kontrollen, nærmere ett år senere.

6.6.3 Konklusjon

Datatilsynet anser at KSF ikke har etablert planlagte og systemtiske tiltak for i sikre at personopplysningslovens bestemmelser etterleves ved behandlingen (internkontroll).

At det ikke er etablert rutiner som loven eksplisitt stiller krav om, hele syv år etter lovens ikrafttredelse, er etter Datatilsynets vurdering svært utilfredstillende.

Datatilsynet anser det for å være skjerpende at det heller ikke ble iverksatt tiltak etter at Datatilsynet pekte på denne mangelen i 2006. Etter tilsynets vurdering kan dette tyde på manglende vilje til å etablere rutiner i samsvar med personopplysningsloven.

Forholdet anses som et brudd på personopplysningslovens § 14, jf. personopplysningsforskriftens 3. kapittel.

6.7 Systematisk tilnærming til informasjonssikkerhet

Personopplysningslovens § 13 stiller krav om den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredstillende informasjonssikkerhet.

Personopplysningsforskriftens kapittel 2 gir utfyllende bestemmelser. Her nevnes blant annet:

- § 2-3 om sikkerhetsledelse, med konkrete krav om etablerte sikkerhetsmål og strategi,
- § 2-7 om organisering, og klare ansvars- og myndighetsforhold,
- § 2-8 om personell og fastlagte rutiner,
- § 2-6 om avviksbehandling, og
- § 2-5 og sikkerhetsrevisjoner.

For sikkerhetsforhold gjelder også internkontrollplikten etter lovens § 14.

6.7.1 Om Kvalitetssystem for informasjonssikkerhet (KIS)

Etter det opplyste skal kvalitetssystemet skal være todelt, og bestå at et sentralt utarbeidet rutinesett (perm 1) og en lokal gjennomførende del (perm 2).

Under kontrollen kom det frem at det ikke var utarbeidet noen lokal del av KIS ved Ila (perm 2). Det er ikke brakt på det rene om dette er en mangel også ved andre anstalter enn Ila. Datatilsynet anser at det er tvingende nødvendig at KSF straks iverksetter undersøkelser for å kontrollere om de lokale rutinene er implementert ved landets øvrige anstalter.

Det som foreligger av sentralt utarbeidede rutiner (perm 1) kan uansett ikke ha fungert etter intensjonene. Det vises til at Ila har etablert en uregulert, lokal praksis med registeret ”innsatt per nummer”. Datatilsynet kan vanskelig se at dette registeret kunne ha oppstått, dersom de kontrollerende delen av KIS har vært gjennomført på et forsvarlig vis.

6.7.2 Konklusjon

Det ble konkret avdekket at KIS - perm 2 ikke var etablert ved Ila. Uten at de lokale delene av et kvalitetssystem følges opp, er verdien av kvalitetssystemet som sådan være svært begrenset. Datatilsynet kan ikke se at den behandlingsansvarlige har etablert planlagte og systematiske tiltak i samsvar med lovens krav.

Annet sted i rapporten pekes det på manglende risikovurdering av den behandlingen av personopplysninger som finner sted i kriminalomsorgen (pkt 6.9). Det ses også som en systemsvikt at et så konkret krav i sikkerhetsbestemmelsene, som kravet til risikovurderinger er, synes å være neglisjert.

Forholdet anses som et brudd på personopplysningslovens § 13.

6.8 Konfidensialitetssikring – tilgang og logger

I henhold til personopplysningslovens § 13 jf. personopplysningsforskriftens § 2-11 plikter den behandlingsansvarlige å sørge for tilfredsstillende konfidensialitetssikring. I praksis er dette å forstå slik at den behandlingsansvarlige plikter å sørge for at den interne tilgangen til opplysningene skal gis i samsvar med den ansattes tjenstlige behov.

Logging er et sikkerhetstiltak som er nødvendig for å oppnå tilfredstillende konfidensialitetssikring, i samsvar med personopplysningslovens § 13 jf. personopplysningsforskriftens § 2-11. Personopplysningsforskriften oppstiller følgende krav til logging:

- autorisert bruk og forsøk på uautorisert bruk skal logges, §§ 2-8 og 2-14.
- loggene skal gjøre det mulig å avdekke eventuelt uautorisert bruk av informasjonssystemet, § 2-14.

Hvor tilgang i det videre diskuteres i forhold til konfidensialitetssikring, menes lesetilgang til personopplysninger, herunder gjennom søkebilder.

6.8.1 Tilgang til Kompis

Etter det opplyste skal tilgangen til opplysningene i Kompis være basert på den enkelte ansattes tjenstlige behov. Dette fremgår av departementets brev av 15. desember 2006[2]:

"Taushetsbelagte opplysninger skal bare gjøres tilgjengelig for medarbeider som har et saklig behov for tilgang til slike opplysninger. … Dette vil i stor grad kunne begrenses ut fra hvilket tilgangsnivå den enkelte bruker gis til Kompis systemene…".

Pr i dag er det ca 4100 personer på landsbasis som har tilgang til Kompis. Antallet samtidige brukere (brukere som til enhver tid er pålogget) ligger mellom 350 og 400.

Tilgangen til opplysningene i Kompis er ordnet i tre nivåer, nivå 3, 4 og 5. "Rutine Autorisasjonstildeling" (KIS) gir ingen beskrivelse av hva den normale tilgangen til informasjonssystemet skal være. Under kontrollen ble det opplyst at nivå 3 (det laveste nivået) er å anse som normaltilgangen. Ved Ila var alle tilganger allikevel gitt på nivå 4 og 5, uten at dette ble begrunnet særskilt. Differensieringen mellom tilgangene 3-5 er etter det opplyste relatert til skriverettigheter.

6.8.1.1 Tilgang til historiske data

I henhold til det opplyste blir det ikke slettet opplysninger i Kompis. Lesetilgangen er ikke differensiert i forhold til om den registrerte er innsittende eller ikke. Det innebærer at alle registrerte opplysninger om alle som er eller har vært innesittende

[2] Justisdepartementets "Krav om redegjørelse – Autorisasjonsrutiner for Kompis og andre personopplysninger ved fengslende", ref. 200608491, 15.12.2006, side 2, siste avsnitt.

ved et norsk fengsel siden 1992 fremdeles ligger fullt tilgjengelige for lesing i Kompis. Tilgangen til opplysninger om personer som *har vært* innesittende er således like tilgjengelige som opplysninger om personer som til enhver tid *er* innesittende.

Opplysningene ligger på det laveste tilgangsnivået (nivå 3). Etter hva Datatilsynet forstår har alle ansatte i alle landets fengsler med tilgang til Kompis (over 4.000 personer) denne tilgangen. For Ilas del innbærer dette at alle ansatte med tilgang til Kompis har tilgang til detaljerte opplysninger om over 2.000 tidligere innsatte ved anstalten (se også pkt 6.8.1.2).

Datatilsynet kan ikke se at de ansattes tilgang til opplysninger om *tidligere innsatte* er forsvarlig begrunnet i den enkeltes tjenstlige behov, når den aktuelle personen ikke er innesittende. Tilsynet kan heller ikke se at KSF har vurdert og begrunnet dette konkret.

Under kontrollen ble det anført fra KSF at Riksarkivaren har uttalt at opplysningene er arkivverdige, og derfor ikke skal slettes. Datatilsynet vil bemerke at arkivering ikke tidligere er anført som et formål med behandlingen av personopplysninger i Kompis. Etter hva Datatilsynet forstår, vil arkivplikten kunne ivaretas tilfredsstillende gjennom oppbevaring av det papirbaserte arkivet. Arkivplikten kan uansett ikke begrunne at historiske opplysninger ligger fullt tilgjengelige i Kompis

6.8.1.2 Tilgang til opplysninger om innsatte ved andre anstalter

Under kontrollens innledende møte ble det opplyst at de ansatte bare hadde tilgang til opplysninger om innesittende eller tidligere innsatte ved den anstalten der man har sitt daglige arbeide. Ansatte ved Ila skulle etter dette bare ha tilgang til opplysninger om personer som har vært innesittende eller er innsatt *ved Ila fengsel*.

Under tilsynets verifikasjon ble det imidlertid avdekket at *de ansatte ved Ila har tilgang til opplysninger om alle som er eller har vært innsatt, ved hvilket som helst fengsel i Norge, siden Kompis ble innført i 1992*. Dette gjelder etter det opplyste over 30.000 personer.

Følgende informasjon var tilgjengelig:

- Navn
- Fødselsnummer
- Anstalt
- Tidsom for soningen
- Innsattkategori (varetekt, sikring, forvaring, bøtesoning)
- Status for soningen (sykehus, lukket avdeling, åpen avdeling, behandlingsinstitusjon)

Opplysningene fremkommer i søkebildet i Kompis, og ligger på det laveste tilgangsnivået, nivå 3. Etter hva Datatilsynet forstår innebærer dette at alle ansatte i alle landets fengsler, som har tilgang til Kompis, har tilgang til alle disse opplysningene.

Datatilsynet kan ikke se at de ansattes tilgang til opplysninger om *innsatte ved andre anstalter* er forsvarlig begrunnet i den enkeltes tjenstlige behov, når den aktuelle personen ikke er innesittende ved den anstalten der man har sitt daglige arbeide. Tilsynet kan heller ikke se at KSF har vurdert og begrunnet dette konkret.

Det vises for øvrig til rapportens pkt 6.10 om den behandlingsansvarliges opplysningsplikt, hvor KSF sine redegjørelser om nevnte forhold behandles.

6.8.2 Logging

Det er ikke etablert logging av oppslag i personopplysninger Kompis. Det innebærer i praksis at den behandlingsansvarlige ikke har mulighet til å se hvilke konkrete opplysninger den enkelte ansatte tilegner seg i systemet. Det vil således ikke være mulig for KSF å kontrollere at den enkelte ansatte kun behandler opplysninger som er nødvendige ut fra vedkommendes tjenstlige behov.

6.8.3 Konklusjon

Tildelte tilganger i Kriminalomsorgen innebærer i praksis at over 4.000 ansatte har tilgang til sensitive personopplysninger om over 30.000 enkeltpersoner.

Datatilsynet kan ikke se at de ansattes generelle tilgang til opplysninger om innsatte ved andre anstalter enn den man selv arbeider ved er forsvarlig begrunnet i den enkeltes tjenstlige behov. Tilsynet kan heller ikke se at de ansattes tilgang detaljerte historiske data er forsvarlig begrunnet i vedkommendes tjenstlige behov. Tilsynet kan uansett ikke se at KSF har vurdert og begrunnet den enkelte ansattes generelle tilgang til nevnte opplysninger.

I forbindelse med kontrollen oversendte Kriminalomsorgens it-tjeneste (KITT) et forslag til en ny tilgangsinndeling i Kompis. Denne skrev seg fra november 1999. Det går imidlertid frem at endringen er besluttet ikke innført, og at KSF i stedet har prioritert å planlegge et nytt etatssystem.

Etter Datatilsynets vurdering gir dårlig tilgangsstyring, i kombinasjon med manglende logging av oppslag i systemet, utilfredsstillende informasjonssikkerhet.

Mangelfull tilgangsstyring anses som et brudd på personopplysningslovens § 13, jf. personopplysningsforskriftens 2-11 om konfidensialitetssikring.

Manglende logging og systematisk kontroll av loggene for å avdekke uautorisert bruk, ses som et avvik fra personopplysningslovens § 13, jf. personopplysningsforskriftens § 2-11 om konfidensialitetssikring og §§ 2-8 og 2-14 om logger og sikkerhetstiltak.

6.9 Risikovurderinger

Personopplysningslovens § 13 stiller krav om at virksomheten etablerer tilfredstillende informasjonssikkerhet gjennom planlagte og systematiske tiltak.

Personopplysningsforskriftens stiller krav om at virksomheten dokumenterer tilfredstillende informasjonssikkerhet gjennom bruk av risikovurderinger, § 2-4. Den behandlingsansvarlige plikter selv å sette kriterier for akseptabel risiko, og vurdere sine løsninger opp mot disse.

Det stilles videre krav om at ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

6.9.1 Om Risikovurderingen fra 1997

Datatilsynet ba under kontrollen om å få ettersendt gjeldende risikovurdering vedrørende fagapplikasjonen Kompis. Datatilsynet mottok i ettertid en risikovurdering som skrev seg fra desember 1997.

Datatilsynet vil bemerke at en risikovurdering som er ti år gammel vanskelig kan sies å være relevant. Den er på ingen måte tilpasset gjeldende trusselbilde, sett i lys av den teknologiske og samfunnsmessige utviklingen som har funnet sted i løpet av de siste ti årene. En risikovurdering skal oppdateres jevnlig, og i forbindelse med konkrete endringer i trusselbildet som har betydning for behandlingen.

I risikovurderingen fra 1997 identifiserte KITT alvorlige svakheter hva gjaldt logging, og den følgende evnen til å avdekke sikkerhetsbrudd. Forholdet er imidlertid ikke utbedret. Hvorvidt øvrige forhold som er avdekket gjennom risikovurderingen er korrigert, er for Datatilsynet uklart.

6.9.2 Konklusjon

Datatilsynets vurderer at den oversendte dokumentasjonen ikke tilfredstiller regelverkets krav til en risikobasert tilnærming til informasjonssikkerhet. Videre er det identifisert at vesentlige svakheter i den gjennomførte vurderingen uansett ikke er utbedret.

Forholdet anses som et brudd på personopplysningslovens § 13, jf. personopplysningsforskriftens 2-4.

6.10 Den behandlingsansvarliges opplysningsplikt overfor Datatilsynet

I henhold til personopplysningslovens § 44, 1. ledd kan Datatilsynet kreve de opplysninger som er nødvendige for at det kan gjennomføre sine oppgaver etter personopplysningslovens § 42, herunder kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt.

6.10.1 KSFs opplysninger om tilgangsstyring

Datatilsynet mottok den 22. august 2006 klage fra innsatte ved Ila, hvor det blant annet ble hevdet at *"Datasystemet Kompis er tilgjengelig for hele kriminalomsorgen"*

og at *"systemet beskriver tidligere innsatte som ikke lenger er under kriminalomsorgen"*.

Med hjemmel i personopplysningslovens § 44 ba Datatilsynet derfor om en redegjørelse fra KSF vedrørende sletting og autorisasjon i fagapplikasjonen Kompis, jf tilsynets brev av 13. november 2006.

Redegjørelsen fra KSF ble oversendt med brev av 15. desember 2006[3]. Vedlagt denne fulgte også redegjørelser fra Kriminalomsorgen region nordøst[4] og Ila fengsel[5]. I redegjørelsen fra Ila heter det:

"Når det gjelder påstanden om at ansatte gjennom KOMPIS har tilgang til informasjon om alle innsatte i Norge, så gjelder dette kun de personer som har ansvar for plasslogistikk og overføring av innsatte mellom fengslene, samt IKT-ansvarlige. Øvrige ansatte med autorisert tilgang i KOMPIS vil kun ha tilgang på informasjon om innsatte som befinner seg i anstalten (vår uthevning)." (side 4, 5. avsnitt).

Dette bekreftes i redegjørelsen fra Kriminalomsorgen region nordøst side 2 under overskriften "Merknader til enkelte punkter i klagers brev av 22. august 2006":

"Som direktøren redegjør for er det kun utvalgte tjenestemenn med ansvar for fangelogistikk og overføringer av innsatte mellom fengsler, som har tilgang til hele kriminalomsorgen, dvs opplysninger om innsatte i andre fengsler."

Etter Datatilsynets vurdering er Kriminalomsorgens skriftlige fremstillinger for tilsynet direkte feilaktige. Slik det fremgår av foreliggende rapport (pkt 6.8), har de ansatte tilgang til opplysninger om samtlige personer som har vært til soning i hele landet, siden oppstarten av Kompis.

Datatilsynet vil bemerke at den vide tilgangen til innsattopplysninger heller ikke ble lagt frem av den behandlingsansvarliges representanter under den stedlige kontrollen, men ble avdekket av tilsynet på egen hånd, gjennom egne søk i Kompissystemet.

6.10.2 KSFs opplysninger om "innsatt pr nummer"

Datatilsynet finner videre grunn til å stille spørsmål ved at registeret "innsatt per nummer" aldri er blitt berørt i redegjørelsene fra KSF til Datatilsynet. Dette fremstår som besynderlig, sett i forhold til at en vesentlig del av informasjonsbehandlingen ved Ila skjer nettopp i dette registeret, og at KSF har redegjort detaljert for de øvrige sider av informasjonsbehandlingen.

[3] Justisdepartementets "Krav om redegjørelse – Autorisasjonsrutiner for Kompis og andre personopplysninger ved fengslende", ref. 200608491, 15.12.2006
[4] Kriminalomsorgen region nordøsts "Autorisasjonsrutiner for Kompis og andre personopplysninger ved fengslene ", ref. 2006/28717-7/053.1, 08.12.2006
[5] Ila fengsels " Autorisasjonsrutiner for Kompis og behandling av personopplysninger", ref. 2006/789 001.2 KB/jan, 30.11.2006

Heller ikke dette var et forhold som ble lagt frem for Datatilsynet i forbindelse med den stedlige kontrollen, men som tilsynet selv avdekket gjennom personlige intervjuer med de ansatte og innsyn i mappestrukturen.

6.10.3 Konklusjon

Datatilsynet finner at KSF har presentert feilaktige og mangelfulle opplysninger for tilsynet, både gjennom årelang skriftlig korrespondanse og under tilsynets stedlige kontroll. De alvorlige forhold som fremkommer av foreliggende rapport hadde ikke blitt avdekket, dersom Datatilsynet ikke hadde foretatt en stedlig kontroll og selv utført kontrollhandlinger direkte i informasjonssystemene.

Datatilsynet anser at dette er alvorlig, særlig med bakgrunn i at de skriftlige redegjørelsene fra KSF tilsynelatende er kvalitetssikret i flere nivåer innen kriminalomsorgsforvaltningen.

Det fremstår for Datatilsynet som om KSF bevisst har holdt tilbake vital informasjon for tilsynet. Den eneste mulige forklaringen på manglende informasjon er at både KSF, Kriminalomsorgen region nordøst og Ila fengsel, forvarings- og sikringsanstalt mangler vesentlig kunnskap om sin egen fagapplikasjon. Datatilsynet har ikke kunnet tilegne seg den oppfatning at fravær av faktisk kunnskap frir den behandlingsansvarlige fra sitt ansvar.

Forholdet anses å innebære et brudd på personopplysningslovens § 44.

Datatilsynet gjør oppmerksom på at brudd på § 44 er belagt med straff, jf personopplysningslovens § 48 første ledd litra f.