

Rapport 15. mai 2012

INFOFLYT

Informasjonsutveksling mellom politiet og kriminalomsorgen
i saker med alvorlig kriminalitet og høy risiko



Rapport 15. mai 2012

INFOFLYT

Informasjonsutveksling mellom politiet og kriminalomsorgen
i saker med alvorlig kriminalitet og høy risiko



Til Justis- og beredskapsdepartementet

Justis- og politidepartementet nedsatte 4. mai 2010 et utvalg som skulle foreslå hensiktsmessige regler for behandlingen av opplysninger, herunder informasjonsutvekslingen med politiet i INFOFLYT.

Utvalget legger med dette frem sin rapport som inneholder utvalgets syn på de temaer som beskrives i mandatet og forslag til lov- og forskriftsendringer.

Utvalgets forslag er enstemmige. Det er dissens på den lovtekniske løsningen. Utvalgets oppdrag er dermed avsluttet.

Oslo 15. mai 2012

Karen Alette Melander
Leder

Inger Marie Sunde

Sylvia Peters

Tom A. Enger

Per Håkon Sand

Kim Ellertsen

Tor André Jenssen
Sekretær

Innholdsfortegnelse

1	Innledning.....	6
1.1	Utvalgets sammensetning og mandat.....	6
1.2	Rapportens hovedtrekk.....	8
1.3	Utvalgets arbeid.....	9
1.4	Avgrensning og fortolkning av mandatet.....	9
2	Sammendrag av utvalgets forslag.....	11
3	Historikk og bakgrunn for nedsettelsen av utvalget.....	14
3.1	Foranledningen til INFOFLYT.....	14
3.2	INFOFLYT etableres.....	15
3.3	Bakgrunn for nedsettelsen av utvalget.....	16
3.3.1	Innledning.....	16
3.4	Sivilombudsmannens kritikk av INFOFLYT.....	17
3.5	Øvrige rapporter som begrunner en gjennomgang.....	18
3.5.1	Datatilsynets tilsyn ved Ila.....	18
3.5.2	FN's arbeidsgruppe mot vilkårlig fengsling – rapport 2007.....	19
3.5.3	Kritikk for manglende effektivitet - Riksrevisjonen.....	20
3.5.4	Stortingsmeldingene som har behandlet INFOFLYT.....	21
3.6	Oppsummering.....	23
4	Gjeldende rett.....	24
4.1	Innledning.....	24
4.2	Internasjonal lovgivning om menneskerettighetene og personvernet.....	24
4.3	Personopplysningsloven.....	26
4.3.1	Innledning.....	26
4.3.2	Behandlingsansvaret.....	28
4.3.3	Behandlingsgrunnlag og grunnvilkår.....	28
4.3.4	Informasjonsplikt.....	30
4.3.5	Innsyn.....	31
4.3.6	Meldeplikt og konsesjonsplikt.....	31
4.3.7	Øvrige plikter i loven som er særlig sentrale for INFOFLYT.....	32
4.3.8	Tilsyn og klage.....	32
4.4	Straffegjennomføringsloven.....	32
4.4.1	Innledning.....	32
4.4.2	De nye lovreglene om behandling av personopplysninger i straffegjennomføringsloven.....	34
4.4.3	Gjeldende regler om unntak fra forvaltningslovens regler om taushetsplikt, partsinnsyn, plikten til å begrunne vedtak og adgang til å utlevere opplysninger til andre.....	36
4.5	Politiregisterloven.....	38
4.5.1	Generelt om politiregisterlovgivningen.....	38
4.5.2	Politiets rett og plikt til å utlevere opplysninger til Kriminalomsorgen.....	39
4.6	INFOFLYT – gjeldende instruks og øvrige retningslinjer.....	41
4.7	Behandling av gradert materiale.....	48
4.8	Beskrivelse av det elektroniske fangesakssystemet KOMPIS.....	49
4.9	Beskrivelse av saksbehandlings- og arkivsystemet DocuLive.....	50
5	Ordningene i Sverige og Danmark.....	52
5.1	Sverige.....	52
5.1.1	Generelt.....	52
5.1.2	Regelverket for Kv-KUT - Säkerhetsregistret.....	53
5.1.3	Kriminalvårdens etterretningsorganisering Kv-KUT.....	54
5.1.4	Säkerhetsregistret.....	54
5.1.5	Opplysningenes art, kildene og utlevering.....	55
5.1.6	Innsyn og informasjon til de registrerte.....	55

5.2	Danmark.....	55
5.2.1	Generelt.....	55
5.2.2	Kriminalforsorgens Etterretningssystem (KES).....	56
5.2.3	Målgruppe og type kriminalitet.....	57
5.2.4	Kvalitetssikring.....	57
5.2.5	Hvordan personer avregistreres.....	58
5.2.6	Taushetsplikt, informasjonsplikt og innsyn.....	58
6	Nærmere om regelverk knyttet til den registrertes rettigheter.....	59
6.1	Innledning.....	59
6.2	Informasjonsplikt.....	59
6.3	Innsyn.....	60
6.3.1	Noen innledende merknader.....	60
6.3.2	Partsinnsyn.....	60
6.3.3	Innsyn i henhold til personvernlovgivningen.....	60
6.3.4	Retting, sperring og sletting av personopplysninger.....	61
6.3.5	Klageadgang og adgang til å be om Datatilsynets kontroll.....	63
6.3.6	Tilsyn og tilsynsorganets kompetanse.....	64
7	Utvalgets vurdering av hvordan INFOFLYT har vært praktisert.....	65
7.1	Innledning.....	65
7.2	Hvordan informasjonsutvekslingen skjer i dag.....	65
7.2.1	Innledning.....	65
7.2.2	Saksmappene.....	65
7.2.3	Hovedfunn fra gjennomgangen.....	66
7.2.4	Informasjonssikkerheten i INFOFLYT-mappene.....	67
7.2.5	Forsendelse.....	67
7.2.6	Utvalgets vurderinger av mappene.....	67
7.3	Kriminalomsorgens syn på INFOFLYT.....	68
7.4	Utvalgets inntrykk av kriminalomsorgens og politiets syn på nytteverdien.....	69
7.4.1	Politiets oppfatning av nytteverdi og potensiale for dette.....	69
7.4.2	Kriminalomsorgens oppfatning av nytteverdi og potensiale for INFOFLYT.....	70
7.5	Rapporteringsrutiner.....	71
7.6	Utvalgets oppsummering.....	71
8	Krav som bør stilles til INFOFLYT - utvalgets vurderinger.....	73
8.1	INFOFLYT må forankres i et klart hjemmelsgrunnlag.....	73
8.1.1	Innledning.....	73
8.1.2	Legalitetsprinsippet krever klar hjemmel i lov.....	74
8.1.3	Spørsmålet om behov for et nytt tilsyns- eller kontrollorgan.....	74
8.1.4	Behov for lovhjemmel for kriminalomsorgens adgang til å utlevere personopplysninger utenfor INFOFLYT.....	75
8.1.5	Innsyn i domstolsbehandling – tvisteloven § 22-3.....	76
8.1.6	Bevisforbud etter straffeprosessloven § 117 og 118.....	77
8.1.7	Behandling av opplysninger om tredjepersoner i INFOFLYT.....	77
8.1.8	Lovhjemmelen bør tilpasses politiregisterloven.....	78
8.2	Saksbehandling og samarbeid.....	80
8.2.1	Kompetanse, tillit og samarbeidsfora.....	80
8.2.2	Hvem som kan registreres, kvalitet på opplysninger og bruken i en risikovurdering.....	83
8.2.3	Samarbeid internt i kriminalomsorgen.....	84
8.2.4	Internasjonalt samarbeid.....	85
9	Økonomiske og administrative konsekvenser.....	86
9.1	Økonomiske konsekvenser.....	86
9.1.1	Tiltak på kort sikt.....	86
9.1.2	Tiltak på lengre sikt.....	86
9.2	Administrative konsekvenser.....	87
10	Merknader til forslaget til regelendringer.....	88

10.1 Merknader til forslaget til lovbestemmelser	88
10.2 Merknader til forslaget til forskrift	90
10.3 Behov for regulering i rundskriv/ saksbehandlingsinstruks	98
10.3.1 Generelt.....	98
10.3.2 Særlig om behandling av gradert informasjon	100
11 Forslag til lov og forskrift	104
11.1 Utvalgets forslag til endringer i straffegjennomføringsloven	104
11.2 Utvalgets forslag til forskrift	104
11.2.1 Innledende merknader	104
11.2.2 Utkast til forskrift	105
Vedlegg 1:	109
Rundskriv G-3 2005 (det generelle samarbeidet om informasjonsutveksling)	109
Vedlegg 2:	113
Saksbehandlingsinstruks INFOFLYT, KSF 2/ 2005	113
Vedlegg 3:	120
Dokumentliste	120

1 Innledning

1.1 Utvalgets sammensetning og mandat

Utvalget har hatt følgende sammensetning:

Ekspedisjonssjef Karen Alette Melander, Justis- og beredskapsdepartementet (leder)

Fagdirektør Sylvia Peters, Justis- og beredskapsdepartementet

Advokat Inger Marie Sunde, Stavanger

Politiadvokat Per Håkon Sand, Oslo Politidistrikt

Professor Dag Wiese Schartum, Universitetet i Oslo

Avdelingsdirektør Kim Ellertsen, Datatilsynet

Fengselsleder Tom A. Enger, Ullersmo fengsel

Utvalgets sekretær har vært seniorrådgiver Tor André Jensen, Justis- og beredskapsdepartementet.

Dag Wiese Schartum gikk ut av utvalget 25. mai 2011.

Utvalget ble nedsatt av Justisdepartementet 4. mai 2010 og ble gitt frist til 31. desember 2010, senere utsatt til 1. juli 2011. Bakgrunnen for at utvalget ble ytterligere forsinket var terrorangrepet mot regjeringskvartalet 22. juli. I tillegg forutsetter utvalgets mandat at forslag til regelverk skal samordnes med forskriftene til politiregisterloven, som også har vært forsinket.

Arbeidet ble igangsatt ved første møte 19. mai 2010. Utvalget har avholdt 16 møter, det siste 7. mars 2012. Det ble ikke avholdt møter mellom 30. juni 2011 og 7. mars 2012. Utredningen ble overlevert 22. mai 2012.

Utvalget ble gitt følgende mandat:

«Både kriminalomsorgen og politiet har som formål å forebygge kriminalitet og trygge samfunnet. Samarbeid og informasjonsutveksling er svært viktig for å nå disse målene. Justisdepartementet etablerte derfor i 2005 et INFOFLYT-system for gjensidig utveksling av informasjon mellom kriminalomsorgen og politiet, jf. rundskriv G-3/2005. Systemet skulle gi kriminalomsorgen et bedre grunnlag for å sikkerhetsvurdere varetektsfengslede og dømte. Politiet/påtalemyndigheten på sin side skulle få et bedre grunnlag for etterforskning og oppfølging.

Sivilombudsmannen har flere ganger stilt kritiske spørsmål ved sider av INFOFLYTsystemet.

Kritikken er særlig knyttet til den særskilte saksbehandlingsinstruksen som er utarbeidet av Kriminalomsorgens sentrale forvaltning, jf. rundskriv KSF 2/2005. På denne bakgrunn har Justisdepartementet besluttet å nedsette et utvalg som skal

gjennomgå INFOFLYT-systemet og foreslå regler for kriminalomsorgens behandling av personopplysninger og bruken av slike opplysninger i saksbehandlingen. Formålet med utredningen er å finne frem til et hensiktsmessig regelverk som både ivaretar formålet med informasjonsutvekslingen og rettssikkerheten til domfelte, innsatte og andre registrerte.

Dette innebærer at utvalget først skal kartlegge og vurdere hvordan kriminalomsorgens utveksling av informasjon med politiet fungerer i dag. Dette gjelder både behandlingen av personopplysninger (som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter), og bruken av slike opplysninger i saksbehandlingen – både forvaltnings- og domstolsbehandlingen. Kartleggingen skal omfatte et representativt utvalg av saker knyttet til innsatte ”registrert” i INFOFLYT-systemet i 2009.

På bakgrunn av kartleggingen skal utvalget foreslå hensiktsmessige regler for behandlingen av opplysninger og hvilke saksbehandlingsrutiner som bør følges ved informasjonsutveksling. Når det gjelder behandlingen av personopplysninger, må utvalget vurdere om utkastet til ny §§ 4c og 4d i straffegjennomføringsloven om kriminalomsorgens behandling av personopplysninger gir en klar, tydelig og tilstrekkelig hjemmel for informasjonsutvekslingen med politiet.

Utkastet til endringer i straffeprosessloven og straffegjennomføringsloven (kriminalomsorgens behandling av personopplysninger og innsyn i benådningssaker mv.) ble sendt på høring 23.mars 2009 og planlegges fremlagt for Stortinget våren 2010. Utover dette bør utvalget ta utgangspunkt i utkast til ny § 4e i straffegjennomføringsloven ved utformingen av forslag til regler om behandling av opplysninger. Videre skal utvalget lage utkast til forskrift og retningslinjer som regulerer saksbehandlingen i tilknytning til informasjonsutvekslingen, jf. for eksempel forslag til § 27 siste ledd i den nye politiregisterloven. Det understrekes at mandatet ikke omfatter utlevering av opplysninger fra politiet til kriminalomsorgen, idet dette er regulert i forslag til ny politiregisterlov, jf. Ot.prp. 108 (2008-2009), og vil bli ytterligere presisert i forskriften til politiregisterloven.

Utvalget skal også foreslå hensiktsmessige regler for bruk av personopplysningene i kriminalomsorgens saksbehandling (fangesaker). Dette gjelder for eksempel regler om nedtegning av opplysninger, innsynsrett, klagerett og taushetsplikt. Tilsvarende skal utvalget vurdere og eventuelt foreslå hensiktsmessige regler om innsynsrett i personopplysninger ved domstolsbehandling. Aktuelle regler er i dag hjemlet i tvisteloven § 22–3 og straffeprosessloven § 117 og § 118.

Utvalgets tilrådinger skal også innbefatte konkrete forslag til mulige lov- forskrifts- og retningslinjeendringer. Forslagene skal utformes i tråd med anbefalingene i Justisdepartementets hefte Lovteknikk og lovforberedelse, 2000. Forslaget må dessuten harmonere med tilsvarende regler for politiets informasjonsutveksling, jf. politiregisterloven og forskrift og retningslinjer til loven.

Forslaget må ivareta hensynet til et oversiktlig og enkelt regelverk og ligge innenfor rammen av Norges folkerettslige forpliktelser.

Utvalget skal utrede økonomiske, administrative og andre vesentlige konsekvenser som forslagene kan medføre. Økonomiske og administrative konsekvenser må vurderes opp mot forventet effekt av hvert enkelt tiltak. Utvalget skal avgi minst ett forslag som baseres på uendret ressursbruk.

*Utvalget skal utarbeide en rapport til Justisdepartementet **innen 31. desember 2010.***»

1.2 Rapportens hovedtrekk

Rapporten består av i alt 11 kapitler:

Kapittel 1 er innledning og beskriver mandat, hvordan utvalget har arbeidet, fortolket og avgrenset sitt mandat.

Kapittel 2 er sammendrag av utvalgets forslag og vurderinger.

Kapittel 3 er historikk og angir bakgrunnen for at INFOFLYT-utvalget ble opprettet, som er den kritikk som er framført av Sivilombudsmannen, Datatilsynet og Riksrevisjonen.

Kapittel 4 beskriver gjeldende rett for INFOFLYT. Her angis hovedreglene for behandling av personopplysninger i personopplysningsloven, politiregisterloven og straffegjennomføringsloven. I tillegg beskrives den gjeldende INFOFLYT-instruks og enkelte relevante retningslinjer, samt elektroniske systemer som berører INFOFLYT.

Kapittel 5 beskriver ordningene for behandling av opplysninger i saker med alvorlig og organisert kriminalitet i den svenske og danske kriminalomsorgen.

Kapittel 6 beskriver gjeldende rett om den registrertes rettigheter, personvernet og forholdet mellom politiregisterlovens og personopplysningslovens regler om innsyn, retting, sletting og tilsyn.

Kapittel 7 beskriver hvordan informasjonsutvekslingen skjer i praksis. Riksrevisjonens undersøkelse, politiets og kriminalomsorgens vurderinger av INFOFLYT beskrives, og til slutt utvalgets vurdering av hvordan INFOFLYT praktiseres.

Kapittel 8 beskriver utvalgets vurderinger av hvilke utfordringer INFOFLYT står overfor og utvalgets forslag til forbedringer. Dette omfatter både behovene for et bedre rettslig grunnlag og øvrige forbedringer for å få informasjonsutvekslingen mellom politiet og kriminalomsorgen til å fungere bedre.

Kapittel 9 angir økonomiske og administrative konsekvenser.

Kapittel 10 gir merknader til lov- og forskriftsbestemmelsene som foreslås.

Kapittel 11 inneholder utkastet til lov og forskrift om INFOFLYT.

1.3 Utvalgets arbeid

Utvalget har besøkt KRIPOS, Politiets sikkerhetstjeneste (heretter kalt PST), Ringerike fengsel og Bastøy fengsel for å få deres syn på samarbeidet i INFOFLYT. Utvalget har også hatt møte med nøkkelpersoner i kriminalomsorgens regioner og med tillitsvalgte fra Norsk Fengsels- og friomsorgsforbund (NFF) og Kriminalomsorgens Yrkesforbund (KY). I tillegg har utvalget intervjuet sentrale medarbeidere i Kriminalomsorgens sentrale forvaltning (heretter kalt KSF) som arbeider med INFOFLYT. Utvalget har fått en orientering og demonstrasjon av kriminalomsorgens elektroniske fangesakssystem KOMPIS og fått demonstrert den arkivmessige håndtering og registreringsrutinene i Justisdepartementets Dokumentasjonssenters hemmelige arkiv – «H-arkivet». Utvalget har i tillegg innhentet informasjon fra Sverige og Danmark om deres tilsvarende systemer.

For å få en oversikt over saksbehandlingen og håndteringen av dokumentene i INFOFLYT-mappene, har utvalget gjennomgått om lag 50 saker. Alle sakene som var opprettet i 2009 ble gjennomgått, i tråd med mandatets forutsetning om å se på alle sakene der innsatte ble registrert det året. Deretter ble 10 saker med forvaltningsmessig behandling plukket ut. Det var saker der den innsatte har søkt om soningsprogresjon, flytting til annet fengsel, innsyn og om å bli tatt ut av INFOFLYT.

1.4 Avgrensning og fortolkning av mandatet

INFOFLYT er et system for gjensidig utveksling av beskyttelsesverdig informasjon mellom kriminalomsorgen og politiet.

Utvalget har gjennomgått INFOFLYT-systemet (heretter bare kalt INFOFLYT), gjort vurderinger og foreslått nye regler for kriminalomsorgens behandling av opplysninger i INFOFLYT. Utvalget har ikke undersøkt politiets bruk av systemet eller foreslått regelendringer for politiets virksomhet, jf. mandatet på dette punkt. Det vises i den sammenheng til ny politiregisterlov med forskrifter som vil regulere politiets bruk av slike opplysninger, herunder samarbeidet med bl.a. kriminalomsorgen. Selv om utvalget ikke skal se på utlevering av opplysninger fra politiet til kriminalomsorgen, har utvalget likevel funnet det naturlig å se på helheten i samarbeidet. Utvalget har derfor beskrevet og vurdert de opplysninger som kriminalomsorgen mottar i INFOFLYT, politiets interesse i INFOFLYT, saksbehandlingen i kriminalomsorgen og kriminalomsorgens rutiner for samarbeid med politiet.

Vurderingene og forslagene i rapporten har etter utvalgets syn overføringsverdi til samarbeidet om informasjonsutveksling mellom politiet/ påtalemyndigheten og kriminalomsorgen generelt. Det vises her til det arbeid som kriminalomsorgen har i satt i gang som oppfølging av St.meld. nr. 37 (2007-2008) «Straff som virker» - sidene 95-96 og Meld. St.7 (2010-2011) «Kampen mot organisert kriminalitet» - sidene 94-95 om en mer metodisk måte å bearbeide og behandle informasjon om innsatte i forbindelse med kriminalitetsbekjempelse.

Mandatet sier at utvalget eventuelt skal foreslå regler for innsyn i domstolsbehandlingen (sivile saker). Utvalget mener dette spørsmålet må vurderes på bredere basis enn bare for informasjonsutvekslingen mellom politiet og kriminalomsorgen og har derfor ikke vurdert spørsmålet inngående. For eksempel har dette spørsmålet konsekvenser også for utlendingsmyndighetene.

Utvalget skal lage utkast til retningslinjer for saksbehandlingen for INFOFLYT, i tillegg til forskrift og eventuelt lovbestemmelse. Utvalget har utarbeidet forslag til retningslinjer for behandling av gradert materiale, men har for øvrig begrenset seg til å liste opp de elementer som bør reguleres i retningslinjer, knyttet opp mot forskriften og med utgangspunkt i gjeldende instruks.

2 Sammendrag av utvalgets forslag

Formålet med dette kapitlet er å oppsummere utvalgets forslag til mål for INFOFLYT og til administrative rutiner, samarbeidsformer og nødvendige regelendringer.

Utvalget mener at et velfungerende INFOFLYT er viktig både for å forebygge alvorlig kriminalitet og for sikkerheten i fengslene. Utvalget foreslår en klar lovregulering som tilpasses politiregisterloven. Det foreslås forskrifter og skisser til administrative rutiner for kriminalomsorgen som skal bidra til å sikre ensartet behandling av personopplysninger i INFOFLYT, samtidig som personvernet ivaretas.

Hele utvalget stiller seg bak de forslag og vurderinger som nevnt nedenfor. Det er imidlertid dissens på den lovtekniske løsningen om tilpasningene til politiregisterloven og politiregisterforskriften, se punkt 8.1.8.

Formålet med å utveksle beskyttelsesverdig informasjon mellom politiet og kriminalomsorgen er å sikre at:

- kriminalomsorgen får informasjon fra politiet som er viktig for ivaretagelsen av den generelle sikkerheten i fengslene
- kriminalomsorgen får tilstrekkelig informasjon fra politiet for å kunne treffe nødvendige sikkerhetsmessige tiltak rundt den enkelte innsatte for å forebygge eller forhindre ny kriminalitet
- politiet får nødvendig informasjon om den innsatte for å kunne forebygge eller forhindre ny kriminalitet

Et slikt system innebærer at det kan treffes tiltak som kan være inngripende for den innsatte når det gjelder straffegjennomføringen og progresjonen i denne. Det er derfor nødvendig å sikre at den innsattes rettigheter ivaretas. Det er viktig å ha klare regler for hvilke rettigheter den enkelte innsatte skal ha.

Et fremtidig regelverk må derfor ha regler for kriminalomsorgens bruk av den informasjon som kommer fra politiet. I tillegg må kriminalomsorgen ha rutiner for utlevering av informasjon til politiet. Det må også gis klare regler for de innsattes rett til innsyn og begrensingene i denne.

Utvalget foreslår:

- en klar lovhjemmel for INFOFLYT
- at politiregisterloven kommer til anvendelse i lovforslagene om den registrertes rettigheter
- en forskrift forankret i lovhjemmelen
- et robust system for utveksling av beskyttelsesverdig informasjon mellom kriminalomsorgen og politiet
- et system basert på tillit og godt samarbeid mellom politiet og kriminalomsorgen
- sentral koordinering og kontroll, samt at hensynet til rask saksbehandling ivaretas

- klarere retningslinjer for hvilken informasjon som skal registreres og hvordan informasjonen skal behandles
- strukturerte rutiner for samhandling
- at personvernet ivaretas ved klarere regler for å sikre kvalitet, formålsbestemthet, innsyn, retting og sletting
- kompetanse og tilstrekkelige personellressurser i kriminalomsorgen for å redusere sårbarheten i samarbeidet
- en klarere ledelsesforankring
- et system for tilsyn og kontroll i kriminalomsorgen

Nye lovbestemmelser i straffegjennomføringsloven foreslås å regulere:

- at kriminalomsorgen skal bidra til å forebygge, forhindre og bekjempe alvorlig kriminalitet
- hjemmel for utlevering av opplysninger i INFOFLYT til politiet for å bidra til kriminalitetsbekjempelse
- den registrertes rettigheter ved behandling av personopplysninger i INFOFLYT

Forslaget til forskrift regulerer:

- formålet med informasjonsutvekslingen
- hvem det kan behandles opplysninger om
- hvem som skal være behandlingsansvarlig
- fremgangsmåten ved registrering
- krav til kvalitet på opplysningene
- hvem som skal gis autorisasjon
- samarbeid
- konkrete regler for saksbehandling om innsyn, retting, sperring, sletting og oppbevaring, og
- klageadgang

Andre vurderinger utvalget har gjort:

- Det bør vurderes om det er behov for en klarere lovregulering av behandling av beskyttelsesverdig informasjon også utenfor INFOFLYT
- Samarbeidet bør forankres i formelle møter mellom politidirektøren og ekspedisjonssjefen i KSF
- Det bør vurderes om straffegjennomføringsloven trenger klarere regler både i og utenfor INFOFLYT enn de som følger av forvaltningsloven § 13b nr. 5 og 6 for utlevering av opplysninger til andre etater. Det vises til reguleringen av dette i politiregisterloven kapittel 5 og forslaget til utleveringshjemmel i INFOFLYT, se kapittel 11
- Opplysningene i INFOFLYT må integreres i et moderne og databasert saksbehandlings- og arkivsystem. Det bør etableres systemer for sikker overføring mellom politiet og kriminalomsorgen og mellom kriminalomsorgens enheter

- Dagens merking med et rødt flagg i KOMPIS bør erstattes av et system der bare de autoriserte ansatte vet at det er registrert beskyttelsesverdige opplysninger om en innsatt
- Helheten i samarbeidet mellom politiet og kriminalomsorgen bør utredes. INFOFLYT er bare en liten del av dette samarbeidet
- Det bør vurderes om politiregisterloven skal gjelde for all behandling av personopplysninger i kriminalomsorgen
- Det bør vurderes et nærmere nordisk samarbeid, som eventuelt også inkluderer de baltiske landene
- Det er behov for internasjonale avtaler som kan gi kriminalomsorgen hjemmel til å gi og motta informasjon til eller fra et annet avtaleland om utenlandske innsatte som har soningstilknytning til flere avtaleland og som driver grenseoverskridende kriminalitet. Dette bør utredes nærmere.
- Tvisteloven § 22-3 bør vurderes i en større sammenheng enn bare forholdet mellom politiet og kriminalomsorgen
- KSF bør spre de gode erfaringene fra enkelte regioner til andre regioner og politidistrikter, slik det ble gjort i brev fra KSF til regionene 2. juli 2010.

3 Historikk og bakgrunn for nedsettelsen av utvalget

Dette kapitlet redegjør for de hendelser som var den direkte foranledningen til at politiet og kriminalomsorgen i samarbeid startet å vurdere hva som kunne forbedre samarbeidet mellom de to etater, med sikte på å forebygge kriminalitet på en bedre måte enn tidligere. I tillegg redegjøres for den kritikk som har vært reist mot INFOFLYT fra forskjellige instanser, i særlig grad Sivilombudsmannen og Riksrevisjonen, og som går på manglende rettssikkerhet og manglende effektivitet.

3.1 Foranledningen til INFOFLYT

I 1996 omkom en identitetsløs utlending etter å ha tent på sin fengselscelle i Bergen fengsel. Politiet hadde før hendelsen forsøkt å finne identiteten til vedkommende slik at han kunne uttransporteres. Vedkommende hadde brukt fengselets telefon for å ringe hjem. Derved hadde fengslet kunnskap om hvem vedkommende kunne være. Denne kunnskapen ble ikke gitt videre til politiet. Dødsfallet kunne vært unngått om politiet hadde kjent den innsattes identitet. Fengselet anførte hensynet til taushetsplikten som grunn til ikke å gi opplysningene videre til politiet.

Hendelsen utløste et arbeid for å formalisere informasjonsutvekslingen mellom politiet og kriminalomsorgen. Utlendingsmyndighetene deltok også i arbeidet fordi de ønsket kunnskap om innsattes overgang til åpnere soningsforhold og senere løslatelse. Slik kunne utlendingsmyndighetene lettere få effektiv utvisning og uttransportering fra landet.

Arbeidet var preget av vanskelige avveininger mellom politiets ønske om å få informasjon om kriminalomsorgens kjennskap til innsattes mulige planlegging av alvorlig kriminalitet, kriminalomsorgens behov for opplysninger fra politiet om forhold av betydning for fengselssikkerheten, og hensynet til de innsattes personvern.

Målet for arbeidet var å få mer enhetlig informasjonsutveksling. Praksis var dominert av tilfeldigheter og lokale variasjoner. Målet var å få enhetlig praksis der hensynet til rettsikkerhet og personvern ivaretas, sikring av god informasjonsflyt for å hindre grov kriminalitet og rømningsfare, samtidig som fengselssikkerheten sikres på en god måte. Mange ansatte i kriminalomsorgen var negative til å tjene som politiets forlengede arm og derved kunne ødelegge tillitsforholdet mellom innsatt og ansatt.

På den annen side ønsket kriminalomsorgen mer informasjon om innsatte enn det de fikk fra politiet, som var kontroll av besøkendes vandel. Dette gjaldt særlig opplysninger om varetektsfanger som overføres til soning, tips om innsmugling av våpen, planlegging av rømning, aksjoner mot anstalten, ny straffeforfølgning av den innsatte, samt opplysninger om personer vedkommende ikke bør sone sammen med.

Samtidig økte truslene knyttet til organisert kriminalitet, og politisk og religiøs ekstremisme, og med stadig økt utenlandsk påvirkning. Kriminalomsorgen ble derfor

fra 1998 stadig mer opptatt av å finne fram til bedre informasjonsflyt med politiet. Samme år laget Justisdepartementet derfor en strategi der bedre informasjonsflyt mellom de to sektorer var et viktig virkemiddel. Det ble opprettet en arbeidsgruppe «Prosjektgruppe INFOFLYT» med medlemmer fra politi og fengselsmyndigheter 17. september 1999. Av ulike grunner stoppet arbeidet opp, før det daværende fengselsstyret og Politidirektoratet, heretter kalt POD, besluttet å gjenoppta arbeidet i 2001. En arbeidsgruppe for INFOFLYT ble opprettet. Dette ledet til en rapport/samordnet notat 19. februar 2002, som foreslo et utvidet og formalisert samarbeid. Rammene for INFOFLYT-samarbeidet ble lagt. I følge notatet skulle KRIPOS eller annen enhet utpekt av POD være den sentrale enhet som skulle kvalitetssikre og vurdere politiinformasjonen før den skulle videresendes POD, for videre forsendelse til KSF. Det ble poengtert at begge etatene måtte ha tillit til systemet. Det ble nevnt som forutsetning at Datatilsynet måtte kontaktes med tanke på avklaring av om det måtte konsesjon til eller om melding om registeret var tilstrekkelig.

3.2 INFOFLYT etableres

Høsten 2002 startet utprøving av INFOFLYT. I begynnelsen konsentrerte man seg om et lite antall innsatte som ble antatt å innebære størst risiko. Ved dette ønsket man å prøve ut systemet i praksis og å lære.

Ved brev 29. juli 2004 fra KSF fikk regionene oversendt en tiltaksplan for straffegjennomføring for innsatte med tilhørighet til organisert kriminalitet. Bakgrunnen var departementets ønske om å rette søkelyset mot organisert kriminalitet i særdeleshet. Det omfattet dermed ikke alle som senere kom til å bli registrert i INFOFLYT, som dreier seg om også andre typer kriminalitet enn den organiserte.

I brevets tiltak nr. 1 forutsettes kriminalomsorgen å ha oversikt over miljøene med tilknytning til organisert kriminalitet. For å oppfylle målet om å ha en god oversikt over disse, skal det være et fast og systematisk samarbeid med politiet. Samarbeidet skal sikre etterretningsinformasjon fra politiet, herunder også når det vurderes slik at *«(...) den innsatte ikke lenger skal anses som så farlig at han tilhører målgruppa for denne tiltaksplanen.»*

Brevets tiltak nr.2 tar for seg gjeldende regelverk: Når det gjelder vurdering av permisjoner, prøveløslatelse mv. går det fram at man må *«(...) legge seg på en særlig streng linje (...) for den gruppen innsatte man her snakker om. I disse tilfellene vil god oppførsel i anstalt ikke være noe argument for at sikkerhetsrisikoen er liten. Det må i større grad sees hen til hva de er dømt for, hvem de er dømt sammen med og hvor mange dommer de har. Det er også helt legitimt å begrunne avslag med at det er lagt vekt på tidligere og nåværende straffbare forhold.»*

Hensynet til rettsikkerheten tas opp i avsnittet under: *«Ved skjønnsutøvelsen må det imidlertid tas hensyn til de begrensninger andre regler enn straffegjennomføringsloven oppstiller. Eksempler er internasjonale menneskerettigheter, det forvaltningsrettslige forbud*

mot å treffe avgjørelser som innebærer usaklig eller urimelig forskjellsbehandling, domstolenes legalitetskontroll og Sivilombudsmannens kontroll (...)». I brevets punkt 3 om sikkerhetstiltakene i fengsel, slås det fast at «Det må understrekes at informasjon fra politi og påtalemyndighet alltid må nedfelles skriftlig. Innsatte (eller dennes advokat/forsvarer) har ikke innsyn i disse opplysningene, jf. strgf. § 7 c, siden dette kan være utilrådelig av sikkerhetsmessige forhold eller utilrådelig av hensyn til etterforskning av straffbare forhold.»

Like etter – høsten 2004 - ble den første INFOFLYT- saken behandlet og registrert av KSF. Det ble utarbeidet et generelt rundskriv om informasjonsutvekslingen mellom politiet/ påtalemyndigheten og kriminalomsorgen G-3 2005 av 18. mars 2005. Dette rundskrivet forutsatte en særskilt saksbehandlingsinstruks om INFOFLYT. Denne instruksen ble formalisert 13. april 2005 med rundskriv KSF 2/ 2005, utarbeidet av KSF, Riksadvokaten, POD og PST.

Fra starten i 2004 av det formelle samarbeidet til januar 2011 har om lag 190 innsatte vært registrert i systemet. Av dette var om lag 50 på undersøkelsestidspunktet «aktive» i INFOFLYT, det vil si gjenstand for saksbehandling etter INFOFLYT-instruksen.

3.3 Bakgrunn for nedsettelsen av utvalget

3.3.1 Innledning

Formålet med INFOFLYT er at kriminalomsorgen og politiet skal forebygge kriminalitet og trygge samfunnet ved en systematisert og kvalitetssikret informasjonsutveksling.

Straff er definert som et onde som staten tilføyer en lovovertreder på grunn av lovovertrædelsen, i den hensikt at han skal føle det som et onde. I tillegg skal samfunnet sikres trygghet mot nye lovovertrædelser. Det å sitte i fengsel innebærer at de innsatte berøves vesentlige deler av privatlivet og personvernet, som alle ute i samfunnet ellers tar som en selvfølge. Men også innsatte som har begått alvorlig kriminalitet har rettigheter. Kriminalomsorgen opererer med et normalitetsprinsipp som skal sikre innsatte velferd som den øvrige befolkningen nyter godt av, så langt som det er sikkerhetsmessig forsvarlig.

Innsatte som er registrert i INFOFLYT kan bli underlagt et strengt kontroll- og overvåkningsregime for å forebygge rømning og planlegging av ny kriminalitet. De registrerte opplysningene vil kunne bli brukt som grunnlag for f. eks. nektelse av permisjoner, prøveløslatelse og derfor påvirke progresjonen i straffegjennomføringen. Den innsattes rett til å bli kjent med opplysninger som kan bli brukt mot ham og kunne ta til motmæle skal ivaretas så langt som mulig når dette kan skje uten at risikoen for samfunnssikkerheten og enkeltpersoners liv og helse blir for stor.

Legalitetsprinsippet krever lovhjemmel for å kunne gripe inn i borgernes rettigheter. Det kreves en klarere lovhjemmel jo mer inngripende tiltak som er aktuelle. Med

graden av inngripende tiltak økes kravene til kompetanse, grundighet og likebehandling hos dem som behandler opplysningene.

Unntak fra retten til innsyn og kontradiksjon kan bare begrunnes i tilfeller der en kvalifisert sikkerhetsmessig vurdering viser at det er utilrådelig med innsyn av hensyn til samfunnets sikkerhet eller andre enkeltpersoner, jf. straffegjennomføringsloven § 7 første ledd bokstavene c og d, jf. h, se omtalen i punkt 4.4.

I det følgende oppsummeres kritikken som danner bakgrunnen for INFOFLYT-utvalget, samt øvrige dokumenter som viser behovet for å gjennomgå INFOFLYT.

3.4 Sivilombudsmannens kritikk av INFOFLYT

Sivilombudsmannens kritikk av INFOFLYT ved brev 5. juni 2009 (2007/2274), utgjør den direkte foranledning til at INFOFLYT skal gjennomgås. Sivilombudsmannen stiller spørsmål ved det rettslige grunnlaget for INFOFLYT og legger også vekt på at systemet kan utgjøre et inngrep i privatlivets fred, jf. EMK artikkel 8. Slike inngrep betinger klare og presise lovhjemler for behandlingen. Sivilombudsmannen kritiserer at det heller ikke er søkt konsesjon for behandlingen eller sendt melding til Datatilsynet om dette, jf. personopplysningsloven § 31. I brevet vises også til en klagesak der det pekes på at det ikke er rettslig grunnlag for i rundskrivs form å bestemme at innsyn generelt ikke skal gis i INFOFLYT. Ombudsmannen ber om at departementet vurderer det rettslige grunnlaget for INFOFLYT, herunder om det nye kapittel 1a om behandlingsgrunnlag i straffegjennomføringsloven vil gi tilstrekkelig lovhjemmel for INFOFLYT eller om det bør gis en egen lov om behandling av opplysninger i INFOFLYT.

Rundskriv KSF 2/2005 angir straffegjennomføringsloven §§ 10 og 11 som hjemmel for INFOFLYT. § 10 regulerer ulike straffegjennomføringsformer, mens § 11 setter vilkårene for disse ved innsettelse i fengsel. I sivilombudsmannens nevnte brev av 5. juni 2009, skriver han at «*Det er ut fra ordlyden i disse bestemmelsene vanskelig å se at de gir hjemmel (...) i rundskrivs form (...) å opprette et sentralt register (...)*»

Sivilombudsmannen ber videre i brevet om en redegjørelse for om det er søkt Datatilsynet om konsesjon, om det har vært sendt melding til tilsynet om dette, og om det øvrige hjemmelsgrunnlaget for INFOFLYT. KSF svarer 21. september 2009 at det ved en inkurie var anvendt feil hjemmel og at riktig grunnlag skal være straffegjennomføringsloven § 5 fjerde ledd og forskriften til loven § 8-1, samt alminnelig instruksjonsmyndighet.

Lovens § 5 fjerde ledd er en forskriftshjemmel til å gi regler om kriminalomsorgens virksomhet, organisering og gjennomføring av fengselsstraff. Forskriftens § 8-1 andre ledd bestemmer at KSF gir nærmere retningslinjer til straffegjennomføringsloven og forskriften til loven.

KSF svarer videre i samme brev at det ble søkt om konsesjon for det elektroniske fangesakssystemet KOMPIS, men at Datatilsynet i brev 16. februar 2004 svarte at behandling ikke var omfattet av konsesjonsplikten, men meldepliktig etter personopplysningsloven §§ 31b og 32.

KOMPIS ble meldt Datatilsynet 7. mai 2004. KSF ba så 24. juni 2005 Datatilsynet om en forhåndsvurdering av utvidet registrering i INFOFLYT av opplysninger i KOMPIS. 9. november 2005 svarer Datatilsynet: «*Etter Datatilsynets oppfatning, vil trolig ikke straffegjennomføringsloven kunne anses som behandlingsgrunnlag for alle de ønskede utvidelser av registreringsadgangen i KOMPIS. I så tilfelle må andre behandlingsgrunnlag som nevnt i personopplysningsloven §§ 8 og 9 vurderes. Kriminalomsorgsavdelingen har ikke søkt om konsesjon eller sendt melding til Datatilsynet for INFOFLYT-systemet (...)*»

3.5 Øvrige rapporter som begrunner en gjennomgang

3.5.1 Datatilsynets tilsyn ved Ila

Kriminalomsorgen hadde konsesjon for KOMPIS etter den gamle personregisterloven av 1978. Da personopplysningsloven erstattet denne, falt konsesjonen bort.

Kriminalomsorgen søkte ny konsesjon 2. desember 2002. Datatilsynet svarte 16. februar 2004 at kriminalomsorgen ikke trenger konsesjon fordi det kan unntas fra konsesjonsplikt, jf. personopplysningsloven § 33, 4. ledd. Begrunnelsen var at det var tilstrekkelig at særloven implisitt forutsetter registrering fordi kriminalomsorgen trenger kunnskap ved å registrere sikkerhetsmessige forhold rundt den innsatte. Datatilsynet mente da at behandlingen i stedet skulle meldes til Datatilsynet.

Blant annet på bakgrunn av at en forvaringsdømt klaget til Datatilsynet over behandlingen av personopplysninger på Ila, foretok tilsynet en kontroll ved Ila fengsel og forvaringsanstalt 13. september 2007. Tilsynet avdekket flere brudd på personopplysningsloven.

Tilsynet resulterte i en rapport som belyser hjemmelsproblemet generelt for behandling av personopplysninger i kriminalomsorgen. Datatilsynets kontrollrapport av 25. januar 2008 (saksnr. 07/01455) pekte på en rekke mangler, blant annet manglende lovhjemmel for behandlingen av personopplysninger, svakheter ved informasjonssikkerheten og manglende internkontroll.

I rapporten konkluderte Datatilsynet med at kriminalomsorgen ikke har hjemmel for å behandle personopplysninger i KOMPIS. Dette ble særlig begrunnet med:

- straffegjennomføringsloven gir ikke tilstrekkelig hjemmel for behandling av personopplysninger i anstaltene
- en implisitt lovhjemmel til å behandle personopplysninger tilfredsstillende ikke nødvendigvis personopplysningslovens krav til lovhjemmel, til tross for at det må være forutsatt at kriminalomsorgen skal behandle sensitive personopplysninger
- hjemmelskravet skjerpes for behandling av sensitive personopplysninger
- formålet med behandlingen må være klart angitt, noe som mangler i KOMPIS.

3.5.2 FN's arbeidsgruppe mot vilkårlig fengsling – rapport 2007

FNs arbeidsgruppe mot vilkårlig fengsling (Report of the Working Group on Arbitrary Detention Mission to Norway A/HRC/7/4 ADD.2, 11. oktober 2007, framlagt for Utenriksdepartementet 10. mars 2008) har besøkt anstalter i Norge og gitt ut en bekymringsrapport («issue of concern») om INFOFLYT. Kritikken er begrunnet i rettssikkerheten for de innsatte, i særlig grad manglende innsyn og dermed manglende mulighet for kontradiksjon for innsatte og for domstolene (punktene 83-90 i rapporten):

«(...) This information, however, does not only form the basis for decisions taken by the prison authorities to impose restrictions upon inmates up to the point of total isolation in order to maintain safety and security inside and outside the prison; it also becomes relevant when prisoners are, in principle, eligible for early release, usually after having served two thirds of their prison term, and for those in preventive detention (...)

86. Only a few high-ranking officials within the Norwegian correctional services at central level, the prison governor as head of the prison, and the National Police Directorate have access to the database. Access to the persons concerned or their lawyers may be granted in exceptional circumstances only. Norwegian courts do not have access. The Supreme Court of Norway has accepted this scheme.

87. Access to information is vital for prison inmates when they apply for early release or termination of a preventive detention term. Without disclosure of the information that the State holds against them, the persons concerned are not in a position to assess or dispute allegations, given that even the deciding judge has no access to the information.

88. The Working Group understands that the only external control mechanism in place at present is the mandate of the Parliamentary Ombudsman, who is able to consult the database, but may not disclose any information contained therein. Moreover, the Ombudsman, although his mandate allows him to receive and act upon individual complaints, is not in a position to provide for an effective remedy to the detainees, since he is answerable solely to Parliament

89. The Working Group is by no means arguing that the database should be abolished. It serves an important purpose as far as security is concerned and increases the availability, reliability and quality of information. However, if information is also used to reject applications for release and, in certain instances, to impose restrictions or partial or total isolation upon the prisoner concerned, and the prison inmates are not aware of the information the State is holding against them, then the situation affects the right of the detainees to challenge the legality of the regime of detention.

90. In this context, the Working Group would like to emphasize that there is no right to early release on parole in international human rights law as such. However, according to principle 4 of the Body of Principles for the Protection of Persons Under any Form of Detention or Imprisonment, any form of detention and all measures affecting the human rights of the person and any form of detention or imprisonment shall be ordered by, or be subject to, the effective A/HRC/7/4/Add.2 page 23 control of a judicial or other authority. Consequently, the Working Group, in its opinion No. 34/2000⁷ stated that the extension by two years of a prison term, three times by a parole board after the minimum term had been served, despite the outstanding behavioural record of the person concerned without giving substantive reasons,

and in the absence of effective judicial review, amounted to arbitrary detention. Although that case differs from the present concern of the Working Group in that all information was available in the latter, the principles developed in the Working Group's opinion apply even more so if not all pertinent information, which does not require classification, is known to the prisoner or the courts.»

3.5.3 Kritikk for manglende effektivitet - Riksrevisjonen

Det har kommet kritikk mot INFOFLYT fordi det ikke anses å fungere effektivt for å bekjempe kriminalitet. Med bakgrunn i en spørreundersøkelse stiller Riksrevisjonen i Rapport 3:10 (2009-2010) *Riksrevisjonens undersøkelse av politiets innsats mot organisert kriminalitet*, spørsmål om informasjonsutvekslingen generelt mellom kriminalomsorgen og politiet er tilstrekkelig for å avdekke og forebygge kriminalitet.

Den generelle informasjonsutvekslingen

9 av 24 politidistrikter svarer at de i liten eller i svært liten grad utveksler informasjon med kriminalomsorgen. Av kommentarene til spørreundersøkelsen framgår det at de politidistriktene som i liten grad samarbeider med kriminalomsorgen, mangler rutiner for informasjonsutveksling.

Intervjuundersøkelsen med to regioner i kriminalomsorgen bekrefter forskjeller i rutiner for samarbeid med politiet, både på operativt nivå (lokalt nivå) og på ledernivå (regionalt nivå). De øvrige fire kriminalomsorgsregioner ble spurt ved spørreundersøkelsen.

Dette ga følgende hovedfunn:

- I flertallet av regionene er det etablert rutiner og inngått avtaler mellom enkelte anstalter og lokalt politi
- Flere oppgir at kontakten skjer fra sak til sak via telefon og skriftlig
- Andre har etablert mer formelle samarbeidsmøter
- Et flertall av regionene oppgir at den daglige informasjonsutvekslingen på lokalt nivå fungerer tilfredsstillende
- Flere regioner oppgir at samarbeidet er mer formalisert på ledelsesnivå
- Alle regionene har etablert faste årlige eller halvårlige møter med politiet
- Region sør mener det er utfordrende at det ikke er gitt tydelige føringer om hva kriminalomsorgen skal bidra med når det gjelder å gi politiet etterretningsinformasjon
- Flere regioner savner opplæring for tjenestemennene og rutiner for kvalitetssikring
- Politiet er varsomme med å gi informasjon fordi de mangler kontroll med hvordan informasjonen kan bli brukt
- Ett politidistrikt opplyser at deres trusselvurderinger brukes som grunnlag for kriminalomsorgens forvaltningsvedtak, bl.a. som grunnlag for avslag på permisjoner. Slik kan innsatte få tilgang til sensitiv informasjon gjennom for eksempel innsynsbegjæringer
- Regionene anfører tillit som forutsetning for god informasjonsutveksling

INFOFLYT

Både politidistriktene og kriminalomsorgens regioner har kritiske merknader til hvordan samarbeidet fungerer. Av de 25 politidistriktene som svarte på spørsmålene i undersøkelsen mente 8 at INFOFLYT brukes i svært liten grad, mens 9 mente at INFOFLYT brukes i noen grad. De fire regionene i kriminalomsorgens som ble spurt mente at INFOFLYT er for byråkratisk og omstendelig. Det trengs et operativt verktøy som er mindre tungvint. I tillegg mener én region at man mangler klare føringer for hva som skal rapporteres og når personer ikke lenger skal omfattes av systemet. Det fremheves at det er lite konkrete føringer om hva politiet og kriminalomsorgen skal samarbeide om og på hvilken måte dette skal skje. Samarbeidet er for avhengig av viljen til samarbeid ved den enkelte region og det enkelte politidistrikt.

Fra politiets side fremheves at tilliten til systemet må økes slik at politiet kan være sikre på at opplysninger ikke brukes på en måte som forhindrer politiets oppgaver eller utsetter andre for fare.

Riksrevisjonens vurdering

Riksrevisjonen påpeker (side 72) at jevnlig utveksling av informasjon mellom politiet og kriminalomsorgen er viktig for å avdekke og forebygge organisert kriminalitet. På bakgrunn av resultatene fra spørreundersøkelsen stiller Riksrevisjonen spørsmål ved om informasjonsutvekslingen er tilstrekkelig for å avdekke og forebygge kriminalitet.

3.5.4 Stortingsmeldingene som har behandlet INFOFLYT

Stortingsmelding nr. 37 (2007-2008) «Straff som virker» (s.95-96)

Meldingen gir klart uttrykk for behovet for å videreutvikle både den generelle informasjonsutvekslingen og INFOFLYT spesielt. Også tiltak for å øke kriminalomsorgens evne til å arbeide metodisk og systematisk med uverifisert informasjon berøres:

«Informasjon om sikkerhetsmessige forhold fra innsatte

Kriminalomsorgen mottar til tider opplysninger fra innsatte direkte eller via andre, om rykter eller planer om mulige uønskede hendelser i fortid eller framtid. Bruk av denne type informasjon i kriminalomsorgen, ofte kalt kildeinformasjon, er et omstridt tema.

Det er ofte meget vanskelig å verifisere riktigheten av opplysningene som kommer fram. Foreligger det en reell mulighet for en uønsket hendelse eller ikke? Bruk av denne type informasjon kan samtidig øke avstanden mellom tilsatte og innsatte, vanskeliggjøre rehabiliteringsarbeidet og ha negative konsekvenser for prosesser som fremmer den dynamiske sikkerheten. Det kan være tilfeller der den som er kommet med opplysningen, utsettes for fare. På den annen side foreligger det konkrete eksempler på at bruk av denne type informasjon har bidratt til å forhindre ny kriminalitet og alvorlige hendelser i kriminalomsorgen.

Spørsmålet er således ikke om kriminalomsorgen skal benytte dette virkemiddelet, men hvordan. Det foreligger ingen felles metodikk eller systematikk i håndtering, analyse og bruk av informasjonen. Det er derfor behov for utvikling av et nytt metodisk system som

kan gjøre kriminalomsorgen bedre til å håndtere og bruke denne type informasjon på en måte som ivaretar rettssikkerhetsmessige, sikkerhetsmessige og etiske hensyn.

Informasjonsutveksling mellom kriminalomsorgen og politiet

Informasjon fra politiet er nødvendig for at kriminalomsorgen skal kunne foreta gode risikovurderinger av enkeltindivider og grupper av innsatte og domfelte. Informasjon fra kriminalomsorgen til politiet kan bidra til å avdekke kriminalitet under straffegjennomføring og forebygge ny kriminalitet.

Det er i dag rutinemessige samarbeidsmøter mellom politiet og kriminalomsorgen, hvor informasjon om innsatte og domfelte og eventuelt kriminelle nettverk blir gjennomgått.

For denne type informasjon er det etablert egne rutiner (INFOFLYT).

Formålet og bakgrunnen for INFOFLYT-systemet er at kriminalomsorgen og politiet/påtalemyndigheten skal forebygge kriminalitet og trygge samfunnet ved en systematisert og kvalitetssikret informasjonsutveksling.

Departementet vil påse at Infoflytsamarbeidet videreutvikles med sikte på at kvaliteten på informasjonen er best mulig og at hensynet til samfunnssikkerheten, personvern og rettsikkerhet blir ivare tatt på en god måte.

Departementet vil påse at samarbeidet mellom kriminalomsorgen, politiet og påtalemyndigheten videreutvikles. Et viktig arbeid i denne sammenheng vil være regjeringens forslag til ny lov om politiets og påtalemyndighetens behandling av opplysninger (politiregisterloven), som etter planen skal fremmes våren 2009.»

Meld. St. 7 (2010-2011) «Kampen mot organisert kriminalitet» (s. 94-95)

Meldingen viderefører signalene i «Straff som virker» som omtalt foran:

«(...)Kriminalomsorgen skal ved valg av soningssted, straffeprogresjon og rehabilitering, foreta individuelle sikkerhetsvurderinger av den innsatte. At en innsatt er dømt for organisert kriminalitet vil være et svært viktig moment i en slik helhetsvurdering. Dette innebærer at hensynet til innsattes rehabilitering i mange tilfeller må vike i situasjoner hvor det anses å være fare for ny kriminalitet. På samme måte som for politiets virksomhet, er hensynet til samfunnets sikkerhet et overordnet mål i lovgivningen om kriminalomsorgens behandling av innsatte.

For å gi kriminalomsorgen et bedre grunnlag for å sikkerhetsvurdere varetaktsfengslede og dømte, har regjeringen som mål at samarbeidet mellom kriminalomsorgen, politiet og påtalemyndigheten skal videreutvikles. Et viktig virkemiddel i kampen mot organisert kriminell virksomhet under straffegjennomføring, er å ha et system for informasjonsutveksling mellom politiet og kriminalomsorgen som holder høy kvalitet. (...)

Så langt har utfordringene for kriminalomsorgen, knyttet til organisert kriminelle, i hovedsak vært å forhindre rømning, fritakning/gisselsituasjoner, fortsatt kriminell virksomhet og å ivareta ro og orden i enhetene. Kriminalomsorgens oppgave er først og fremst å identifisere de innsatte som utgjør en sikkerhetsrisiko for å kunne ta hensyn til dette i forbindelse med viktige avgjørelser under straffegjennomføringen. Utfordringen har for eksempel vært å velge «forsvarlig» sikkerhetsnivå under soning og å kunne foreta sikkerhetsmessige forsvarlige beslutninger i forbindelse med progresjon og løslatelse.

En mer variert sammensetning av innsatte stiller kriminalomsorgen overfor nye utfordringer. En voksende del av de innsatte er utenlandske statsborgere knyttet til organisert kriminalitet på tvers av landegrensene. Norske myndigheter har begrenset kunnskap om bakgrunn og tidligere kriminell virksomhet til denne gruppen innsatte.

Videre er det en utfordring at en stor andel innsatte kommer fra land med et annet språk og en annen kulturbakgrunn. Departementet vurderer derfor å tilrettelegge egne fengsler eller fengselsavdelinger for utenlandske innsatte, herunder hvilke særskilte krav til kompetanse og innholdsmessig tilbud som bør være i slike enheter.»

Stortingsmeldingen viser også til Riksrevisjonens rapport, jf. omtalen av den i punkt 3.5.3 og at departementet vil følge opp denne. Likeledes vises det til Sivilombudsmannens kritikk og nedsettelsen av INFOFLYT-utvalget.

Justiskomiteen sluttet seg til departementets anbefalinger for informasjonsutveksling mellom etatene i Innst. 300 S (2010-2011). Det heter følgende i punktet om tverretattlig samarbeid: «Komiteen vil påpeke at når flere instanser skal samarbeide, vil det kunne oppstå usikkerhet og dilemmaer når det gjelder taushetsplikt, i forhold til informasjonsplikten. Komiteen mener det er viktig at taushetsplikt ikke blir et hinder for forebygging, og vil påpeke viktigheten av god informasjonsdeling for å oppnå gode resultater.»

3.6 Oppsummering

Gjennomgangen ovenfor viser at det er behov for en rekke forbedringer av INFOFLYT:

- Behandling av opplysninger i INFOFLYT må få et rettslig grunnlag
- Informasjonssikkerheten må bli bedre
- INFOFLYT må fungere mer effektivt for å være egnet til å forebygge kriminalitet
- Samarbeidet med politiet og tilliten til at informasjon utlevert til kriminalomsorgen brukes etter formålet, må bedres
- INFOFLYT har behov for et moderne saksbehandlingsverktøy
- Det trengs klarere regler og rutiner for hvem som skal registreres og når innsatte skal tas ut av systemet
- Kriminalomsorgen trenger et metodisk system for å vurdere og håndtere ikke-verifisert informasjon
- Kriminalomsorgen må få bedre kunnskap om utenlandske innsatte knyttet til organisert kriminalitet.

4 Gjeldende rett

I dette kapitlet gjennomgås gjeldende rett som berører INFOFLYT: Personopplysningsloven, straffegjennomføringsloven, politiregisterloven, INFOFLYT-rundskrivnet, samt beskyttelsesinstruksens og sikkerhetslovens regler om behandling av gradert materiale. I tillegg beskrives kort det elektroniske fangesakssystemet KOMPIS og saksbehandlings- og arkivsystemet DocuLive.

4.1 Innledning

Det fremgår av straffegjennomføringsloven § 2 at «Straffen skal gjennomføres på en måte som tar hensyn til formålet med straffen, som motvirker nye straffbare handlinger, som er betryggende for samfunnet og som innenfor disse rammene sikrer de innsatte tilfredsstillende forhold.»

For å oppnå disse målene er kriminalomsorgen avhengig av kunnskap om de innsatte. Både nasjonale og internasjonale regler kommer til anvendelse for kriminalomsorgens behandling av personopplysninger. Verken INFOFLYT eller den generelle behandlingen av personopplysninger i kriminalomsorgen, som skjer i fangesakssystemet KOMPIS, er direkte hjemlet i straffegjennomføringsloven, jf. omtalen i kapittel 3. INFOFLYT er heller ikke nevnt i politiregisterloven.

I nye lovbestemmelser i straffegjennomføringsloven – endringslov 17. desember 2010 nr. 85 i nytt kapittel 1a, er det gitt hjemmelsgrunnlag for å behandle personopplysninger i kriminalomsorgen. Bestemmelsene vil imidlertid ikke tre i kraft før det er gitt forskrifter til § 4 e. Utvalget skal etter sitt mandat vurdere om disse bestemmelsene gir tilstrekkelig hjemmel for INFOFLYT.

4.2 Internasjonal lovgivning om menneskerettighetene og personvernet

Det er en rekke forskjellige internasjonale regelsett som danner rammene for norsk lovgivning. Som nevnt i punkt 4.3, er EUs personverndirektiv 95/46 EF gjennomført i norsk rett. Det ble bindende ved innlemmelsen i EØS-avtalen i 1999. Personopplysningsloven bygger direkte på direktivet.

Nedenfor nevnes de to viktigste konvensjonene, som er folkerettslig bindende for Norge:

FN-konvensjonen om sivile- og politiske rettigheter (SP) av 16. desember 1966 er en traktat om menneskerettigheter. Art. 17 regulerer retten til privatliv:

1 «1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep i ære eller omdømme. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.»

Konvensjonens betydning for Norge kommer særlig til uttrykk gjennom FNs menneskerettighetskomite uttalelse til art. 17 om at bestemmelsen krever en rettslig regulering slik at behandling av personopplysninger innen offentlig og privat sektor skjer slik at grunnleggende prinsipper om personopplysningsvern ivaretas. (General Comment nr.16 av 23.3 1988 avsnitt 7 og 10).

Ved menneskerettsloven 21. mai 1999 nr. 30 § 2 er SP gjort gjeldende som norsk lov.

Av større praktisk betydning for Norge er *Den europeiske menneskerettskonvensjonen* av 4. november 1950 (EMK) art. 8 om personvern. Den er også gjennom menneskerettsloven gjort til norsk lov. I følge dens § 3 går konvensjonen foran annen norsk lovgivning ved motstrid.

Artikkel 8 har følgende ordlyd:

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

2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

Vernet etter EMK artikkel 8 (1) er altså begrenset dersom vilkårene i EMK artikkel 8 (2) er oppfylt. Inngrepet mot personvernet må ha hjemmel i lov, ha et relevant formål og være nødvendig i et demokratisk samfunn. I det siste vilkåret ligger det også et krav til proporsjonalitet. Opplysningene må være så beskyttelsesverdige at innsyn i dem vil kunne true samfunnssikkerhet eller andre personers sikkerhet.

Uten at det direkte er uttrykt i EMK art. 8 må opplysningene som registreres ha en tilfredsstillende grad av kvalitet og sannferdighet. Retten til innsyn og kontradiksjon i den enkelte sak må uansett vurderes konkret. Det er altså for eksempel ikke tilstrekkelig å rubrisere opplysningene som «INFOFLYT-informasjon» uten vurdering av om opplysningene kan avgraderes.

Utgangspunktet er at regelen som hjemler inngrepet må være offentliggjort. Regelen må også gi en tilfredsstillende indikasjon på når et inngrep kan bli aktuelt. Samtidig må den berørte kunne overskue konsekvensene av inngrepet. I de tilfellene der regelen gir rom for skjønn, må det gis rammer for skjønnsutøvelsen for å unngå vilkårlige inngrep. I vilkåret «nødvendig i et demokratisk samfunn» ligger det et krav om forholdsmessighet, og dette vilkåret er for øvrig det eneste som begrenser lovgiverens adgang til å gi politiet fullmakter for inngrep som faller inn under de vernede interesser i EMK artikkel 8 (2). Det sentrale ved vilkåret er at det må være forholdsmessighet (proporsjonalitet) mellom mål og midler. Det kreves ikke at inngrepet skal anses uunnværlig, men det er på den annen side ikke tilstrekkelig at tiltaket er «nyttig».

Det er også minstekrav til effektivitet i saksbehandlingen og at den faktisk fører til resultater etter formålet med behandlingen. Det må også kreves at de aktuelle reglene ivaretar dette behovet på en effektiv måte.

Den europeiske menneskerettighetsdomstolen (EMD) har i flere dommer fastslått at art. 8 krever personopplysningsvern. Inngrepet må være i samsvar med lov eller en gyldig offentlig norm, som må være tilgjengelig og forutberegnelig.

I dette ligger også et krav om lik behandling av like forhold. Vilkaarlighet og usaklig forskjellsbehandling er forbudt.

4.3 Personopplysningsloven

4.3.1 Innledning

Personopplysningsloven (lov 14. april 2000 nr. 31.) med tilhørende forskrift er det sentrale og generelle personvernregelsettet i Norge. Loven bygger på personverndirektivet i EU – direktiv 95/46 EF. Norge vil være bundet av avgjørelser fra EU domstolen, og fortolkningen av den norske loven vil påvirkes av tolkningen av det underliggende direktivet.

Formålsbestemmelsen i lovens § 1 sier: *«Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at opplysningene blir behandlet i samsvar med grunnleggende personvern hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.»*

Personopplysningsloven er bindende for kriminalomsorgens behandling av personopplysninger i den utstrekning straffegjennomføringsloven, eller annen lovgivning ikke har egne regler om hvordan personopplysninger skal håndteres. Det følger av fortolkningsprinsippet om *lex specialis*, og fremkommer i tillegg av bestemmelsene i personopplysningsloven, jf. §§ 5 og 6:

- § 5 bestemmer at personopplysningsloven ikke gjelder om en annen særskilt lov regulerer behandlingsmåten
- § 6 bestemmer at loven ikke begrenser annen lovbestemt innsynsrett, og at den behandlingsansvarlige plikter å veilede om retten til å be om innsyn når annen lov gir tilgang til flere opplysninger enn personopplysningsloven gir rett til.

Begrepet «personopplysning» er sentralt og er definert i personopplysningsloven § 2 nr. 1; alle opplysninger og vurderinger som kan knyttes til en enkeltperson. I tillegg til navn vil det kunne være en rekke direkte og indirekte kjennetegn og opplysningstyper som oppfyller lovens kriterium om knytning til en person. Det kan være bilder, fingeravtrykk, fødsels-, bil-, og bankkontonummer med mer. Personopplysningsloven er en generell lov som i utgangspunktet omfatter all behandling av personopplysninger som foretas av enkeltpersoner og juridiske personer.

Noen personopplysninger har større beskyttelsesbehov og er definert som sensitive. I personopplysningsloven er disse listet opp i § 2 nr. 8 og er opplysninger om

- a. *Rasemessig eller etnisk bakgrunn eller politisk, filosofisk eller religiøs oppfatning*
- b. *At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,*
- c. *Helseforhold*
- d. *Seksuelle forhold,*
- e. *Medlemskap i fagforeninger*

Kravene som stilles for å behandle denne typen personopplysninger er strengere og snevrere enn ved annen behandling, noe som fremkommer av lovens § 11 jf. § 9.

Alle opplysninger som kan knyttes til en bestemt person i en av kriminalomsorgens anstalter, jf. bokstav b, vil normalt være sensitive. Når vedkommendes adresse f. eks. er Ullersmo fengsel, vil det være en sterk indikasjon på at vedkommende er dømt for en straffbar handling. Denne opplysningen bør derfor i utgangspunktet behandles som sensitiv.

Med «behandling» etter § 2 nr. 2 omfattes enhver bruk av personopplysninger, som f. eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av disse bruksmåtene.

Loven omfatter all behandling av personopplysninger der man kan finne igjen eller søke fram opplysninger om enkeltpersoner. *For det første* gjelder loven etter § 3 første ledd bokstav a for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. Dette omfatter blant annet all behandling av personopplysninger i forvaltningens saksbehandling.

For det andre omfatter loven også etter § 3 første ledd bokstav b; «*annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister.*» Dette krever at fortegnelsene mv. er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, se lovens § 2 nr. 3.

Utvalget legger til grunn at INFOFLYT i sin nåværende form faller innenfor personopplysningslovens virkeområde. Begrunnelsen er at det er mulig å finne frem til personer via journalføringen av dokumenter som skjer i Justisdepartementets dokumentasjonssenter samt via Kriminalomsorgens fangsakssystem Kompis.

Sivilombudsmannen legger også til grunn at INFOFLYT omfattes av personopplysningsloven i sitt brev til Justisdepartementet 5. juni 2009, hvor han stiller spørsmål om hjemmelsgrunnlaget for INFOFLYT.

Personopplysningsloven omfatter ikke behandling av personopplysninger som følger rettspleielovene, dvs. domstolsloven, straffeprosessloven, tvisteloven og tvangfullbyrdelsesloven mv. Dette framgår av personopplysningsforskriften § 1-3. Disse lovene har delvis egne bestemmelser om behandlingen av personopplysninger. Unntaket er tolket slik at det bare omfatter behandling av enkeltsaker, ikke generelle

krav til behandlingen (for eksempel krav om rettslig grunnlag og internkontroll men ikke krav om innsyn). Bakgrunnen for unntaket er særlig at disse lovene har egne utfyllende regler om behandlingen av personopplysninger.

4.3.2 Behandlingsansvaret

Personopplysningslovens definisjon av behandlingsansvarlige er etter § 2 nr.4: «den som bestemmer formålet med behandling av personopplysninger og hvilke hjelpemidler som skal brukes,». Den behandlingsansvarlige skal sørge for at alle regulatoriske krav til behandlingen er oppfylt. Kravene kan fremkomme av spesiallovgivning eller følge av personopplysningsloven. Plassering av behandlingsansvar presiserer og klargjør hvem som er ansvarlig overfor de registrerte, bl.a. ved tydelig å vise hvem de kan henvende seg til for å gjøre sine rettigheter gjeldende.

I følge lovens forarbeider (Ot.prp. nr. 92 1998-99) i merknadene til § 2 nr. 4, kan behandlingsansvaret deles:

«En og samme behandling kan i enkelte tilfeller ha flere behandlingsansvarlige, jf direktivets formulering «alene eller sammen med andre». Det vil kunne være slik at et overordnet organ, f eks et departement, fastsetter de overordnede formålene for personopplysningsbehandlingen, mens underordnede organer, f eks direktorater, vil detaljere formålene med behandlingen og velge praktiske hjelpemidler. I slike tilfeller vil begge organene kunne være «behandlingsansvarlig» etter loven her, og ha en selvstendig plikt til å oppfylle lovens krav. Man bør imidlertid tilstrebe og plassere behandlingsansvaret i ett og samme organ. I denne sammenheng vil det gjerne være naturlig å plassere behandlingsansvaret der man har den daglige og mest omfattende befatningen med personopplysningene.»

Det er praksis i Datatilsynet for å søke å redusere antall delte behandlingsansvarsløsninger da det kan skape uklarheter i ansvarsforholdene i praksis.

For INFOFLYT ligger behandlingsansvaret i KSF ved ekspedisjonssjefen.

4.3.3 Behandlingsgrunnlag og grunnvilkår

Lovens § 11 er hovedbestemmelsen og angir grunnvilkårene for å kunne behandle personopplysninger:

- a. Opplysninger kan «bare behandles når dette er tillatt etter §§ 8 og 9» - som angir de nærmere vilkår for når behandling av personopplysninger kan skje, se nedenfor
- b. Opplysningene må bare brukes til «uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,»
- c. Opplysningene må «ikke brukes til senere formål som er uforenlig med det opprinnelige formålet med innsamlingen uten at den registrerte samtykker»
- d. Opplysningene må være «(...) tilstrekkelige og relevante for formålet med behandlingen»
- e. Opplysningene må være «(...) korrekte og oppdatert, og ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen (...)».

§ 11 første ledd, bokstav b) krever altså at det skal være et på forhånd angitt formål med behandlingen. Man kan altså ikke først samle inn en mengde opplysninger om en person, for deretter å vurdere hva de skal brukes til. Dette er selve essensen i formålsangivelsen – at innhenting av personopplysninger skal være formålsstyrt for bl.a. å forhindre at en ikke samler inn mer enn det som er nødvendig og relevant. Dette fremkommer også av lovens § 11 bokstav d) – «tilstrekkelige og relevante for formålet med behandlingen».

For å behandle personopplysninger er det etter lovens § 8 satt opp 3 alternative vilkår. Grunnlaget kan være *for det første* et gyldig samtykke eller *for det andre* at det er fastsatt i lov at opplysninger kan behandles. Det *tredje grunnlaget* er at behandlingen er nødvendig for å oppfylle ulike offentlige eller private interesser og forpliktelser, som oppregnet i § 8 bokstavene a)-f).

I tillegg gjelder vilkårene i lovens § 9 for å kunne behandle sensitive personopplysninger. Personopplysninger i INFOFLYT vil være sensitive, jf. § 2, nummer 8, bokstav b), som sier at opplysninger om «*at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling*» er sensitive. De alternative vilkårene i § 9 er:

Sensitive personopplysninger (jf. § 2 nr. 8) kan bare behandles dersom behandlingen oppfyller et av vilkårene i § 8 og

- a) den registrerte samtykker i behandlingen,*
- b) det er fastsatt i lov at det er adgang til slik behandling,*
- c) behandlingen er nødvendig for å beskytte en persons vitale interesser, og den registrerte ikke er i stand til å samtykke,*
- d) det utelukkende behandles opplysninger som den registrerte selv frivillig har gjort alminnelig kjent,*
- e) behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav,*
- f) behandlingen er nødvendig for at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter,*
- g) behandlingen er nødvendig for forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling eller for forvaltning av helsetjenester, og opplysningene behandles av helsepersonell med taushetsplikt, eller*
- h) behandlingen er nødvendig for historiske, statistiske eller vitenskapelige formål, og samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for den enkelte.*

For å behandle *sensitive* personopplysninger må som nevnt et av vilkårene i § 8 være oppfylt og i tillegg ett eller flere av vilkårene i § 9. Bestemmelsen i § 9 første ledd bokstav b) er et relevant kriterium, nemlig at det er fastsatt i lov at det er adgang til slik behandling.

Samtykke etter bokstav a må være gyldig, jf. § 2 nummer 7): «*samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte(...)*». Ved kriminalomsorgens behandling av opplysninger vil ikke en innsatts samtykke alltid være gyldig. Vedkommende vil kunne være i en tvangssituasjon. Man må derfor finne et annet gyldig grunnlag for behandlingen enn samtykke, for eksempel lovgrunnlag etter bokstav b.

Dersom behandlingen ikke har *uttrykkelig* hjemmel i lov, eller det finnes unntak fra konsesjonsplikten, se personopplysningsforskriftens kapittel III og IV, kan et rettslig grunnlag være konsesjon fra Datatilsynet etter § 33. Har behandlingen hjemmel i lov, er det tilstrekkelig å melde behandlingen til Datatilsynet etter §§ 31 og 32.

Det ligger som en forutsetning for å oppfylle hensynene til sikkerhet i det enkelte fengsel, samfunnssikkerheten generelt og for å motvirke straffbare handlinger i straffegjennomføringsloven § 2, at vitale opplysninger nedtegnes og bevares som grunnlag for gjenfinning for andre tjenestemenn med tjenstlig behov. Innsatte kan representere farer for samfunnet. Kriminalomsorgen vil derfor regelmessig ha behov for oppdaterte risikovurderinger om innsatte i samband med vurdering av sikkerhetsnivå i fengsel, permisjoner, prøveløslatelse med mer. Som kommentar til dette spørsmålet, sier Datatilsynet i den nevnte kontrollrapporten av 25. januar 2008 at «*Det at behandlingen av opplysningene er en nødvendig forutsetning for at kriminalomsorgen skal gjennomføre sine øvrige plikter, tilfredsstillende etter Datatilsynets vurdering ikke kravet til lovhjemlet behandling etter personopplysningsloven § 9 litra b.*»

Opplysninger skal normalt slettes når formålet ikke lenger begrunner behandling, se personopplysningsloven §§ 11 første ledd bokstav e), 27 og 28. Om det er nødvendig å bevare opplysningene lenger enn det opprinnelige formålet tilsier, må dette reguleres.

4.3.4 Informasjonsplikt

Etter personopplysningsloven §§ 19 og 20 har den behandlingsansvarlige informasjonsplikt overfor den registrerte, uavhengig av om opplysningene samles inn fra den registrerte selv eller fra andre. Informasjonsplikten skal sikre at den registrerte får kunnskap om behandlingen av opplysninger. Dette innebærer at den registrerte skal informeres om sentrale forhold ved behandlingen, som for eksempel hvem som er behandlingsansvarlig, hva som er formålet med behandlingen og om opplysningene vil bli utlevert og eventuelt til hvem. I noen tilfeller kan de registrerte informeres samlet gjennom informasjon til allmennheten. Et eksempel er at et offentlig organ på sine nettsider gir opplysninger om hvordan de i gitte sammenhenger forvalter personopplysninger. Velges en slik løsning må en sikre at de registrerte vet hvor informasjonen er tilgjengelig. I de tilfellene der informasjonsplikten knyttes til den enkelte, innebærer plikten at den enkelte må informeres om at det behandles opplysninger om vedkommende, hvilket formål som ligger til grunn, hvem som er ansvarlig og hvem disse opplysningene eventuelt ble utlevert til mv.

Her nevnes også noen av unntakene fra informasjonsplikten. Et unntak er at den registrerte kjenner til behandlingen av opplysningene og de viktigste

behandlingsvilkårene, se § 19 annet ledd. Dersom opplysningene er samlet inn av andre enn den registrerte, er det unntak for situasjoner hvor «innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov», jf. personopplysningsloven § 20 annet ledd bokstav a. Tanken er at den registrerte antas å kjenne til at en slik behandling skjer.

Et annet unntak som utvalget har sett på og som kan være viktig å se hen til i INFOFLYT-sammenheng er når andre hensyn må gå foran den enkeltes rett til informasjon, jf. § 23 dersom «*det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger*». Videre er opplysninger som er taushetsbelagt også unntatt informasjonsplikt, jf. personopplysningsloven § 23 første ledd bokstav d.

4.3.5 Innsyn

En av de sentrale rettighetene for personer som er registrert er at de har innsyn i de opplysninger som er registrert om dem. Personopplysningsloven § 18 regulerer to typer innsyn: Det generelle og det spesielle. Enhver har rett til å kreve innsyn i hvilke behandlinger den behandlingsansvarlige foretar, og i tillegg rett til ytterligere opplysninger om den enkelte behandling dersom vedkommende er registrert.

Den registrerte har i tillegg rett til å kreve innsyn i de opplysninger som behandles om ham, og sikkerhetstiltakene ved behandlingen. Personopplysningsloven har ingen unntak basert på at den registrerte antas å kjenne til opplysningene, slik den har for informasjonsplikten. Derimot gjelder de samme unntakene fra innsynsretten som for informasjonsplikten etter personopplysningsloven § 23 om taushetsbelagte opplysninger mv.

4.3.6 Meldeplikt og konsesjonsplikt

Etter lovens § 33 kreves det konsesjon fra Datatilsynet for å behandle sensitive (jf. lovens § 2 nr. 8) personopplysninger dersom de ikke er avgitt uoppfordret. Etter § 33 fjerde ledd gjelder ikke konsesjonsplikt når behandling av personopplysninger i stat og kommune har hjemmel i egen lov. Se også § 5 som slår fast at personopplysningsloven ikke gjelder når det er en «*særskilt lov som regulerer behandlingsmåten*».

Datatilsynet kan bestemme at også ikke-sensitive personopplysninger kan kreve konsesjon dersom behandlingen åpenbart vil krenke tungtveiende personverninteresser.

Spørsmålet om hva som er det rettslige grunnlaget for kriminalomsorgens behandling av personopplysninger har vært en sentral problemstilling i kriminalomsorgens kontakt med Datatilsynet og Sivilombudsmannen vedrørende KOMPIS og INFOFLYT, se kapittel 3 om bakgrunnen for dette utvalget og historikken.

Hvis behandlingen ikke er konsesjonspliktig er lovens hovedregel (§ 31) at den behandlingsansvarlige skal gi melding til Datatilsynet før

- a. *behandling av personopplysninger med elektroniske hjelpemidler,*

b. Opprettelse av manuelt personregister som inneholder sensitive personopplysninger.

Meldingen skal gis senest 30 dager før behandlingen tar til.

Dersom det skulle være uklart for den behandlingsansvarlige om en planlagt behandling vil kreve konsesjon, kan den behandlingsansvarlige kreve at Datatilsynet vurderer om den aktuelle behandlingen vil kreve konsesjon, jf. § 33, 3. ledd.

4.3.7 Øvrige plikter i loven som er særlig sentrale for INFOFLYT

Særlig sentrale er kravene til planlagte tiltak for informasjonssikkerhet og internkontroll. For å innfri kravene er det et krav om at virksomheten gjennomfører risiko- og sårbarhetsanalyse (personopplysningsforskriften § 2-4) og dokumenterer resultatene av denne. Lovens § 13 stiller krav til informasjonssikkerheten og til at sikkerhetstiltakene er dokumentert. Dette innebærer planlegging og gjennomføring av systematiske og egnede informasjonssikkerhetstiltak for å sikre konfidensialitet, integritet og tilgjengelighet.

Lovens § 14 om internkontroll pålegger den behandlingsansvarlige en plikt til å vurdere behov for tiltak for å innfri kravene i personvernlovgivningen. En viktig del av dette er å sikre opplysningenes kvalitet (integritet). Tiltakene kan være organisatoriske, juridiske, fysiske eller kompetansegivende.

Reglene i personopplysningsloven gjelder for alle som behandler personopplysninger, og vil således være supplerende for annen regulering som gjelder innenfor det enkelte rettsområdet ved at de kommer inn dersom noe ikke er særlig regulert.

4.3.8 Tilsyn og klage

Datatilsynet er det sentrale tilsynsorganet i henhold til personopplysningsloven og etter noen spesiallover, særlig innen helsefeltet og lov om Schengen Information System (SIS). Datatilsynet kan gi pålegg om opphør eller atferdsendring, og har i tillegg et sanksjonsregime de kan benytte i form av tvangsmulkt, overtredelsesgebyr og anmeldelse til politiet, i og med at personopplysningsloven inneholder en straffehjemmel, jf. § 48. Det kan også ilegges erstatning i noen tilfeller, jf. lovens § 49.

4.4 Straffegjennomføringsloven

4.4.1 Innledning

Straffegjennomføringsloven har fått et nytt kapittel 1a ved lov 17. desember 2010 nr. 85. om behandling av personopplysninger i kriminalomsorgen. Endringsloven er ikke trådt i kraft i påvente av at det gis utfyllende forskrifter. Bakgrunnen for de nye lovreglene er Datatilsynets pålegg om å etablere et rettslig grunnlag, se omtalen i punkt 3.5.1 og forarbeidene i Prop. 151 L (2009-2010) på side 7.

Utvalget har registrert at det er en viss usikkerhet i etaten i hvor langt kriminalomsorgens adgang til å behandle personopplysninger om innsatte og

tredjepersoner med tilknytning til disse for å forebygge kriminalitet, herunder graden av samarbeid med politiet, strekker seg. Særlig gjelder det grensegangen mellom politiets oppgaver med å bekjempe kriminalitet og kriminalomsorgens oppgaver med å sørge for sikkerhet i fengsel og motvirke at de innsatte begår kriminalitet.

Utvalget skal ifølge sitt mandat utrede om straffegjennomføringsloven §§ 4c (formål med å behandle personopplysninger) og 4d (hvilke personer kriminalomsorgen kan behandle opplysninger om) gir en klar og tydelig hjemmel for informasjonsutveksling med politiet. De sentrale drøftingene om grensegangen mellom politiets- og kriminalomsorgens oppgaver i forarbeidene i nevnte proposisjon, omtales derfor i det følgende.

I Prop. 151 L kom det fram motstridende syn på kriminalomsorgens rolle i samarbeidet med politiet. På side 15 i proposisjonen vises til departementets høringsbrev der det stod: *“I tråd med formålsføresegna i straffegjennomføringslova § 2, som også viser til forebygging av kriminelle handlingar, gjer departementet framlegg om å føye til ein ny bokstav d i § 4c som kan lyde: “d) forebygge nye straffbare forhold.” Rett nok blir det i bokstav b vist til opphealding av ro og orden og av tryggleiken i samfunnet, men det dekker ikkje alle straffbare forhold.”*

Datatilsynet var uenig og mente at å forebygge nye straffbare handlinger først og fremst er en politioppgave, se proposisjonen på side 17.

Departementet skriver om dette i proposisjonen på side 21: *«Datatilsynet er kritisk til formålet om å forebygge nye straffbare handlingar og peiker på at forebygging først og fremst er ei politioppgåve. Straffegjennomføringa har likevel også som formål å motverke nye straffbare handlingar, (...), men dette gir uttrykk for eit overordna formål knyt til domfelte og innsette. Dette må ein skilje klart frå den politioppgåva det er å etterforske og hindre straffbare handlingar.»*

Dette synes å innebære at kriminalomsorgen verken i eller utenfor INFOFLYT har et tilstrekkelig rettslig grunnlag for å behandle personopplysninger for forebyggingsformål. Det samme gjelder i hvilken grad kriminalomsorgen kan bidra med opplysninger til politiets etterforskning.

I bokstav § 4c bokstav b fremgår at kriminalomsorgen kan behandle personopplysninger for å opprettholde ro, orden og ivareta sikkerheten for ansatte, innsatte og samfunnet for øvrig. Heller ikke denne bestemmelsen gir kriminalomsorgen en klar hjemmel for å utøve forebygging og etterforskning. Dette er oppgaver som er tillagt politiet. Kriminalomsorgen skal derimot behandle opplysninger for å forhindre og motvirke at de enkelte innsatte begår kriminalitet mens de soner straff.

§ 4 d gir heller ikke kriminalomsorgen adgang til å behandle personopplysninger om tredjepersoner utenfor fengslet for å forebygge kriminalitet. Det dreier seg om

tredjepersoner som ikke har kontakt med kriminalomsorgen men som har kontakt med- eller forsøker å kontakte den innsatte (og omvendt) med det formål å planlegge og begå kriminalitet sammen med den innsatte. Det vises her blant annet til Prop 151 L på side 22 der departementet konkluderer med at «*registrering av tredjepersonar er ei oppgave for politiet.*»

INFOFLYT skal i følge instruksjen tjene som informasjonsutvekslingssystem for å klarlegge risiko for kriminalitet. For dette formål trenger kriminalomsorgen etter utvalgets oppfatning en entydig hjemmel for å behandle opplysninger om innsatte og berørte tredjepersoner. Utvalget mener dessuten at en ensartet ordlyd i formålsbestemmelsene i straffegjennomføringsloven og politiregisterloven er en fordel ved behandling av personopplysninger i INFOFLYT. Det vises til utvalgets vurderinger i punkt 8.1.1, lovforslagene i kapittel 11.1 og forslaget til forskrift § 2 om tredjepersoner.

4.4.2 De nye lovreglene om behandling av personopplysninger i straffegjennomføringsloven

Det nye kapittel 1a med paragrafene 4a til § 4e regulerer forholdet til andre lover, definerer behandlingsansvaret, angir kriminalomsorgens formål med å behandle personopplysninger og hvem det kan behandles opplysninger om og angir til slutt en hjemmel til å gi forskrifter:

- § 4a slår fast at personopplysningsloven gjelder “med utfyllende regler som fastsatt i dette kapitlet.” I forarbeidene i Prop. 151 L 2009-2010 på side 38 heter det at “*Føresegna presiserer at personopplysningslova gjeld med utfyllande reglar som er fastsette i kapittel 1a. Presiseringa er teken inn av pedagogiske grunnar*”. Dette innebærer at kapittel 1a med forskrifter ikke kan svekke personvernrettighetene i personopplysningsloven.
- § 4b definerer behandlingsansvaret og tilsvare personopplysningloven § 2 nr. 4. Forskjellen fra personopplysningsloven er at § 4b har tilføyd “*(...)alene eller sammen med andre, bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes.*” I forarbeidene begrunnes motsetningen til personopplysningsloven med at en etter denne bestemmelsen kan ha to behandlingsansvarlige med delt behandlingsansvar og at en slik løsning kan være praktisk for fangesakssystemet Kompis. I dag har kriminalomsorgens IKT-tjeneste KITT systemansvaret for Kompis.
- § 4c angir formålene med behandlingen. Det angis 5 formål i bokstavene a-e. Behandling kan foretas når det er nødvendig for å:
 - a) *planlegge, administrere og gjennomføre reaksjoner og tvangsmidler etter straffegjennomføringsloven § 1, dvs. kunne gjennomføre straff og varetekt på en forsvarlig måte.*
 - b) *oppretholde ro og orden og ivareta sikkerheten for ansatte, innsatte, domfelte og samfunnet for øvrig.* I forarbeidene nevnes en omfattende liste relevante opplysninger for sikkerheten. Dette er tidligere dommer, disiplinærbrudd, rømninger, rusproblemer, rettspsykiatriske erklæringer, utagerende atferd og

bruk av tvangsmidler. I tillegg kan det behandles opplysninger om andre innsatte som ikke bør ha kontakt med den aktuelle innsatte.

c) sikre innsatte og domfelte tilfredsstillende forhold under straffegjennomføringen og tilby dem et innhold som skal bidra til å motvirke ny kriminalitet, herunder legge forholdene til rette for tjenester fra andre etater med sikte på å fremme innsattes og domfeltes tilpasning til samfunnet. I forarbeidene nevnes at bare opplysninger som direkte påvirker valget av tiltak etter bestemmelsen kan behandles etter c, jf. formålet i straffegjennomføringsloven § 2 om å motvirke straffbare handlinger. Som eksempel nevnes helseopplysninger som bare helsetjenesten kan behandle og helseopplysninger som er nødvendig for en forsvarlig og tilrettelagt straffegjennomføring.

d) sikre barns rett til samvær med foreldrene.

e) varsle fornærmede eller deres etterlatte, jf. straffegjennomføringsloven § 7b.

- § 4d angir hvem det kan behandles opplysninger om etter formålet i § 4c:
 - a) domfelte og innsatte*
 - b) pårørende og andre som har kontakt med eller prøver å oppnå kontakt med domfelte og innsatte.*
 - c) personer som har eller søker tilgang til fengselsområder og*
 - d) domfeltes eller innsattes barn og barnets pårørende eller andre omsorgspersoner*

I forarbeidene nevnes “*Typiske eksempler*” for å behandle opplysninger om aktuelle personer i kretsen rundt den innsatte. Formålet kan være å varsle dem hvis det skjer noe, besøkende, samboere når straffegjennomføringen skjer utenfor fengsel (for eksempel ved elektronisk kontroll - EK), ressurspersoner for den innsatte, kontaktpersoner ved skole og arbeidsplass og arbeidsgivere.

Det nevnes ikke om det også kan behandles personopplysninger om tredjepersoner som mistenkes å planlegge kriminalitet i samarbeid med den innsatte. Sett i sammenheng med omtalen av dette i forarbeidene på side 22 der departementet framhever at dette er en politioppgave, gir § 4d neppe adgang til dette. Det legges derfor til grunn at slike personer ikke kan anses å falle under «*personer som har kontakt eller prøver å oppnå kontakt(...)*», se punkt 4.4.1 og utvalgets vurderinger i punkt 8.1.7. Dersom fengselet får opplysninger om at tredjepersoner er involvert i kriminelle handlinger med forgreininger til innsatte, skal politiet varsles.

- § 4e er forskriftshjemmelen. Forskriftene skal regulere en rekke forhold:
 - a) hvilket rettslig grunnlag som hjemler behandlingen,*
 - b) formålet med behandlingen,*
 - c) hvem som er behandlingsansvarlig,*
 - d) hvilke opplysningskategorier som kan registreres,*
 - e) hvem i kriminalomsorgen som har tilgang til opplysningene,*
 - f) adgang til å utlevere opplysningene,*

- g) *informasjonsplikt, innsyn, retting, sperring og sletting av opplysninger,*
- h) *informasjonssikkerhet og internkontroll.*

Det understrekes i forarbeidene at listen ikke er uttømmende. Det forutsettes at nødvendige forskrifter gis før loven kan tre i kraft.

4.4.3 Gjeldende regler om unntak fra forvaltningslovens regler om taushetsplikt, partsinnsyn, plikten til å begrunne vedtak og adgang til å utlevere opplysninger til andre

Taushetsplikt

Straffegjennomføringsloven § 7 om saksbehandlingsregler regulerer unntak fra og presiseringer til forvaltningsloven §§ 18 og 19. § 7 første ledd bokstav h slår fast: *«Enhver som (...) utfører tjeneste eller arbeid for kriminalomsorgen, har taushetsplikt om det vedkommende i forbindelse med tjenesten får vite om sikkerhetsmessige forhold i fengslene.»*

Taushetsplikten omfatter også plikt til taushet overfor innsatte som er parter etter forvaltningsloven i tilfeller som nevnt i § 7 første ledd bokstav c om unntak fra retten til partsinnsyn og første ledd bokstav d om unntak fra plikten til å begrunne vedtak. Se omtalen av taushetsplikten i proposisjonen - Ot.prp. nr. 5 (2000-2001) på sidene 43-45.

Det understrekes at bestemmelsene bare gjelder unntak fra partsrettighetene etter forvaltningsloven og får ikke anvendelse på personvernlovgivningen. Straffegjennomføringsloven har ikke spesialregler for personvern, herunder innsyn. Personopplysningsloven får derfor anvendelse fullt ut. Dette innebærer at unntakene fra informasjonsplikt og innsyn i personopplysningsloven § 23 gjelder for kriminalomsorgen. Som nevnt over i punkt 4.2 har § 23 unntak fra innsynsretten dersom det er nødvendig av hensyn til forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger, eller opplysningene er taushetsbelagt. Se omtalen av forholdet mellom politiregisterloven og personopplysningsloven når det gjelder innsynsretten i punkt 6.3.3.

Unntak fra partsinnsyn etter § 7 første ledd bokstav c.

§ 7 første ledd c dels begrenser og dels presiserer unntakene fra domfelte og innsattes rett til dokumentinnsyn i forhold til forvaltningsloven §§ 18-20.

Bestemmelsen slår fast at en part ikke har rett på innsyn i et dokument som inneholder opplysninger som det av hensyn til en annen person anses utilrådelig at parten får kjennskap til. En annen person kan for eksempel være andre domfelte eller innsatte, pårørende. Unntak kan også begrunnes i beskyttelse av kriminalomsorgens eller politiets kilder i forbindelse med etterforskning av straffbare forhold.

Videre kan opplysninger i et dokument unntas fra innsyn dersom det er utilrådelig av sikkerhetsmessige hensyn eller av hensyn til etterforskning av straffbare forhold. Dette

gjelder i hovedsak hensyn til fengselssikkerheten, herunder arbeidet med å bekjempe narkotika i fengsel og forøvrig motvirke straffbare handlinger.

Unntak fra plikten til å begrunne vedtak etter § 7 første ledd bokstav d

Etter bokstav d kan det gjøres unntak fra plikten til å begrunne vedtak etter forvaltningsloven § 24 hvis begrunnelsen vil røpe opplysning som er unntatt fra innsyn etter bokstav c. Begrunnelse kan helt utelates i den utstrekning begrunnelse ikke kan gis uten å røpe opplysninger som parten etter forvaltningsloven § 19, jf. straffegjennomføringsloven § 7 bokstavene c og h, ikke har krav på å bli kjent med.

Adgang til å utlevere taushetsbelagte opplysninger til andre

Straffegjennomføringsloven mangler, til forskjell fra straffeprosessloven og politiregisterloven, unntak fra taushetsplikten gjennom en generell hjemmel til å utlevere personopplysninger til andre. Enkelte bestemmelser gir en særskilt adgang. Et eksempel er § 36 siste ledd om varsling av fornærmede når den innsatte innvilges permisjon og straffavbrudd. Det finnes i spesiallovgivningen bestemmelser om kriminalomsorgens plikt til å utlevere opplysninger om de innsatte til andre offentlige organer, som for eksempel nevnes barnevernloven § 6-4 som pålegger alle offentlige myndigheter å melde fra om mistanker om mishandling omsorgssvikt mv. uten hinder av taushetsplikt.

I hvilken grad kriminalomsorgen kan gi politiet taushetsbelagte opplysninger, oppleves av etaten som usikkert. Grunnlaget for kriminalomsorgens adgang til å utlevere slike opplysninger må finnes i forvaltningsloven. Forvaltningsloven § 13 b nr. 5 og 6 gir forvaltningsorganer rett til å utlevere informasjon til andre organer i visse tilfeller. Nr. 5 gir kriminalomsorgen adgang til å gi andre organer visse opplysninger som kriminalomsorgen trenger å utlevere for å fremme egne oppgaver etter lov og instruks. Adgangen omfatter ikke utlevering i mottakerorganets interesse slik som etter politiregisterloven § 30.

Bestemmelsen i § 13 nr. 6 omhandler avgiverorganets rett til å anmelde eller gi opplysninger om lovbrudd til påtalemyndigheten eller kontrollmyndigheten når dette er ønskelig av allmenne hensyn eller har naturlig sammenheng med avgiverorganets oppgaver. Dette er en hjemmel som regelmessig vil være aktuell for kriminalomsorgen.

I tillegg til taushetspliktsbestemmelsene gjelder bestemmelsene etter sikkerhetsloven og beskyttelsesinstruksen dersom opplysningene er graderte, jf. omtalen av disse bestemmelsene i punkt 4.7.

Straffegjennomføringsloven § 7 første ledd bokstav b tillater at saksbehandlingen kan være muntlig dersom det haster. Muntlighet kan være aktuelt i mange saker ved utlevering av opplysninger i INFOFLYT. Det vises til forslaget til krav om nedtegning av opplysninger ved muntlig utlevering av opplysninger i forslaget til forskrift § 7 annet ledd.

Forskriftshjemmelen i straffegjennomføringsloven § 4e bokstav f forutsetter at det blir gitt forskrift om utlevering. En forskrift kan imidlertid ikke åpne for en videre utleveringsadgang enn det er lovhjemmel for, se forslaget til utleveringshjemmel for INFOFLYT i ny § 4g og punkt 8.1.4 der utvalget foreslår at en generell utleveringshjemmel utredes.

4.5 Politiregisterloven

Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) er ikke trådt i kraft i påvente av at det utarbeides forskrifter. Loven og tilhørende forskrift skal etter planen tre i kraft i desember 2012. Politiregisterloven og forskriftene til denne vil regulere politiets måte å behandle personopplysninger på, og vil således være av betydning for utvalgets forslag til regelendringer for kriminalomsorgens behandling av personopplysninger.

Politiregisterloven gjelder for politiets og påtalemyndighetens behandling av opplysninger, med unntak av behandling av opplysninger som er del av politiets forvaltningsvirksomhet eller sivile gjøremål. Loven samler regelverket om politiets taushetsplikt og utlevering av opplysninger fra politiet til andre etater.

Utvalgets mandat forutsetter at regelforslagene tilpasses den nye politiregisterloven. De viktigste bestemmelsene med relevans for INFOFLYT og øvrig informasjonsutveksling omtales nedenfor.

4.5.1 Generelt om politiregisterlovgivningen

Politiets rett og plikt til å utlevere opplysninger er regulert i kapittel 5 og 6 i politiregisterloven. Utkast til forskrift er sendt på høring. I det følgende vil utvalget bare omtale de bestemmelsene som er av interesse for utlevering av opplysninger til kriminalomsorgen, herunder via INFOFLYT-kanalen. Det er likevel nødvendig å gjøre innledningsvis kort rede for visse grunnleggende trekk ved måten taushetspliktsbestemmelsene i politiregisterloven er bygget opp på.

Selv om taushetspliktsbestemmelsene i politiregisterloven i det alt vesentlige er en videreføring av gjeldende rett, er det likevel foretatt enkelte strukturelle endringer. Ved utformingen av de gjeldende taushetspliktsbestemmelser for politiet og påtalemyndigheten i henholdsvis straffeprosessloven, politiloven og strafferegistreringsloven har man tatt utgangspunkt i *hvilket formål opplysningene er innhentet for*, og sekundærbruken er regulert deretter. I politiregisterloven vil det derimot være styrende *hvilke formål opplysningene utleveres til*, uavhengig av hvor de kommer fra, så lenge de kommer fra politimessig arbeid. Det innebærer at det er formålet med utleveringen som er avgjørende, uavhengig av om opplysningene kommer fra straffesaker, politiets registre eller annet politimessig arbeid. Politiregisterloven kapittel 6 regulerer nærmere hvilke formål opplysninger kan utleveres til. Det mest sentrale skille går mellom utlevering i politiets egen interesse og mottakerens interesse. Når utlevering skjer i politiets interesse er dette

sammenfallende med at opplysningene utleveres til politimessige formål, herunder til etterforskning og kriminalitetsforebyggende virksomhet.

I tillegg til dette må det skilles mellom politiets utleveringsrett og utleveringsplikt av opplysninger. Bestemmelsene om begrensninger i taushetsplikten i politiregisterloven kapittel 6 gir politiet adgang til å utlevere opplysninger, det vil si at ingen av disse bestemmelsene pålegger politiet en plikt til å utlevere opplysninger. §§ 30 og 31, som omhandler utlevering av opplysninger til henholdsvis offentlige organer og private i deres interesse, inneholder imidlertid en forskriftshjemmel hvoretter Kongen i forskrift kan fastsette hvilke offentlige eller private mottakere det «skal» utleveres opplysninger til. En slik utleveringsplikt er i dag regulert i påtaleinstruksen kapittel 5, og er videreført i utkast til kapittel 10 i politiregisterforskriften. Utover dette inneholder politiregisterlovgivningen ingen bestemmelser om utleveringsplikt. Dersom politiet skal ha en utleveringsplikt utover det som er nevnt, må dette fastsettes i spesiallovgivningen.

I denne sammenheng kan også nevnes at politiregisterloven § 35 annet ledd åpner for at politiet og påtalemyndigheten kan pålegge enhver som utfører tjeneste for statlig eller kommunalt organ taushetsplikt om opplysninger når organet mottar opplysninger som er taushetsbelagt i henhold til politiregisterloven. Dette innebærer at politiet vil kunne pålegge enhver som arbeider i kriminalomsorgen taushetsplikt, herunder når det utleveres opplysninger til bruk i INFOFLYT.

4.5.2 Politiets rett og plikt til å utlevere opplysninger til Kriminalomsorgen

Som nevnt i punkt 4.5.1 må det skilles mellom utlevering av opplysninger avhengig av hva som er formålet med utleveringen. Det skillet som i vår sammenheng er av størst interesse er om utlevering skjer i politiets interesse eller i mottakerorganets interesse. Utlevering i politiets interesse er sammenfallende med at politiet kan utlevere opplysninger til politimessige formål, som i politiregisterloven § 2 nr. 13 er definert som politiets kriminalitetsbekjempende virksomhet, herunder etterforskning, forebyggende arbeid, ordenstjeneste og politiets service- og bistandsfunksjon samt føring av vaktjournaler. Disse ulike politimessige formålene gjenspeiler seg i §§ 26, 27 og 28 som regulerer taushetsplikt når opplysninger skal utleveres i den enkelte straffesak (§ 26), ved avvergende og forebyggende virksomhet (§ 27) og ved politiets andre oppgaver (§ 28). I forhold til utlevering av opplysninger til INFOFLYT er det særlig § 27 som er av interesse. Bestemmelsen åpner for at politiet kan utlevere opplysninger for å avverge eller forebygge et lovbrudd, jf. § 27 første og annet ledd. I tillegg må det i henhold til bestemmelsens tredje ledd foretas en forholdsmessighetsvurdering i den konkrete situasjon, der det skal særlig legges vekt på om opplysningene formidles til en mottaker som er underlagt taushetsplikt, hvordan det kan forventes at mottaker benytter opplysningene og om opplysningene etter sin art eller kilde er beheftet med usikkerhet. I utkast til forskriften § 4-2 om nødvendighetskravet er det gitt ytterligere kriterier som skal legges til grunn ved en forholdsmessighetsvurdering. Herunder skal det legges vekt på hva som er formålet med behandlingen, hvilke opplysninger som skal behandles, om behandlingen gjelder alvorlig eller mindre alvorlig kriminalitet og behandlingens omfang av personer som får tilgang til opplysningene. I forbindelse med

utlevering av opplysninger til politimessige formål legger utkastet til forskriften ikke opp til noen ytterligere begrensninger av adgangen til å utlevere visse typer opplysninger, som for eksempel kriminaletterretningsinformasjon, jf. nærmere om dette nedenfor.

Utlevering av opplysninger i mottakerorganets interesse er regulert i § 30. I følge denne bestemmelsen er taushetsplikten ikke til hinder for at opplysninger utleveres til andre offentlige organer, herunder kriminalomsorgen, i deres interesse dersom dette er nødvendig for å fremme mottakerorganets oppgaver etter lov eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte. I utkast til politiregisterforskriften gis det i § 9-6 en opplisting av hvilke offentlige organer det kan utleveres opplysninger til og til hvilket formål. Opplistingen er ikke ment å være uttømmende. Kriminalomsorgen er nevnt i bestemmelsens første ledd bokstav j, hvoretter politiet kan utlevere opplysninger til kriminalomsorgen til straffegjennomføringsmessige formål.

Selv om verken lovens § 30 eller forskriftens § 9-6 gir uttrykk for noen begrensninger med henblikk på hvilke typer opplysninger som kan utleveres i mottakerorganets interesse, er ikke det ensbetydende med at det ikke finnes begrensninger. Som det fremgår av forskriften § 9-1 gjelder bestemmelsene i forskriftens kapittel 9 bare dersom ikke noe annet er bestemt i blant annet forskriftens del 11, som omhandler politiets registre. En slik begrensning finnes for eksempel i § 47-9 for etterretningsregistre, der det er uttalt at etterretningsinformasjon bare kan utleveres i politiets interesse eller dersom vesentlige samfunns- eller sikkerhetsmessige hensyn tilsier det. Dette innebærer blant annet at slike opplysninger ikke kan utleveres til kriminalomsorgen dersom utlevering utelukkende er begrunnet i kriminalomsorgens interesse. Dette kan likevel ikke antas å være av nevneverdig praktisk betydning, idet kriminalomsorgens lovregulerte oppgaver med henblikk på sikkerhet mv. regelmessig vil være sammenfallende med politimessige formål og de øvrige formålene som er nevnt i § 47-9.

I tillegg er det i henhold til § 30 gitt forskrifter om i hvilke tilfeller politiet har en utleveringsplikt til andre organer. Dette er regulert i kapittel 10 i utkastet til forskriften og er i hovedsak en videreføring av kapittel 5 i påtaleinstruksen. Det er viktig å merke seg at kapittel 10 i utkast til forskriften regulerer utleveringsplikt av eget tiltak, og må således ikke forveksles med utleveringsplikt etter anmodning fra et annet organ. Sistnevnte tilfeller må regelmessig være regulert i spesiallovgivningen. At overskriften i kapittel 10 lyder «underretningsplikt», mens kapittel 5 i påtaleinstruksen heter «meldeplikt» innebærer ingen realitetsforskjell. Bakgrunnen for de ulike betegnelsene er at «meldeplikt» i politiregisterloven innebærer at den behandlingsansvarlige må sende melding til Datatilsynet, jf. kapittel 10 i politiregisterloven. Det var derfor nødvendig å innføre en annen betegnelse for den meldeplikten som er regulert i påtaleinstruksen. Det fremgår av utkast til § 10-5 om underretning til kriminalomsorgens organer om forhold knyttet til personer som er underlagt kriminalomsorgen og som gjennomfører straff som nevnt i straffegjennomføringsloven § 10, at politiet straks skal underrette kriminalomsorgen om forhold politiet har fått kjennskap til. Dette omfatter iverksatt etterforskning mot personen, at en person som er

under straffegjennomføring har brutt vilkårene for gjennomføringen og oversikt over straffbare forhold en person tidligere er dømt for i utlandet i forbindelse med overføring til varetekt eller straffegjennomføring.

4.6 INFOFLYT – gjeldende instruks og øvrige retningslinjer

Sikkerhet i fengsel reguleres i rundskriv og retningslinjer for kriminalomsorgen, som er tilgjengelige på «kriminalomsorgen.no». Når det gjelder kontakten med politiet om sikkerhetsvurderingene, herunder i INFOFLYT, siteres her de generelle retningslinjene til straffegjennomføringsloven, med forskrifter, fastsatt av KSF 16. mai 2002 pkt. 1.8 på side 10: *«Kriminalomsorgen må vurdere om det er hensiktsmessig å ta kontakt med politiet i forbindelse med den sikkerhetsmessige vurderingen. Videre må man sette seg nøye inn i straffesaksdokumentene og andre dokumenter av betydning for vurderingen. Det må også vurderes om det er behov for å be Kriminalomsorgens sentrale forvaltning om opplysninger fra Infoflyt-systemet (...)*».

Den formelle forankring for INFOFLYT finnes i to rundskriv, se vedlegg 1 og 2. Det ene er det felles rundskrivet for politiavdelingen og kriminalomsorgsavdelingen i Justisdepartementet - G-3/2005 - samarbeid om generell informasjonsutveksling mellom politiet/ påtalemyndigheten og kriminalomsorgen av 11. april 2005. Dette rundskrivet er utarbeidet i felleskap av politiavdelingen og kriminalomsorgsavdelingen i Justisdepartementet og bestemmer at *«(...) for utveksling av informasjon i særlig alvorlige saker og med særlig høy risiko, skal INFOFLYT-systemet benyttes. For behandling av disse sakene vises det til særskilte, interne saksbehandlingsinstruksjoner utarbeidet av (...) KSF, Riksadvokaten, Politidirektoratet (POD) og Politiets sikkerhetstjeneste (PST).*»

Det andre er det særskilte rundskrivet for INFOFLYT - KSF 2/2005 av 13. april 2005, forankret i ovennevnte rundskriv. Dette er utarbeidet av kriminalomsorgsavdelingen i Justisdepartementet. I det følgende beskrives den særskilte saksbehandlingsinstruksen for INFOFLYT som de autoriserte tjenestemennene i kriminalomsorgen må forholde seg til.

Det understrekes i instruksen at INFOFLYT-samarbeidet ikke skal tre istedenfor det eksisterende og nødvendige samarbeid mellom kriminalomsorgens lokale enheter og lokalt politi, men skal være en kvalitetssikring av informasjon om *«visse innsatte, dømte og personkretsen rundt disse, og av informasjon om visse sakskomplekser av en viss alvorlighetsgrad, i tillegg til å gi ny informasjon om disse*».

Informasjonsutvekslingen mellom politiet og kriminalomsorgen skal i INFOFLYT-sakene foregå og kvalitetssikres sentralt mellom KSF og Kripas, eventuelt mellom KSF og PST. KSF skal ha et sentralt register over hvem som omfattes av INFOFLYT og som inneholder relevante opplysninger om disse. Personer registrert i INFOFLYT-registeret er også særskilt markert med rødt flagg i det elektroniske fangesakssystemet KOMPIS. Dette er for å gi den enkelte fengselsansatte informasjon om at det eksisterer sensitiv informasjon knyttet til den innsatte. Her vil det også framgå dato for registreringen.

Informasjonen kan være viktig i forbindelse med behandling av den innsattes søknad om permisjoner, prøveløslatelse mv.

Det registreres ikke gradert informasjon om vedkommende i KOMPIS, kun manuelt i vedkommendes mappe, se nedenfor. Ordinær fangeinformasjon (hendelsesrapporter, fangejournaler m.) om vedkommende registreres imidlertid elektronisk i KOMPIS. INFOFLYT har bare forbindelse til det elektroniske fangsakssystemet KOMPIS ved det røde flagget. Ut over dette er det ingen forbindelse mellom KOMPIS og INFOFLYT. Se omtalen av KOMPIS, se punkt 4.8.

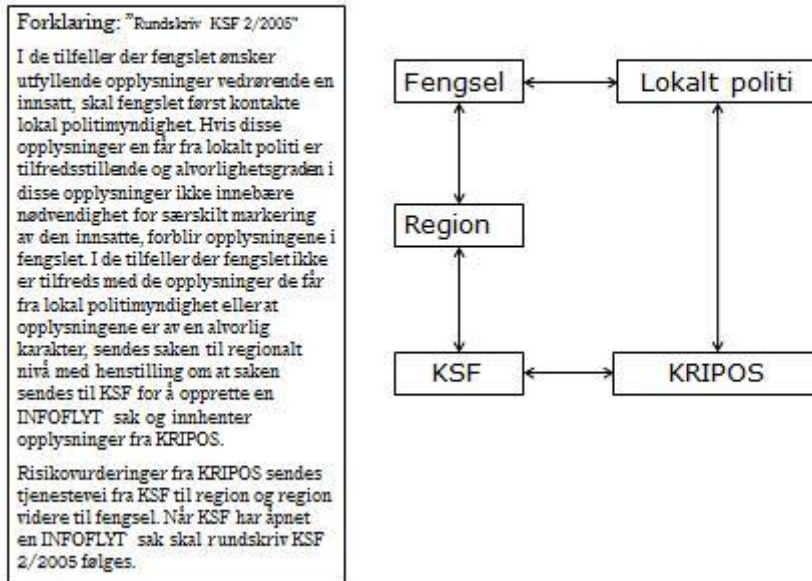
For lagring av papirmappene i systemet er det opprettet et eget arkiv i det hemmelige arkivet – H-arkivet - i Justisdepartementet. I tillegg til papirmappene har H-arkivet en elektronisk registrering av saken (innholdet i dokumentene registreres ikke) og registrerer fortløpende inn nye dokumenter som kommer til i saken. H-arkivet opererer med strenge krav til adgangskontroll og utlånsprosedyrer. Det gjelder et særskilt autorisasjonsregime og det benyttes graderte pc'er som ikke er tilknyttet datanettverket. Saksbehandleren har sitt eget skyggearkiv og disponerer en stasjonær pc for behandling av gradert informasjon.

Regionalt og lokalt nivå i kriminalomsorgen har også egne papirarkiv der mappene oppbevares etter beskyttelsesinstruksens og sikkerhetslovens regler for arkivering, utlån, adgangskontroll mv. Mappene skal etter kriminalomsorgens arkivregler lagres i 10 år før de tas ut av H-arkivet og oversendes Riksarkivet. Regionalt og lokalt nivå skal makulere sine papirmapper så snart den innsatte ikke lengre skal behandles etter INFOFLYT, dvs. tas ut av systemet ved at den innsatte «avflagges» i KOMPIS.

INFOFLYT er offentlig kjent og omtales i ulike offentlige dokumenter. Saksbehandlingsinstruksen for INFOFLYT, KSF 2/2005 er offentlig tilgjengelig, bl.a. på «Regjeringen.no».

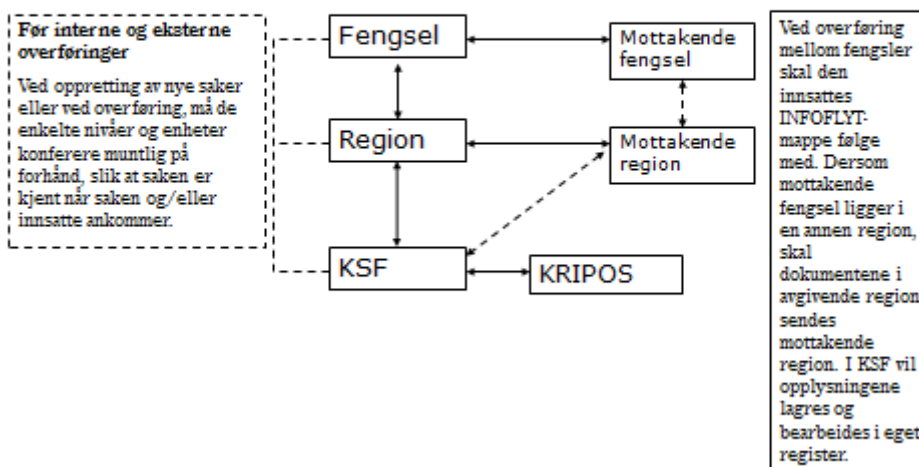
Nedenfor vises to illustrasjoner for INFOFLYT. Den første viser saksgangen og den andre viser saksbehandlingen i INFOFLYT:

Flytskjema INFOFLYT



Figur 1.1 Flytskjema INFOFLYT

Saksbehandling INFOFLYT



Figur 1.2 Saksbehandling INFOFLYT

Nærmere om bestemmelsene i INFOFLYT-instruksen

I innledningen til instruksen heter det:

«Riktige sikkerhetsmessige vurderinger i kriminalomsorgen er avhengige av et så godt informasjonsgrunnlag som mulig. Dette gjelder både de løpende sikkerhetsvurderinger på den enkelte enhet, men også ved nyinnsettelse og overføringer, samt i trusselsaker. Slik

informasjon har til tider vært av varierende kvalitet. Det er derfor nødvendig med en sentral kvalitetssikring av slik informasjon og et formalisert operativt system som kan behandle den. Pga. opplysningenes meget sensitive art, må systemet sikre minst mulig spredning av disse.»

For å sikre et operativt fungerende system, skal, i tillegg til det sentrale samarbeidet, alle samarbeidende enheter på samme nivå i politiet og kriminalomsorgen fortsatt utveksle informasjon om domfelte og personkretsen rundt disse for å forebygge kriminalitet og trygge samfunnet. Det sentrale samarbeidet skal tjene som kvalitetssikring av lokal/ regional informasjonsutveksling i alvorlige saker. Opplysningene skal brukes som grunnlag for tiltak *«mot de aktuelle personene.»*

Kriminalomsorgens beslutninger om å legge opplysninger inn i INFOFLYT, gi opplysninger til politiet eller å innhente ny informasjon fra politiet skal tas av KSF, jf. forvaltningsloven § 13 b første ledd nr.5. Beslutningen skal treffes på ledelsesnivå. Det er KSFs ekspedisjonssjef som er ansvarlig for beslutningen i egenskap av leder og som behandlingsansvarlig etter personopplysningsloven. Beslutningsmyndigheten er delegert til KSFs utviklingsseksjon ved avdelingsdirektør.

Det daglige arbeidet i KSF håndteres av en saksbehandler, benevnt som sambandsmann. Vedkommende har ukentlige arbeidsdager i KRIPOS. Sambandsmannens virksomhet er regulert i en egen instruks, utarbeidet av KSF. Instruksen gjelder både sambandsmannens ordinære samarbeid med politiet og kontakten med egne enheter i kriminalomsorgen utenfor INFOFLYT, og samarbeidet knyttet til innsatte i INFOFLYT. Sambandsinstruksen henviser derfor både til det generelle rundskrivet G-3/ 2005 og KSF 2/ 2005.

Alle henvendelser om å gi ut informasjon til- eller innhente informasjon fra politiet skal skje tjenestevei, jf. rundskrivet pkt. 5. Interne henvendelser fra lokalt nivå skal gå via regionen og til KSF og motsatt. Utvekslingen av informasjon som skal inn i INFOFLYT skjer mellom KSF og KRIPOS/PST.

Alle forespørsler skal være skriftlige. Det praktiseres en stor grad av fleksibilitet dersom det haster. Overlevering av opplysninger kan derfor skje muntlig og direkte til samarbeidende lokale enhet dersom det er opplysninger av høy alvorlighetsgrad eller det haster. Så snart det er tid til det skal kopi eller skriftlig referat av samtalene oversendes KSF og KRIPOS/PST.

Informasjon fra sentral enhet i kriminalomsorgen og politiet skal i følge instruksen gis i bearbeidet form. Dette gjelder likevel ikke dersom det dreier seg om opplysninger om sikkerhetsrisiko for innsatte.

I følge instruksen skal INFOFLYT-saker «som hovedregel» inneholde opplysninger som vil skade offentlige interesser eller enkeltpersoner om de ble kjent. De skal derfor som regel graderes FORTROLIG eller STRENGT FORTROLIG. Dokumentene skal

behandles etter beskyttelsesinstruksen. Dette omfatter sikker lagring og forsendelse og innebærer innlåsing i eget skap, atskilt fra de andre fangesakene. I enkelte saker gjelder sikkerhetslovens bestemmelser.

Hvem som kan behandle INFOFLYT-saker

I følge instruksen skal 3-4 personer på sentralt og regionalt nivå autoriseres til å arbeide med INFOFLYT mens 2-4 personer skal arbeide med sakene på lokalt nivå. I tillegg kommer administrativt personell, som forværelse og arkiv.

Når det kommer inn nye opplysninger i en allerede etablert sak – vanligvis ved brev til Justisdepartementet, skal brevet registreres i H-arkivet. KSFs sambandsmann kontaktes for å hente brevet. Vedkommende låner da hele mappen og saksbehandler den nye informasjonen. Han leverer deretter mappen tilbake og får tatt kopi av den siste innkommende- og utgående korrespondansen. Sambandsmannen besitter et skyggearkiv med de aktive sakene, som befinner seg i låst sikkerhetsskap i eget kontor.

Kriminalomsorgen og politiet graderer som oftest sine egne dokumenter. De er vanligvis gradert FORTROLIG eller STRENGT FORTROLIG. Enkelte saker er gradert etter sikkerhetsloven (KONFIDENSIELT eller BEGRENSET).

Kriminalomsorgen foretar også en selvstendig trussel- og kvalitetsvurdering av opplysningene som mottas.

I følge rundskrivet, er det «naturlig» at regional og lokalt nivå har egne INFOFLYT-arkiv. Dersom disse nivåene utformer eller mottar nye dokumenter i saken, skal KSF og KRIPOS ha kopi. Ved oppretting av nye saker eller ved overføring av saker/innsatte fra en enhet til en annen, skal det også konfereres muntlig mellom de berørte enhetene slik at de er forberedt.

Hvilke personer som kan registreres i INFOFLYT

Bare personer som er innsatte kan være registrert, i betydningen gjenstand for saksbehandling i INFOFLYT. Vedkommende må enten være innsatt i varetekt eller gjennomføre straff. Det vil også være nedtegnet opplysninger om personer som er knyttet til en registrert innsatt (slekt, vennskap, kriminelle kontakter mv.) i mappen. Personer som fortsatt gjennomfører straff skal tas ut av systemet hvis de ikke kvalifiserer for å være der.

Målgruppen er innsatte med tilknytning til forhold som nevnt i instruksens punkt 3, dvs. at de utgjør en særlig risiko for orden og sikkerhet i fengsel, fare for tjenestemennene der og for samfunnet for øvrig. Vilkårene om ro og sikkerhet i fengsel og fare for tjenestemennene synes å være alternative vilkår. Det er likevel alltid et vilkår for å bli registrert i INFOFLYT at vedkommende er en fare for samfunnet (men trenger da ikke nødvendigvis å utgjøre en risiko for ro og sikkerhet i fengslet), *eller* er en person som har opptrådt som informant eller vitne i sak knyttet til samfunnsfarlig

virksomhet og derfor trenger beskyttelse, selv om de selv ikke er ansett som farlige, se nedenfor.

Personene i målgruppen er etter instruks knyttet til:

- Særlig rømningsfare
- Fare for anslag utenfra for bistand til rømning
- Gisseltaking
- Fare for ny alvorlig kriminalitet
- Spesielle beskyttelsesbehov, for eksempel knyttet til vitnebeskyttelse, og som kan tilhøre organiserte kriminelle nettverk, eller terrorister, eller politiske, eller religiøse nettverk.

I vurderingen av om vedkommende skal flagges, kan det i følge instruks pkt. 3 tas hensyn til type lovbrudd, domslengde og tidligere adferd i fengslet, for eksempel nye alvorlige straffbare forhold.

Typer av opplysninger som inngår

I følge rundskrivet skal det dreie seg om «*relevante opplysninger.*» (punkt 2). Det ligger som forutsetning i pkt.1 at opplysningene er av «*meget sensitiv(e) art.*». Det sies ikke mer konkret om hvilke opplysninger dette kan være, men det ligger til KSFs skjønn å vurdere hvilke opplysninger dette er gjennom kvalitetssikring. Etter punkt 1 skal opplysningene undergis en sentral kvalitetssikring som grunnlag for sikkerhetsvurderinger. Dette er selve begrunnelsen for INFOFLYT.

Politiet benytter trusselvurderingssystemet, det såkalte 4x4 i sine trusselvurderinger. 4x4 er et system der man vurderer kvaliteten på opplysningene slik:

<u>Kildekode</u>	<u>Opplysningskode</u>
A- Pålitelig	1 Sann
B- Vanligvis pålitelig	2 Opplysningene er kjent av kilden personlig
C- Vanligvis ikke pålitelig	3 Opplysningene er ikke kjent av kilden personlig men styrkes av andre opplysninger
X- Pålitelighet kan ikke vurderes	4 Informasjonsverdien kan ikke vurderes

Trusselnivåene inndeles så i 4 kategorier: Lavt, moderat, høyt og ekstremt. Er for eksempel kilden vanligvis pålitelig – B - og opplysningen er kjent av kilden personlig – 2 - blir trusselen B2, noe som gir et høyt trusselnivå.

Kriminalomsorgen bruker ikke dette systemet for å vurdere opplysningenes kvalitet. Utvalget mener at dagens rutiner for kvalitetssikring bør forbedres, se omtalen i kapittel 8 og forslaget til forskrift § 3 siste ledd.

Hva opplysningene skal brukes til

Etter INFOFLYT-instruksen punkt 1 skal den sensitive informasjonen danne grunnlag for «*løpende sikkerhetsvurderinger*». Tiltakene kan gå ut på sikkerhet i fengsel og forebygging av kriminalitet. Dette kan omfatte både generelle sikkerhetstiltak og tiltak rettet mot en enkelt innsatt. Eksempler på dette kan være overføring av innsatte til annet fengsel av hensyn til å unngå en uheldig fangesammensetning, overføring til fengsel med høyere sikkerhetsnivå for å unngå rømning, og bruk av opplysningene som ledd i behandling av permisjons- og prøveløslatelsessøknader.

Innsynsretten

Etter INFOFLYT-instruksens punkt 8 er det «*(...) naturlig å ha som utgangspunkt at det ikke må gis innsyn i disse spesielle opplysningene.*» Dette har forut for 2009 i praksis blitt tolket slik at det overhode ikke er innsyn i opplysninger om dem selv i INFOFLYT-mappen. Et slikt utgangspunkt har ikke vært ansett å være i samsvar med personopplysningslovens hovedregel om innsynsrett, med de unntak som følger av lovens § 23. Etter sivilombudsmannens uttalelse er det i nyere praksis gitt innsyn i INFOFLYT-opplysninger som ikke vurderes som beskyttelsesverdige.

Kriminalomsorgen behandler innsynsbegjæringer med klagerett etter forvaltningsloven § 21. I KSFs svar i en klagesak fra 2009 heter det: «*(...) informasjon lagret i INFOFLYT vil kunne ha innvirkning på progresjonen i soningen, og kan slik sett ha store konsekvenser for innsatte. Nektelse av innsyn vil avskjære innsattes muligheter for kontradiksjon. Anstalten har på denne bakgrunn vurdert om det av hensyn til innsatte likevel burde gis innsyn i opplysningene. Anstalten har imidlertid kommet til at innsyn ikke kan gis så lenge kriminalomsorgen har taushetsplikt om de sladdede opplysningene (...)*».

Øvrige rundskriv og retningslinjer om innsyn med relevans for INFOFLYT

Man gjør altså i dag rede for bakgrunn for at det ikke kan gis fullt innsyn i den utstrekning dette kan gjøres uten å røpe nettopp det som sladdingen skal skjule. Et eksempel nevnes i retningslinjene til straffegjennomføringsloven punkt 4.2. Dette er dersom grunnlaget for vedtaket er opplysninger gitt av en medinnsatt eller informasjon gitt av politiet som er unntatt fra partsøffentlighet.

KSF har utarbeidet en egen veileder (udatert) om partsinnsyn som regulerer forholdet til forvaltningsloven. I kommentaren til § 7 bokstav c om partsinnsyn heter det blant annet: «*Opplysninger som det anses utilrådelig at domfelte (...) gis innsyn i, skal på anmodning gjøres kjent for en representant for parten, for eksempel fullmektig eller verge.*

Opplysningene skal ikke gjøres kjent for representanten når særlige grunner taler imot det, for eksempel sikkerhetsmessige eller etterforskningsmessige hensyn. Det skal settes som vilkår for innsyn at opplysningene ikke meddeles videre til parten (...) Representanten har samme ansvar for taushetsplikt som fastsatt for offentlig tjenestemann i straffeloven § 121(...)».

Administrative rutiner som ikke er nedfelt i instruksen

Det er visse administrative rutiner som gjelder for sambandsmann/KSF, personell ved KRIPOS, ledelsen i KSF, regionale og lokale autoriserte personer og personell i Justisdepartementets hemmelige arkiv.

Tidspunkt for registrering nedtegnes. Dokumentene i saken oppbevares i Justisdepartementets hemmelige arkiv – H-arkivet, som er et arkiv med høy sikkerhet etter reglene i beskyttelsesinstruksen. Arkivet registrerer saken i sitt datasystem samt alle dokumentene i saken etter innkommet/ utgående dato. Det registreres bare dokumentdato og overskrift, og dermed ingenting av selve innholdet i dokumentene.

4.7 Behandling av gradert materiale

Sikkerhetsloven

Sikkerhetsloven (lov om forebyggende sikkerhetstjeneste av 2. mars 1998 nr.10) regulerer adgangen til opplysninger som kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter, eller andre vitale sikkerhetsinteresser.

Dokumenter graderes i stigende rekkefølge:

- Begrenset
- Konfidensielt
- Hemmelig
- Strengt hemmelig

NATO har egne graderinger.

Beskyttelsesinstruksen

Beskyttelsesinstruksen (kongelig resolusjon av 17. mars 1972 nr. 3352 som er hjemlet i Kongens instruksjonsmyndighet) gjelder bare for statsforvaltningen og gir autorisert personell et personlig ansvar for at informasjonen ikke kommer på avveie. Instruksen brukes på fortrolig materiale som trenger beskyttelse av andre grunner enn etter sikkerhetsloven. Instruksen regulerer informasjon som kan skade offentlige interesser, en bedrift, institusjon eller enkeltperson, om den ble gjort kjent for uvedkommende.

Det gjelder to grader i stigende rekkefølge:

- Fortrolig
- Strengt fortrolig

Når en part søker om innsyn i graderte opplysninger om seg selv, har graderende enhet, dvs. normalt enheten som har utstedt dokumentet, plikt til å vurdere om dokumentet helt eller delvis kan nedgraderes fordi kravet til beskyttelse er endret, jf.

beskyttelsesinstruksen § 5 nr. 4. Dokumentet kan bare nedgraderes av den etat som har foretatt graderingen.

Dette innebærer at dersom kriminalomsorgen får en begjæring fra en innsatte om innsyn i opplysninger om ham registrert i INFOFLYT, og dokumentet er utstedt og gradert av politiet etter beskyttelsesinstruksen, må politiet forelegges spørsmålet om mulig nedgradering før kriminalomsorgen treffer avgjørelse om innsyn jf. § 5 nr. 4 bokstav a).

Instruksen regulerer for øvrig en rekke krav til behandlingsmåter for graderte dokumenter. Dette gjelder spredning, journalisering, oppbevaring, forsendelse, tilintetgjørelse. Endelig krever instruksens § 12 at dokumenter som er graderte, så langt det passer skal behandles elektronisk i samsvar med sikkerhetslovens forskrift om informasjonssikkerhet.

4.8 Beskrivelse av det elektroniske fangesakssystemet KOMPIS

Innsatte som er registrerte i INFOFLYT, registreres også i KOMPIS som alle andre som gjennomfører straff. Derfor gis det nedenfor en kort omtale av systemet.

KOMPIS står for «Kriminalomsorgens produktivitetsfremmende informasjonssystem». Kriminalomsorgens sentrale datasystemer inneholder tre landsdekkende it-systemer. Dette er Kompis-Kia/reskontro, Booking og Kompis-Kif.

Kompis-Kia/Reskontro er kriminalomsorgens eldste system, fra 1992. Det gir støtte til en del arbeidsoppgaver i fengslene, men er ikke et saksbehandlingssystem. Systemet kan utveksle data med friomsorgen (Kompis KIF) for personer som overføres dit. Systemet leverer meldinger om innsettelse og løslatelse i fengslene.

Kompis-Kif er et styringsredskaps- og saksbehandlingssystem som gir støtte i arbeidsoppgaver i friomsorgen. Systemet kan i liten grad utveksle data med fengslene (Kompis-Kia). Systemet samhandler med et elektronisk arkiv. Systemet har ikke samhandling med andre systemer i justissektoren eller med andre offentlige etater som arbeider i kriminalomsorgen.

Bookingsystemet er det nyeste i kriminalomsorgen og støtter behandling av saker fra de kommer fra politi eller påtalemyndighet, til en person settes inn eller møter ved et fengsel eller friomsorgskontor. Systemet kan samhandle med fengslene og friomsorgskontorene (Kompis-Kia og Kompis-Kif). Systemet mottar kjennelser elektronisk fra domstolene.

I rundskriv G-111/2000 «Om journalføring og registrering i Kompis Kia» er det gitt retningslinjer for journalføringen. Det fremgår bl.a. i § 2 at det med journal menes alle nedtegnelser om en innsatt, herunder aktuelle opplysninger om den innsatte, varetekt, soning, dom, bot, forvaring og hendelser (også fremdrift og beslutninger, jf. § 5). I § 3 slås fast at det bare skal føres opplysninger i journalen som har en saklig og nødvendig betydning for fengselsoppholdet. I følge § 6 har den innsatte rett til innsyn i journalen. «Før innsyn innvilges skal det nøye overveies om journalen inneholder opplysninger som

skal være unntatt (...). Unntaksretten følger av forvaltningsloven §§ 18 og 19 samt (tidligere, red.anm.) fengselsloven § 1a femte ledd». Det fremgår videre av § 6 at opplysningene må være fullstendige og korrekte.

Som nevnt i punkt 4.6 skal personer som er registrert i INFOFLYT merkes i KOMPIS med rødt flagg slik at ansatte som behandler personopplysninger i KOMPIS vet at overordnet organ må kontaktes før det besluttes endringer i soningsforhold, innvilges permisjoner mv.

4.9 Beskrivelse av saksbehandlings- og arkivsystemet DocuLive

I det følgende beskrives kriminalomsorgens felles elektroniske sak - og arkivsystem, DocuLive. Bakgrunnen er at DocuLive eventuelt kan bli benyttet som system hvor det bygges inn en modul for et fremtidig elektronisk INFOFLYT. Dette forutsetter at systemet kan tilpasses slik at det teknisk tilfredsstillende kravene til sikker tilgangsstyring og sikker utveksling av opplysninger.

Kriminalomsorgen har i 2011 fullført implementeringen av DocuLive ved alle fengsler, friomsorgskontorer, regionadministrasjoner, kriminalomsorgens utdanningssenter - KRUS og kriminalomsorgens IT-tjeneste - KITT.

DocuLive skal sikre en enhetlig IKT-løsning og gode rutiner i hele kriminalomsorgen. Dette omfatter arkiv- og saksbehandlingsfunksjon og tilgang til ledelsesinformasjon.

Kriminalomsorgen har innført en hierarkisk modell for tilgangsstyring, som innebærer at en leder autoriserer sine tilsatte med de tilganger de skal ha. Dette er innført også i DocuLive-løsningen slik at dokumentene er tilgjengelige når saksbehandlerne trenger dem ut fra tjenstlige behov. For å gjøre de elektroniske saksmappene komplette og lette å finne igjen, er det utviklet en integrasjonsløsning mellom DocuLive og IT-fagsystemene i Kompis, se beskrivelsen av disse i punkt 4.8. Både Kompis-systemene og DocuLive har en sentral database.

Kort skissert er løsningen mot fagsystemene slik: Alle straffegjennomføringssakene i Booking starter ved at det kommer inn et dokument i posten. Når dokumenter ankommer, opprettes en sak i DocuLive. Den bookingansvarlige importerer saken fra DocuLive. Allerede registrerte opplysninger i DocuLive oppdateres av Booking slik at man unngår dobbeltregistrering.

Saken importeres deretter fra KOMPIS Booking til Kompis-KIF eller Kompis-KIA.

Fra Kompis-saken får brukerne tilgang til alle dokumenter i saken. Tilgangen til dokumentene styres fra DocuLive. Ved at det i brukerregisteret i Kompis legges inn initialene brukeren har i DocuLive, er det disse tilganger som også styrer tilgangene i «vis»-funksjonen i Kompis.

Når en domfelt overføres fra en enhet til en annen, sender Kompis melding til DocuLive om at saken skal flyttes til ny enhet. Det skjer automatisk endring av saksansvarlig til ny enhet i DocuLive og rettighetene til å se dokumenter flyttes til den nye enhetens «OVF»-gruppe, se nedenfor.

For å styre tilgang til saker og dokumenter i DocuLive benyttes tilgangsgrupper. Det er bare ansatte som skal ha tilgang og ut fra tjenstlige behov. Det er opprettet følgende grupper på hver enhet:

- ADM: Gruppe for alle dokumenter som skal være tilgjengelig for alle på den respektive enhet
- STRA: Gruppe for dokumenter som skal være tilgjengelig for kun de som arbeider med domfelte
- LEDE: Gruppe for ledelsen pr enhet for dokumenter kun for ledere
- PERS: Gruppe for skjerming av personalsaker
- KONT: Gruppe for skjerming av kontrakter som skal skjermes
- OVF: Gruppe for dokumenter som automatisk overføres fra en enhet til en annen når den domfelte overføres til annet fengsel
- EK: Gruppe for EK saker (elektronisk kontroll)

Det er i tillegg opprettet to standardgrupper i DocuLive:

- ALLE: Denne gruppen brukes for saker og dokumenter alle skal kunne se.
- INGEN: Gruppen har ingen medlemmer, unntatt arkivleder og systemforvalter for å sikre at dokumenter arkiveres og ikke forsvinner. Når denne gruppen brukes må saksbehandler legge inn konkrete personer som skal se dokumentet for å skjermes mot de øvrige i organisasjonen.

Alle landets ansatte i kriminalomsorgen med tilgang til DocuLive vil kunne se at en sak er opprettet. De kan da lese bl.a. navn, personnummer, hvor vedkommende skal sone mv. Årsaken er at en innsatt kan ha flere dommer som skal sones i én straffegjennomføring. Den som oppretter saken må se at det allerede eksisterer en sak, og registrerer så en ny anmodning om soning av dom i denne saken.

Det arbeides med å få til en løsning der bare tilsatte med tjenstlig behov kan lese navn og fødselsdato på dømte personer, da dette er sensitive opplysninger etter personopplysningsloven § 2 nr. 8 bokstav b.

Alle dokumenter i saken er imidlertid skjermet slik at bare de ansatte ved enheten der straffen skal sones, har tilgang. Det brukes også skjerming i forhold til offentlig journal på alle dokumenter ut fra innhold og der avsender/mottaker skal skjermes. For å kunne samhandle på tvers av enheter i kriminalomsorgen i for eksempel klagesaker, bruddsaker og andre henvendelser, er det likevel laget en modul med utvidet tilgang. Det er utviklet et elektronisk brev (EB) som sendes mellom enhetene.

5 Ordningene i Sverige og Danmark

Formålet med dette kapitlet er å beskrive hvordan våre to nærmeste naboland har organisert tilsvarende systemer. Erfaringene fra Sverige og Danmark kan tjene som grunnlag for utvalgets forslag.

5.1 Sverige

5.1.1 Generelt

Kriminalitetsutviklingen, særlig enkelte spektakulære rømninger i 2004, har ført til at Sverige har sett de samme behov som Norge når det gjelder å profesjonalisere analyse og bruk av etterretningsinformasjon, samt å styrke og formalisere samarbeidet mellom kriminalvården og politiet og de øvrige kriminalitetsbekjempende myndighetene.

Regjeringen besluttet i 2008 å utvikle samarbeidsformer mellom politi- og påtalemyndigheten, Skatteverket, Kustbevakningen, Tullverket, Kronofogdemyndigheten og Kriminalvården for å bekjempe grov organisert kriminalitet. Som ledd i dette ble det etablert 5 regionale etterretningssentre i tillegg til de 3 som var der fra før. Alle relevante myndigheter er representert, tilpasset behovene ved den enkelte region. Det legges vekt på at taushetsplikten ikke må være hinder for et effektivt samarbeide mellom kriminalvården og andre myndigheter, samtidig som den dømtes rettigheter ivaretas. For å oppnå dette har Rikspolisstyrelsen avgitt en særskilt lovutredning på oppdrag av Justitiedepartementet. Resultatet er i hovedsak at lovgivningen er blitt tilpasset slik at den legger til rette for informasjonsutveksling i felles etterretningsprosjekter.

Kriminalvården ønsket fastere rammer om samarbeidet og etablerte derfor et nasjonalt sikkerhetsregister over visse straffedømte, forvaltet av et nasjonalt etterretningssenter «NUC» i 2009. Senteret samarbeider nært med egne regionale enheter og med andre myndigheter, særlig politiet.

Kriminalvården har etter de nevnte rømningene i 2004 etablert organet Kriminalvårdens underrättelsetjänst - «Kv-KUT». Formålet med etterretningsvirksomheten er å forebygge rømninger fra lukkede anstalter, avsløre fortsatt kriminell virksomhet i fengsel, bekjempe narkotikainnførsel i anstalter og «häkter» (egne varetektsenheter) og bidra til å begrense trusler og trakassering mot innsatte og ansatte. Virksomheten fokuserer på den grove og organiserte kriminaliteten gjennom kartlegging av gjenger, nettverk og midlertidige fenomener i kriminalomsorgsmiljøet. For å kartlegge på en systematisk og sikker måte, har Kv-KUT et eget register (säkerhetsregistret) for spesielle innsatte eller domfelte som er underlagt kriminalvården.

5.1.2 Regelverket for Kv-KUT - Säkerhetsregistret

Fengselsforordning 2001:682 om behandling av personopplysninger i kriminalvården har fått nye bestemmelser om behandling av opplysninger om visse kriminelle personer og forbrytelser, i kraft 1. april 2011. Særlig relevante er §§ 39-44:

Etter § 39 skal det opprettes et sikkerhetsregister over personer som

- har vært eller er plassert på sikkerhetsavdeling,
- som innsatt gjort seg skyldig i trusler eller vold mot ansatte eller innsatte,
- som innsatt befattet seg med narkotika utover eget bruk,
- har rømt med eller uten bistand, eller forsøk på dette, eller
- som innsatt har deltatt i nettverk som bidrar til alvorlige ordensforstyrrelser eller kriminell virksomhet

Etter § 40 kan registeret også inneholde opplysninger der det er nærliggende grunn til å anta at personer i fengsel, *sammen med andre*, kan komme til å

- begå alvorlige forbrytelser,
- hetse folkegruppe mv.
- begå alvorlige ordensbrudd i anstalten
- delta i nettverk som bidrar til alvorlige ordensbrudd eller kriminalitet, eller
- forberede rømning eller bistand til dette

I tillegg skal det etter den nye fengselsloven kapittel 7 § 11 registreres innsatte som - etter en regjeringsbeslutning - mistenkes å bidra til terror eller for øvrig kan være en fare for rikets sikkerhet.

Etter forordningens § 43 skal kun kriminalvårdens autoriserte ansatte ha tilgang til systemet, etter Generaldirektørens (leder for kriminalvården) beslutning.

Etter § 44 skal autoriserte ansatte i Rikspolisstyrelsen ha direkte tilgang til opplysninger om hvorvidt en person er registrert i sikkerhetsregistret. Disse kan i sin tur utlevere en slik opplysning til personer i politi- og påtalemyndighet i forbindelse med en pågående sak når opplysningen har særlig betydning for etterforskningen. Kriminalvården kan i medhold av samme bestemmelse utlevere opplysninger om den registrerte til politi- og påtalemyndigheten, som disse trenger til etterforskningsformål.

I praksis er opplysningene som utleveres til politiet et sammendrag av opplysninger som kriminalvården mener er relevant i forhold til politiets behov. Det utleveres altså ikke rådata til politiet (fullstendige hendelsesrapporter el.), slik det gjøres i Norge. Dette innebærer at det ikke kan gjennomføres noen automatisert informasjonsutlevering fra sikkerhetsregistret til Rikspolisstyrelsen eller annen politimyndighet. Det er bare spesifikke spørsmål som kan besvares og da først ved at «Kriminalvårdens underrättelsetjänst» vurderer om spørsmålet kan besvares uten bryte med lovbestemt taushetsplikt (jf. Offentlighets- og sekretesslagen 2009:400).

5.1.3 Kriminalvårdens etterretningsorganisering Kv-KUT

Kv-KUT er organisert i en nettverksstruktur og med en sentral ledelse. Kriminalvårdens sentrale etterretningssenters hovedkvarter - KUT-HK- er plassert i kriminalvårdens hovedkonter og i den sentrale sikkerhetsgruppen. KUT-HK består av 10 ansatte som er delt inn i IT-personell og operative etterretningseksperter samt analytikere. De koordinerer og styrer informasjonsflyten og registrering av informasjon i sikkerhetsregisteret med sine underliggende organer. I tillegg samarbeider KUT-HK med politiet og de øvrige samarbeidsorganene som nevnt over, på sentralt nivå.

På 16 utpekte anstalter og haker i kriminalvården er det plassert etterretningsspersonell som består av til sammen 35 etterretningsoperatører. De 35 pluss de 10 i KUT-HK har tilgang til sikkerhetsregisteret, se nedenfor. Utover de 35 lokale operatørene er det på hver lokale enhet plassert sambandsmenn (ca. 150), som melder informasjon inn til systemet. Disse har ikke tilgang til Sikkerhetsregistret men kan be om informasjon fra KUT-HK for å sikre orden og sikkerhet ved sin anstalt.

5.1.4 Sikkerhetsregisteret

«Sikkerhetsregisteret» er kriminalvårdens rapporterings- og etterretningssystem. Det har ingen lokale underregistre slik at det bare finnes ett sentralt slikt register. Alt som legges inn der er fullt sporbart, herunder hvem som har lest eller lagt inn opplysninger. I hovedsak er opplysningene som registreres etterretningsinformasjon, som dermed er gradert materiale. Noen opplysninger kan likevel være ugradert. Opplysningenes pålitelighet rangeres etter 4x4 metoden etter kriminalvårdens sannsynlighetsskala (en internasjonal standard som også det norske politiet bruker, se omtalen i punkt 4.6).

Ingen andre enn kriminalvårdens egne autoriserte ansatte (40 personer til sammen på sentralt og lokalt nivå) har tilgang til systemet. Rikspolisstyrelsen har imidlertid til en hver tid oversikt over hvem som er registrert.

KUT-HK innkaller alle regionale sentre til faste møter for å oppdatere og kvalitetssikre opplysninger, samt slette utdaterte og ukorrekte opplysninger i Sikkerhetsregistret.

De innsatte som registreres i Sikkerhetsregistret er utelukkende personer som tilhører den grove og organiserte kriminaliteten. Videre omfattes innsatte som er plassert på sikkerhetsenheter. For det tredje er målgruppen personer (klienter) som er utsatt for trusler. Formålet med å registrere dem er å beskytte dem under hele straffegjennomføringen eller varetektsoppholdet, mot personer som truer dem eller ønsker å utøve vold mot den beskyttede klienten.

Av de registrerte innsatte med særlig prioritet er det ca. 30 personer som er plassert i sikkerhetsenheter, 30 i sikkerhetsavdelinger og 12 innsatte informanter i egne enheter for personer med særlig beskyttelsesbehov («Witness Protection Units»).

5.1.5 Opplysningenes art, kildene og utlevering

Det er i hovedsak etterretningsinformasjon som registreres. Ofte stammer opplysningene fra ulike typer av menneskelige kilder. Det legges derfor stor vekt på å vurdere opplysningenes og kildenes troverdighet, ikke minst fordi det kan ligge hevnmotiv bak. Alle opplysningene skrives ned og vurderes etter 4X4 metoden.

Det gis ikke ut rådata. Det utleveres bare opplysninger som politiet (og øvrige samarbeidende organer som nevnt over) har behov for. Politiet får derfor bare utlevert opplysninger for spanings- og etterforskningsformål og bare i bearbeidet versjon/sammendrag. Alle enheter skal rapportere til KUT-HK når det er aktuelt å gi permisjon eller løslate en som er registrert i Säkerhetsregistret. Politiet får – slik som i Norge – full orientering om hvor registrerte personer soner, når de får permisjon eller løslates.

5.1.6 Innsyn og informasjon til de registrerte

De registrerte får ikke innsyn i opplysninger om seg selv eller beskjed om at de er registrerte. Dersom de spør om de er registrerte får de ikke vite om de er i registeret eller ikke. Bakgrunnen for dette er å unngå at det kriminelle miljøet som står for grov og organisert kriminalitet skal kunne foreta kartlegging samt å få mulighet til å avsløre mål og metoder i arbeidet. Klienten har lovfestet adgang til å påklage kriminalvårdens beslutning. Klagen behandles i forvaltningsdomstolen og i enkelte tilfeller i regjeringsretten.

Det er ingen automatisk avregistrering av personer i Säkerhetsregistret. Etter § 45 i nevnte fengselsforordning 2001:682, skal opplysningene slettes senest 5 år etter løslatelse. Slettingen gjennomføres av systemeier og informasjonen arkiveres etter gjeldende lov.

5.2 Danmark

5.2.1 Generelt

Tidlig i 1980-årene vokste det fram MC-miljøer som utførte organisert kriminell virksomhet. Det startet med at Hells Angels etablerte seg i 1980. På kort tid utraderte de den konkurrerende klubben Bullshit, og drev etter det »vanlig business», dvs. kriminalitet. Bandidos etablerte seg i Danmark i perioden 1994-1997, og det var starten på det man omtalte som «Den store Nordiske rockerkrigen», hvor de ulike grupperingene forsvarte sine interesser med vold.

Miljøene ble stadig mer brutale og det ble hyppig begått hevndrap i rivaliseringene mellom «Rocker-bandene». Politimyndighetene i Danmark utviklet derfor en nasjonal strategi med ulike innsatsområder:

- En operativ stab på rockerbande-kriminalitet
- Tett samarbeid mellom politidistriktene, kriminalforsorgen, skattevesenet, velferdsmyndighetene oa.
- Intensiv etterretningsvirksomhet og nasjonal og internasjonal etterforskning

- Exit-program (hjelp for bandemedlemmer til å komme seg ut av klubbmedlemskapet)
- Det ble i 2010 etablert en innsatsstyrke TFØ – Task Force Øst – med 70 personer fra alle politidistrikt og det nasjonale etterretningssenteret NEC for å få arrestert de farligste kriminelle

For å bidra til dette arbeidet har den danske kriminalforsorgen etablert et etterretningssenter som på en profesjonell måte skal arbeide med informasjonsinnhenting og analyse av innsatte medlemmer av organiserte kriminelle miljøer gjennom et nært samarbeid internt og med politiet, kalt «Kriminalforsorgens Etterretningscenter» (KE). Enheten fungerer som sentral for hele Danmark og hører til Kriminalforsorgsdirektoratet. Det er 6 ansatte som arbeider i etterretningen og bare disse er autorisert for tilgang til etterretningssystemet. Én av de 6 er jurist, men senteret benytter i stor grad også andre jurister ved behov for rettslige vurderinger og vedtak. Sikkerhetsenheten arbeider ikke bare med etterretningsvirksomhet. Den har i tillegg mange oppgaver knyttet til sikkerhet generelt og har derfor ikke den samme skarpe inndelingen som i Sverige.

Alle åpne og lukkede anstalter i Danmark har en sikkerhetssjef som er ansvarlig for å rapportere til KE.

KE arbeider med å innhente og kvalitetssikre sikkerhetsmessig viktige opplysninger om innsatte, i samarbeid med underliggende enheter og med politiet. KE utleverer også mye informasjon til politiet. Målet er, som i Norge, å hindre alvorlig kriminalitet, hindre organisert kriminalitet, forhindre rømninger og beskytte kilder. Opplysningene registreres på person eller på episoder.

KE anser at samarbeidet med politiet er godt og konstruktivt. Samarbeidet er basert på særlige områder eller det oppstår fra sak til sak. KE har ingen sambandsmann som i Norge men baserer samarbeidet på formelle møter mellom generaldirektøren og rikspolisjefen. I tillegg avholdes det regelmessige møter mellom politiet og kriminalforsorgen om «rocker-/bandeområdet» og terror/radikalisering.

KE driver ikke med aktiv etterforskning. Dette er forbudt etter den danske rettspleieloven.

5.2.2 Kriminalforsorgens Etterretningssystem (KES)

KE har i 2011 tatt i bruk et databaseverktøy – «Kriminalforsorgens Etterretningssystem» (KES). Datatilsynet i Danmark har gitt konsesjon for bruk. Systemet utvikles stadig for å gjøre søk i databasen og arbeidsprosessene mer effektive. Innhenting og kvalitetssikring av sikkerhetsopplysninger vil dermed gå raskere. Når KES er fullt utbygd forventes at det vil omfatte 1000 innsatte. KES kostet 1,5 mill. DKK å anskaffe.

Et viktig verktøy i databasen er en såkalt «snabel» som gjør det mulig med automatiserte søk i fangesaksregisteret for å finne soningsstedene til personer i personkretsen (venn eller fiende) rundt den aktuelle innsatte. Dette sparer mye tid og arbeid. Målet er å finne et sikkerhetsmessig egnet soningssted for den innsatte. Systemet har også den fordel når det hentes ut opplysninger fra fangesaksregisteret at man, via Etterretningssystemet, kan trekke ut rapporter med opplysninger fra fangesaksregisteret og dermed kombinere opplysninger fra begge systemer.

KES kan kommunisere med enkelte øvrige systemer. Bl.a. kan man ved dette holde oversikt over den innsattes økonomi og pengetransaksjoner. KES vil på sikt kunne kommunisere med kriminalforsorgens øvrige systemer.

Systemet har full sporbarhet, både over hvilke saksbehandlere som har logget seg inn og hvorfor. Det registreres uttrekk av opplysninger fra KES ved utskrift eller overføring til minnepinne. De 6 autoriserte medarbeiderne har fjernaksess med sikret innlogging.

5.2.3 Målgruppe og type kriminalitet

I dag er det ca. 600 personer totalt som er registrert, hvorav om lag 320 er innsatte og 280 er løslatte. Målgruppen er i hovedsak organiserte kriminelle grupper, i Danmark kalt «Rocker og bande-miljø» og terror/radikaliseringstiljøer. Også andre personer enn innsatte kan registreres. Det kan f.eks. være besøkende til den innsatte som mistenkes å ha tilknytning til slike grupper. Registrering i KES avhenger av adferd, relasjoner, særlige episoder ol. I tillegg til personer registrert på grunn av relasjoner til rocker/ bandemiljøet er det ca. 50 personer som er registrert på grunn av farlighet, rømningsfare, radikalisering, informantbeskyttelse mv.

For de aller fleste er det dermed ikke kriminalitetens art som er avgjørende for om en innsatt blir registrert. Type kriminalitet for å bli registrert i KES er kun relevant når den innsatte er siktet eller dømt for terror eller krigsforbrytelser, og registreres på bakgrunn av deres kriminalitet.

5.2.4 Kvalitetssikring

Sikkerhetskonsulentene i kriminalomsorgen har fengselsfaglig- og lederbakgrunn, eller juridisk utdannelse. De er dessuten sertifisert i risk management og har kurs hos PET (Politets etterretningstjeneste) i 4x4 «valideringssystem.»

Både kriminalomsorgen og politiet vurderer verdien av opplysningene ved bruk av 4x4 trusselvurderingsmetode. Opplysningene er graderte og samlet i et eget register.

Det er ingen formell utveksling av informasjon. For å få verifisert opplysninger om eksempelvis en innsatts forbindelser til et rocker/bandemiljø, rettes det henvendelser til/ fra politiet elektronisk og politiet svarer også elektronisk.

Informasjonsutvekslingen mellom politiet og kriminalomsorgen skjer i et «felles virtuelt rom» og i sikret nettverk.

5.2.5 Hvordan personer avregistreres

Etterretningssystemet samkjøres med opplysninger fra fangesakssystemet (Klientsystemet) slik at man ser om han er innsatt og dermed «aktiv». Vedkommende tas ikke ut av registeret ved løslatelse. Men dersom det ikke er registrert nye opplysninger om vedkommende over en lengre periode, fjernes han fra systemet etter en viss tid og senest 3 år etter siste registrerte opplysning. Opplysningene slettes fra systemet, men kan gjenskapes i tilfelle de blir relevante i en senere klagesak. Dette forutsetter assistanse fra det firmaet som har laget systemet.

5.2.6 Taushetsplikt, informasjonsplikt og innsyn

At systemet finnes er ikke hemmelig. I denne informasjonen inngår også at adgangen til systemet er begrenset, men likevel slik at relevante opplysninger kan utleveres til anstaltene i den grad det er forsvarlig. Graderingen er utførlig slik at det i hvert tilfelle vurderes i hvilket omfang og i hvilken form de kan gis videre.

De innsatte informeres ikke om at de er registrerte i etterretningssystemet. De gis heller ikke innsyn i opplysningene om dem selv. I en konkret sak gis «Ombudsmanden» opplysningene med pålegg om taushetsplikt. Dersom en innsatt for eksempel er registrert som medlem av en motorsysselgjeng, vil det bare framgå at registreringen beror på en samlet vurdering og ikke hvor opplysningene kommer fra. Dersom den innsatte klager over å være registrert, og får medhold, vil ikke vedtaket vise hvorvidt registreringen finnes. Det vil bare gå fram av vedtaket at kriminalomsorgen ikke lengre anser vedkommende som del av en gruppering.

6 Nærmere om regelverk knyttet til den registrertes rettigheter

6.1 Innledning

Utvalget har i kapittel 4 gjort rede for ulike lover og annet regelverk som gjelder for kriminalomsorgens behandling av opplysninger. I dette punkt vil man konsentrere seg om forhold som er av betydning for den registrertes personvern. Siden utvalget foreslår en utstrakt anvendelse av politiregisterloven for behandlingen av opplysninger i INFOFLYT, har man valgt å gi en sammenlignende fremstilling av de aktuelle bestemmelsene i henholdsvis personopplysningsloven og politiregisterloven. På denne måten illustreres likheter og forskjeller, samtidig som det begrunnes hvorfor man har valgt å anvende politiregisterlovens regler.

6.2 Informasjonsplikt

Informasjonsplikt er et grunnleggende prinsipp innenfor den alminnelige personvernlovgivningen. Den skal sikre at den registrerte får kunnskap om behandlingen av opplysninger om ham/henne. Informasjonsplikten kan både knytte seg til behandlingen som sådan og til opplysninger knyttet til en konkret person. Når informasjonsplikten knyttes til den enkelte, innebærer denne at den enkelte må informeres om at det behandles opplysninger om vedkommende, herunder hvem disse opplysningene eventuelt ble utlevert til.

Utgangspunktet etter personopplysningsloven §§ 19 og 20, er at organet av eget tiltak skal informere den registrerte om behandlingen. Denne hovedregelen gjelder også for kriminalomsorgen.

Personopplysningsloven 23 annet ledd a og b gjør unntak fra informasjonsplikten av hensyn til rikets sikkerhet eller når hemmelighold er påkrevd for å forebygge og avdekke straffbare handlinger.

Å gi den innsatte kunnskap om at han er blitt registrert i INFOFLYT kan bety fare for andre personer eller interesser som nevnt i straffegjennomføringsloven § 7 første ledd bokstav c, og unntakene i personopplysningsloven § 23 annet ledd vil derved normalt stenge for at den innsatte informeres om behandlingen av opplysninger i INFOFLYT. Siden informasjonsplikt likevel er hovedregelen, må Kriminalomsorgen i hvert enkelt tilfelle vurdere om unntaksbestemmelsene kommer til anvendelse.

I politiregisterloven er informasjonsplikt regulert i § 48, og den skiller seg i betydelig grad fra informasjonsplikten i personopplysningsloven. For det første gjelder informasjonsplikten bare dersom politiet utleverer opplysninger i mottakerens interesse. Det innebærer at informasjonsplikten ikke gjelder dersom politiet utleverer opplysninger i egen interesse, det vil si til politimessige formål. Videre er informasjonsplikten ytterligere begrenset ved at det i § 48 annet ledd er oppstilt ulike

unntaksgrunner, herunder hensyn til kriminalitetsbekjempelse, vern av andre personer eller hensyn mottakerorganets kontrollopgaver, jfr. § 48, 2. ledd nr. 2.

Overført til kriminalomsorgen vil det innebære at informasjonsplikten ikke gjelder dersom kriminalomsorgen utleverer opplysninger til andre organer i sin egen interesse, noe som normalt vil være tilfelle. Dersom kriminalomsorgen utleverer opplysninger til politiet i politiets interesse, vil unntaksbestemmelsene i § 48 annet ledd nr. 2 komme til anvendelse.

6.3 Innsyn

6.3.1 Noen innledende merknader

Utvalget finner innledningsvis grunn til å påpeke at begrepet «innsyn» har ulikt innhold i de lovene som gjør seg gjeldende i forbindelse med innsyn i INFOFLYT. Innenfor personvernlovgivningen, herunder personopplysnings- og politiregisterloven, innebærer rett til innsyn utelukkende at vedkommende kan få innsyn i opplysninger om seg selv. Dette i motsetning til såkalt partsinnsyn, slik som man finner det i forvaltningsloven, der vedkommende har rett til å gjøre seg kjent med sakens dokumenter. Partsinnsyn er således ikke begrenset til opplysninger om en konkret person, men omfatter i utgangspunktet alle opplysninger som ligger i saken.

For opplysningene i INFOFLYT vil det kunne være aktuelt at den registrerte begjærer både innsyn etter personvernlovgivningen og innsyn i sakens dokumenter. I punkt 6.3.2 gis det derfor en fremstilling av gjeldende rett hva gjelder partsinnsyn og i punkt 6.3.3 en fremstilling av gjeldende rett om innsyn etter personvernlovgivningen.

6.3.2 Partsinnsyn

Hovedregelen om partenes rett til å gjøre seg kjent med sakens dokumenter går fram av forvaltningsloven § 18 med de unntak som framgår av § 18 a-d. Forvaltningsloven § 19 gjør unntak fra visse typer opplysninger, bl.a. norske sikkerhetsinteresser. Forvaltningslovens regler gjelder med unntak av de særlige bestemmelsene i straffegjennomføringsloven.

Etter straffegjennomføringsloven § 7 første ledd bokstav c kan innsatte nektes innsyn i dokument «(...) som det av hensyn til en annen person er utilrådelig at vedkommende får kunnskap til. Parten har heller ikke krav på å gjøre seg kjent med opplysninger i et dokument dersom innsyn er utilrådelig på grunn av sikkerhetsmessige hensyn, eller av hensyn til etterforskning av straffbare handlinger.» Etter § 7 første ledd bokstav d kan begrunnelse av vedtak nektes av samme årsak. Det vises for øvrig til omtalen av dette i straffegjennomføringsloven i punkt 4.4.

6.3.3 Innsyn i henhold til personvernlovgivningen

Retten til innsyn er i personopplysningsloven regulert i § 18. I følge denne bestemmelsen kan alle få innsyn i informasjon som generelt beskriver hva slags behandling av personopplysninger som foretas, se lovens § 18 første ledd bokstavene a-

f. I tillegg har den registrerte rett til innsyn i hvilke opplysninger som behandles om vedkommende (§ 18 annet og tredje ledd). Unntak gjelder for opplysninger som ikke får noen direkte betydning for den enkelte og behandlingen utelukkende skjer for vitenskapelige, historiske eller statistiske formål. Som nevnt over i punkt 4.3 har § 23 unntak fra innsynsretten dersom det er nødvendig av hensyn til forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger, eller opplysningene er taushetsbelagt.

I politiregisterloven er innsynsretten regulert i § 49. Hovedregelen er også der at den registrerte har rett til innsyn i opplysninger om seg selv. I bestemmelsens fjerde ledd finner man unntakene fra innsynsretten. Disse er delvis sammenfallende med unntaksreglene i personopplysningsloven § 23, men en vesentlig forskjell finner man i politiregisterloven § 49 fjerde ledd nr. 3, hvoretter også hensynet til gjennomføring av strafferettslige reaksjoner kan begrunne unntak fra innsyn. Siden det nettopp er dette unntaket som ofte må antas å være aktuell i kriminalomsorgen, vil politiregisterloven i større grad ivareta etatens behov enn personopplysningsloven.

6.3.4 Retting, sperring og sletting av personopplysninger

I personopplysningsloven er retting, sperring og sletting av personopplysninger regulert i §§ 27 og 28. Begrepet «sperring» er ikke definert i personopplysningsloven § 2, og det er heller ikke andre steder i loven eller i personopplysningsforskriften definert hva sperring innebærer eller hvordan sperrede opplysninger skal viderebehandles.

Sletting av personopplysninger som ikke lenger er nødvendige for formålet er i § 28 uttalt som et forbud mot å lagre unødvendige personopplysninger, jf. § 28 første ledd første punktum. I følge annet ledd skal slike opplysninger slettes med mindre de skal oppbevares i henhold til arkivlovgivningen eller annen lovgivning.

Sletting og sperring av mangelfulle personopplysninger er regulert i § 27, som i utgangspunktet regulerer retting av mangelfulle personopplysninger. I følge bestemmelsens første ledd første punktum skal den behandlingsansvarlige av eget tiltak eller etter begjæring fra den registrerte rette mangelfulle opplysninger. Begrepet «mangelfull» er eksemplifisert i første punktum som uriktige, ufullstendige eller opplysninger som det ikke er adgang til å behandle. I annet ledd gis det anvisning på at den behandlingsansvarlige om mulig skal sørge for at feilen ikke skal få betydning for den registrerte, som eksempel ved å varsle mottakeren av utleverte opplysninger.

I annet ledd gis det anvisning på hvordan mangelfulle opplysninger skal rettes. Bestemmelsen regulerer dog bare opplysninger som kan ha betydning som dokumentasjon. I disse tilfellene skal retting skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

I henhold til tredje ledd kan Datatilsynet uten hinder av annet ledd bestemme at mangelfulle opplysninger sperres eller slettes. Forutsetningen er imidlertid at tungtveiende personvern hensyn tilsier det. Bestemmelsen representerer også et unntak

fra arkivloven, noe som er uttrykkelig presisert i bestemmelsens siste punktum. Dette innebærer at Datatilsynets vedtak om sletting må gjennomføres, selv om opplysningene i henhold til arkivlovgivningen måtte arkiveres. Før Datatilsynet treffer slikt vedtak, skal Riksarkivaren høres.

I politiregisterloven finner man bestemmelser om retting, sperring og sletting i §§ 50 til 54. Bestemmelsene der i det alt vesentlige sammenfallende med §§ 27 og 28 i personopplysningsloven, men det finnes likevel enkelte forskjeller – både hva gjelder systematikken og innhold. I tillegg er det i utkast til politiregisterforskriften foreslått detaljerte bestemmelser om hvordan retting, sperring og sletting skal gjennomføres, mens forskriften til personopplysningsloven ikke inneholder nærmere regler om dette.

I følge § 50 første ledd skal opplysninger som ikke lenger er nødvendige for formålet slettes eller sperres, med mindre de skal oppbevares i henhold til arkivlovgivningen. I utkast til politiregisterforskrift § 16-2 er det nærmere forklart hva som menes med sletting i politiregisterloven. Kort fortalt innebærer sletting alltid at opplysningen skal fjernes fra det systemet den er registrert i. I hvilken grad opplysningen også tilintetgjøres, er avhengig av om den faller inn under arkivloven eller om den kan tilintetgjøres i henhold til arkivlovens kassasjonsbestemmelser.

Retting av opplysninger er regulert i § 51 med utfyllende bestemmelser om gjennomføringen av retting i kapittel 14 i utkast til politiregisterforskriften. I følge § 51 første ledd skal mangelfulle opplysninger rettes, og om mulig eller nødvendig supplere eller oppdateres. I annet ledd omhandles opplysninger som er beheftet med feil som ikke kan rettes. Her siktes det til opplysninger som det ikke var hjemmel for å registrere. Slike opplysninger skal slettes eller sperres. Sperring skal alltid være resultatet dersom det er grunn til å tro at sletting vil kunne påvirke den registrertes legitime interesser. Dette vil for eksempel være tilfelle dersom registreringen kan begrunne et erstatningskrav for den registrerte.

Når det gjelder sperring inneholder politiregisterloven atskillig klarere regler enn hva som er tilfelle i personopplysningsloven. For det første er begrepet definert i politiregisterloven § 2 nr. 10, hvoretter sperring innebærer en markering av opplysninger i den hensikt å begrense den fremtidige behandlingen av disse opplysningene. Hva denne begrensningen går ut på er nærmere regulert i § 51 tredje ledd og § 52. Opplysninger som sperres fordi de er mangelfulle, kan bare brukes dersom det er nødvendig for å dokumentere hva som ble behandlet av opplysninger. I § 52 gis det anvisning på at opplysninger som er slettet i medhold av §§ 50 og 51 eller på annet grunnlag bare kan brukes til de formål som gjorde at opplysningen ikke ble slettet. I utkast til politiregisterforskrift kapittel 15 er det i tillegg gitt nærmere bestemmelser om når opplysninger skal sperres, hvordan sperring gjennomføres og når sperrede opplysninger skal slettes.

Politiregisterloven § 53 regulerer politiets handleplikt ved feil eller mangler. Ifølge første punktum skal den behandlingsansvarlige så langt som mulig sørge for at

mangelfulle opplysninger eller andre brudd på loven ikke får betydning for den registrerte. Bestemmelsen er derved nærmest likelydende med personopplysningsloven § 27 første ledd siste punktum. Politiregisterloven går imidlertid noe lenger i de tilfellene der en mangelfull opplysning er utlevert til andre. Her gir § 53 siste punktum anvisning på at den behandlingsansvarlige skal varsle mottakeren av opplysningene uten unødig opphold, mens slik varsling bare er oppgitt som ett av flere alternative handlingsmønstre i personopplysningsloven § 27.

Endelig gir politiregisterloven § 54 og utkast til politiregisterforskriften kapittel 17 regler om saksbehandlingen i forbindelse med begjæringer om innsyn, sperring, retting og sletting. I personopplysningsloven finnes det ikke en tilsvarende bestemmelse. § 54 gir nærmere anvisning på hvem som kan behandle slike begjæringer og hvilke krav som stilles det innholdet og formen til begjæringen. Videre er det i annet ledd fastsatt at saksbehandlingstiden ikke skal vare lenger enn 30 dager. I siste ledd fremgår det at begrunnelsen for et avslag ikke skal tilkjennegir at vedkommende er registrert. Begrunnelsen for dette er at kunnskap om det faktum at det foreligger en registrering i seg selv kan forspille formålet med behandlingen av opplysningen ved at vedkommende da forstår at han er i politiets søkelys.

6.3.5 Klageadgang og adgang til å be om Datatilsynets kontroll

Personopplysningsloven inneholder ingen regler om adgangen til å kunne påklage avgjørelser om innsyn, retting, sperring og sletting. Dette må ses i sammenheng med at personopplysningsloven både gjelder for private og offentlige aktører. Derimot fremgår det av personopplysningsloven § 42 tredje ledd nr. 7 at Datatilsynet «etter henvendelse» eller av eget tiltak gir uttalelse i spørsmål om behandling av personopplysninger. Dersom den registrerte er misfornøyd med behandlingen av opplysninger om seg selv, herunder dersom han nektes innsyn mv, kan vedkommende henvende seg Datatilsynet med anmodning om kontroll.

I politiregisterloven er adgangen til å kunne påklage avgjørelser om innsyn, sperring, retting og sletting nedfelt i § 55 første ledd nr. 3, hvoretter slike avgjørelser kan påklages til overordnet organ. I følge bestemmelsens tredje ledd kommer bestemmelsene i forvaltningsloven kapittel VI til anvendelse «så langt de passer». Hvilke regler som passer er nærmere regulert i utkast til politiregisterforskriften kapittel 18.

I tillegg til denne klageadgangen har den registrerte i henhold til politiregisterloven § 59 rett til å be Datatilsynet om kontroll av opplysninger om seg selv, og bestemmelsen tilsvarer således personopplysningsloven § 42 tredje ledd nr. 7. Politiregisterloven opererer således med et tosporet system. Den registrerte kan både påklage en sak til overordnet organ og henvende seg til Datatilsynet. Det fremgår videre uttrykkelig av politiregisterloven § 55 tredje ledd at den registrertes rettighet til å be Datatilsynet om kontroll, ikke berøres av klagereglene i § 55. Det betyr at den registrerte kan anmode Datatilsynet om kontroll uavhengig av om klagen er fortsatt under behandling eller om vedkommende har fått avslag i klageomgangen.

6.3.6 Tilsyn og tilsynsorganets kompetanse

Det er et grunnleggende prinsipp innenfor personvernlovgivningen at all behandling av opplysninger skal kunne kontrolleres av et uavhengig tilsynsorgan. I Norge innehar Datatilsynet denne funksjonen, og Datatilsynet er således tilsynsorgan for behandling av opplysninger både i henhold til personopplysningsloven og politiregisterloven, jf. henholdsvis § 42 og § 58. I politiregisterloven er det riktig nok gjort enkelte unntak hva gjelder tilsyn med behandling av opplysninger i Politiets sikkerhetstjeneste, men dette vil utvalget ikke komme nærmere inn på her.

Når man snakker om tilsynsorganets kompetanse må det skilles mellom tilsynskompetansen og påleggskompetansen. Med tilsynskompetanse menes at organet har kompetanse til å føre tilsyn med all behandling av opplysninger hos vedkommende behandlingsansvarlige. Datatilsynet har full tilsynskompetanse både etter personopplysningsloven og politiregisterloven, noe som innebærer at det ikke finnes noen opplysninger som er unntatt fra denne kompetansen. For å kunne utøve slik tilsyn, må tilsynsorganet gis tilgang til alle opplysninger som behandles. Denne retten er nedfelt i personopplysningsloven § 44 og politiregisterloven § 61.

Når det derimot gjelder påleggskompetansen stiller dette seg annerledes. Med påleggskompetanse menes at tilsynsorganet kan gi den behandlingsansvarlige pålegg om hvordan behandlingen skal innrettes. I henhold til personopplysningsloven § 46 fjerde ledd har Datatilsynet full påleggskompetanse, ved at det der uten unntak er bestemt at tilsynet kan gi pålegg om at behandling av personopplysninger i strid med loven skal opphøre eller sette vilkår for at behandlingen kan fortsette.

I politiregisterloven er det i § 60 oppstilt begrensninger hva gjelder Datatilsynets påleggskompetanse. For det første går det et sentralt skille mellom behandling av opplysninger i og utenfor den enkelte straffesak. Utvalget går ikke nærmere inn på disse reglene, idet de ikke kan ses å ha betydning for regulering av INFOFLYT. Det som derimot er av større interesse i vår sammenheng, er unntaket i § 60 første ledd siste punktum, hvoretter Datatilsynet blant annet ikke kan gi pålegg om innsyn. Begrunnelsen for dette er at spørsmålet om innsyn i politiets opplysninger er i sterk grad preget av politifaglige vurderinger, og man ønsket ikke at Datatilsynet skulle kunne overstyre disse vurderingene. Det innebærer at et avslag på begjæring om innsyn fra politiets side, herunder klageorganet, er endelig. I de tilfellene der Datatilsynet ikke har påleggskompetanse, er det imidlertid lagt opp til at tilsynet kan gi en anmerkning til den behandlingsansvarlige med kopi til overordnet organ, jf. § 60 annet ledd. I en slik anmerkning vil Datatilsynet kunne anføre hvorfor tilsynet ikke er enig med den behandlingsansvarliges – eventuelt klageorganets – avgjørelse. Det er videre forutsatt i utkast til politiregisterforskriften § 42-3 siste ledd at den behandlingsansvarlige innen tre uker underretter tilsynet om hvordan anmerkningen er fulgt opp eller eventuelt meddeler at angjeldende behandling ikke anses å være i strid med politiregisterloven.

7 Utvalgets vurdering av hvordan INFOFLYT har vært praktisert

Formålet med dette kapitlet er å redegjøre for hvordan sakene behandles og hva de inneholder av opplysninger. I tillegg redegjøres for hvordan INFOFLYT oppleves av de som arbeider med det. Endelig redegjøres for hvilken nytteverdi politiet og kriminalomsorgen mener INFOFLYT har og utvalgets vurderinger av mulighetene for forbedringer.

7.1 Innledning

Kriminalomsorgen og politiet har alltid utvekslet informasjon om innsatte. Informasjonsutvekslingen var tidligere uregulert, fram til retningslinjene om informasjonsutvekslingen ble utarbeidet og vedtatt i 2005. Se omtalen i kapittel 3.

På tross av reguleringen fra 2005 samarbeides det etter forskjellige modeller. Noen regioner samarbeider med politidistriktene med regelmessige møter. Lokalt samarbeides det på ulike måter. Arbeidsformene er ulike og uten særskilte rutiner.

Spørsmålet som utvalget har stilt seg er om det generelle rundskrivet om informasjonsutveksling og den spesielle saksbehandlingsinstruksen for INFOFLYT følges opp i gjeldende praksis, sentralt, regionalt og lokalt. For å finne ut av dette har utvalget møtt ansatte i KSF, KRIPOS, PST, to anstalter og fire regioner. I tillegg har utvalget hatt møte med de to største tjenestemannsorganisasjonene for kriminalomsorgen, Norsk Fengsels- og friomsorgsforbund - NFF og Kriminalomsorgens Yrkesforbund - KY.

7.2 Hvordan informasjonsutvekslingen skjer i dag

7.2.1 Innledning

I det følgende beskrives hvordan det arbeides i INFOFLYT- sakene. Dette gjelder både hvordan papirmappene håndteres, rapporteringsrutiner, de inntrykk utvalget har fått av rutinene og praktiseringen av dem, samt hvordan de ansatte som arbeider med INFOFLYT beskriver samarbeidet.

7.2.2 Saksmappene

Utvalget har gjennomgått både et tilfeldig utvalg av alle saker fra 2004 til 2009, alle 2009-sakene og i tillegg et utvalg saker som omhandler forvaltningsklager. Sakene dreier seg om fare for:

- liv og helse for den innsatte eller for personkretsen rundt innsatte
- ny kriminalitet
- rømning og
- en kombinasjon av disse truslene

Per januar 2011 var det registrert 190 saker i H-arkivet. Sakene daterer seg fra INFOFLYT ble etablert som system i 2004 og fram til januar 2011. Om lag 50 av sakene

var per januar 2011 aktive saker, dvs. at 50 innsatte var registrert i systemet, markert med rødt flagg i fangesakssystemet KOMPIS. De øvrige saksmapper er fortsatt arkivert i Justisdepartementets H-arkiv for gradert materiale.

Saksmappene er registrert per innsatt. Noen saksmapper har en omfattende dokumentmengde med mye informasjon, mens andre mapper er svært tynne. Dette beror selvsagt ofte på mappens alder, men ikke alltid. En typisk saksmappe inneholder gjerne dommen som ga grunnlag for registrering i INFOFLYT, sikkerhetsvurderinger av den innsatte og forespørsler om slike, blant annet knyttet til spørsmål om flytting til anstalt med endret sikkerhetsnivå, prøveløslatelse og permisjoner. Det er i tillegg ofte vedlagt en del svært detaljerte hendelsesjournaler og rapporter.

Gjennomgangen viste at saksmappene varierer i forhold til mengde dokumenter, type dokumenter, oversikt, innhold og struktur. Ved gjennomgangen av INFOFLYT-sakene og etter samtaler med berørte tjenestemenn har utvalget funnet at arbeidet ikke alltid ser ut til å være basert på de skriftlige rutinene. Rutinene ser heller ikke alltid ut til å være fulgt.

Saksmappene fremstår som lite oversiktlige. Det er likevel visse elementer som er faste. Mappene viser korrespondansen som har foregått. I mange av sakene ligger det hendelsesrapporter. Dokumentene er som regel stemplet FORTROLIG eller STRENGT FORTROLIG. Visse saker er graderte etter sikkerhetsloven på grunn av sitt innhold. Forespørsler om sikkerhetsvurderinger og svar med slik vurdering fra politiet, er det alltid i mappene. Alle saksmappene har rødt omslag.

I enkelte saker ser det ut til at noen dokumenter mangler eller at korrespondansen har stoppet opp.

Alle innkomne og utgående dokumentene er registrert i den elektroniske journalen i Justisdepartementets H-arkiv, se omtalen i punkt 4.6.

7.2.3 Hovedfunn fra gjennomgangen

- Det er ingen dokumentliste i sakene, noe som gjør det vanskelig å få raskt oversikt over sakens relevante fakta. Noen saker synes også å mangle vedlegg.
- Det mangler oversikt over saksgangen, og det fremgår ikke klart hvem som har behandlet sakene og tatt beslutningene om for eksempel registrering
- Med få unntak er det heller ingen liste over de tjenestemenn som har skrevet inn opplysninger eller på annen måte vært sentrale i saksbehandlingen
- Mappene inneholder kopier og originaler om hverandre
- Dokumentene ligger til dels uordnet i mappene.
- Det framgår i enkelte saker ikke når vedkommende innsatt ble flagget (derimot vises dato i KOMPIS). Det framgår heller ikke dokumentasjon på avflagging eller saksbehandling knyttet til vurdering av om vedkommende bør ut av systemet.

- Begrunnelse for å flagge eller å ikke-flagge mangler ofte. Der det er begrunnelse begrenser de seg gjerne til at det på bakgrunn av politiets risikovurdering, besluttes enten å registrere opplysningene/ vedkommende i INFOFLYT, eller ikke å registrere dem.
- I enkelte saker vurderes trusselen som lav men vedkommende registreres likevel inn i INFOFLYT på tross av kravene i rundskrivet. Det er også eksempler på det motsatte.
- Mappene mangler system for oppdatering av informasjonen, f. eks. når det neste gang skal innhentes ny risikovurdering.

7.2.4 Informasjonssikkerheten i INFOFLYT-mappene

Konfidensialitetskravet synes godt ivaretatt i KSF og i H-arkivet ved forsvarlig innlåsing. Regionene har et eget låsbart arkivskap som er plassert på kontoret til en autorisert tilsatt. Utvalget har ikke undersøkt nærmere hvordan sikkerheten for øvrig ivaretas regionalt og lokalt. Utvalget har likevel ingen grunn til å tro at materialet ikke behandles etter reglene i beskyttelsesinstruksen og etter kravene nedfelt i kriminalomsorgens regelverk for informasjonssikkerhet.

Integritetskravet synes ikke tilstrekkelig ivaretatt. Det er i enkelte tilfeller ikke mulig å se om dokumenter mangler. Ofte er opplysningene lite oppdaterte og det kan være en risiko for at opplysninger kan fjernes uten at man kan se dette eller hvilke opplysninger det gjelder.

Tilgjengelighetskravet synes ikke ivaretatt tilstrekkelig. Utvalget er orientert om tilfeller der det mangler mapper, bl.a. ved at de ikke fulgte den innsatte ved soningsoverføring. Siden dokumenter til dels er usystematisk arkivert og mappen mangler oversikt over dokumentmengde og saksgang, vanskeliggjør dette en ryddig og oversiktlig tilgang til informasjonen.

7.2.5 Forsendelse

Informasjonsutvekslingen skal i henhold til rundskrivet skje i linjen og være skriftlig. Dokumentene skal forsendes etter beskyttelsesinstruksen. Politiet synes å sende per brev i stor utstrekning. I hastesaker er det imidlertid tilfeller der INFOFLYT opplysninger sendes internt i kriminalomsorgen per e-post. Det foregår også hyppig informasjonsutveksling per telefon. Det er usikkert i hvilken grad denne informasjonen skrives ned, da dette ikke framgår av papirdokumentene. For øvrig fraktes dokumenter i relativt stort omfang med bud.

7.2.6 Utvalgets vurderinger av mappene

- Selv om det er mange eksempler på god og hurtig saksbehandling, særlig i saker der en persons sikkerhet er truet og det haster med beslutninger om soningssted mv., har utvalget funnet flere tilfeller der saksbehandlingen ser ut til å ha tatt lang tid (2-3 måneder fra begjæring til svar) selv om saken synes å haste
- Mappene sikrer ikke mot uautorisert endring eller fjerning av opplysninger

- Det synes å mangle systematikk i kopiene og det er ingen rutine for oppdatering av lokal kopi, noe som kan medføre risiko for at det kan være opplysninger i en kopi som ikke er i originalen og vice versa
- Det er en stor mengde forskjellig informasjon i mappene. Mye ser ikke ut til å være spesielt sensitivt og kunne vært kommunisert i åpne kanaler
- Det synes å mangle viktige dokumenter, beslutninger og vurderinger i enkelte saker
- Graderingen synes å være noe tilfeldig
- Gjennomgangen i sakene synes å bekrefte inntrykket av at fengselet sjelden spør om risikovurdering med sikte på avflagging
- Det synes som om det er manglende klarhet i rollefordeling mellom sentralt, regionalt og lokalt nivå. Kommunikasjonen går ofte ikke i linjen slik som forutsatt i rundskrivet.
- Kvaliteten i trusselvurderingene varierer, både fra politiets side og fra kriminalomsorgens side

7.3 Kriminalomsorgens syn på INFOFLYT

Da INFOFLYT ble innført i 2004/2005 fikk instruksjonen og planene for samarbeidet en overveiende god mottakelse fra de berørte instanser. Etter hvert som INFOFLYT ble praktisert er det fremsatt en del kritikk og mangler ved systemet.

Flere av dem som utvalget har møtt fra de ulike nivåene i kriminalomsorgen har anført at INFOFLYT har betydelige mangler. Dette gjelder bl.a. manglende kontradiksjon, notoritet og kvalitet på risikovurderinger. I tillegg anføres at saksbehandlingen mangler tverrfaglighet, særlig i form av juridisk kompetanse, noe som øker faren for vilkårlige og svakt funderte vedtak. Mange av opplysningene er lite oppdaterte og irrelevante. Det blir påpekt at det mangler et apparat for å vurdere om en innsatt bør avregistreres. Dette er særlig viktig fordi det å være registrert kan gi negative konsekvenser i soningsforløpet og manglende progresjon i straffegjennomføringen.

Det kan også virke noe tilfeldig hvem registreres i INFOFLYT og hvem som ikke registreres.

Noen tilsatte som ikke er gitt tilgang til INFOFLYT, har pekt på at de vet at en innsatt er registrert i INFOFLYT, men ikke hvorfor. De mener dette er et problem og at det går utover tjenesten at de mangler vital informasjon om innsatte med mulig høy risiko for rømning/ og eller alvorlig kriminalitet.

Tilbakemeldingene kan oppsummeres slik:

- Kriminalomsorgen ønsker bedre rammebetingelser og mer ressurser til samarbeidet
- Politiets sikkerhetsvurderinger i INFOFLYT er ofte ikke oppdaterte og i enkelte tilfeller lite konkrete
- Det er forskjeller i kunnskap om INFOFLYT i de ulike fengsler

- Enkelte betjenter føler at de trenger tilgang til INFOFLYT for å gjøre en best mulig jobb, en tilgang de ikke får
- Det ser i enkelte saker ut til å mangle tilstrekkelig begrunnelse for å registrere en innsatt inn i INFOFLYT
- Det kan være tilfeldig hvem som registreres, noe som kan skape usaklig forskjellsbehandling og svekke rettsikkerheten
- Det er for svak regulering av adgangen til å behandle personopplysninger om tredjepersoner
- Det mangler viktig informasjon om potensielt farlige utlendinger
- Mye informasjon i mappene ser ikke ut til å være særlig beskyttelsesverdig
- Det uttrykkes bekymring over om politiet gir kriminalomsorgen tilstrekkelig etterretningsinformasjon
- Kriminalomsorgen gir politiet for lite informasjon i forhold til det den mottar
- For stor oppmerksomhet om det røde flagget og byråkratisk framgangsmåte forsinker søknader om permisjon mv, noe som svekker rettsikkerheten
- Det mangler rutiner for avregistrering
- Et godt fungerende system krever et tettere samarbeid mellom de to etater
- INFOFLYT må reserveres for informasjon av særlig sensitiv art
- INFOFLYT har for svak samarbeidskultur
- Kriminalomsorgen mangler kompetanse og analyseverktøy når det gjelder å samle inn og bearbeide informasjon
- Man trenger et fungerende og sikkert system for formidling av informasjon

7.4 Utvalgets inntrykk av kriminalomsorgens og politiets syn på nytteverdien

De ansatte i kriminalomsorgen og politiet opplever stort sett INFOFLYT som nyttig. Det er likevel enkelte på lokalt nivå i kriminalomsorgen som mener at INFOFLYT slik det fungerer i dag, ikke har særlig nytteverdi. Alle mener imidlertid at INFOFLYT har et stort uutnyttet potensiale. Samarbeidet etter NOKAS-ranet var meget godt og viser at det er mulig å få til gode samarbeidsformer når begge etatene føler at de har nytte av det, både at de kan gi kvalitetsmessig god informasjon, og at de kan motta nyttige opplysninger om innsatte.

7.4.1 Politiets oppfatning av nytteverdi og potensiale for dette

Utvalget har hatt møter med KRIPOS og PST og mottatt informasjon om deres oppfatning av INFOFLYT.

KRIPOS' oppfatning

KRIPOS mener at det er nyttig å ha en person fra KSF som ukentlig har arbeidssted på KRIPOS. De legger stor vekt på verdien av samarbeidet for å forebygge alvorlig kriminalitet. MC-kriminalitet ble særlig fremhevet. Samarbeidet med KRIPOS omfatter alle innsatte, ikke bare personer registrert i INFOFLYT. Dette betyr at tilbakemeldingene fra KRIPOS omfatter helheten i samarbeidet med KSF, ikke bare INFOFLYT.

I tillegg anser KRIPOS at samarbeidet er viktig fordi kriminalomsorgen alltid melder fra til KRIPOS om forestående flyttinger til annen anstalt og om permisjoner, noe som er svært viktig kunnskap for det lokale politidistriktet.

Det anføres imidlertid at samarbeidet kan bli skadelidende ved at kriminalomsorgen utleverer beskyttelsesverdig informasjon om innsatte i forbindelse med begjæringer om innsyn i opplysninger som er gitt av politiet. Dette er opplysninger som om de blir kjent vil kunne skade etterforskningen eller hindre forebygging av kriminalitet.

I tillegg mener KRIPOS at det bør fokuseres på kompetanse og profesjonalisering for å styrke informasjonsutvekslingen og kvaliteten på denne.

PSTs oppfatning

PST mener samarbeidet er nyttig men påpeker at det er et potensiale for en mer effektiv utnyttelse av INFOFLYT. PST mener det er et problem at innsatte har blitt varslet om, eller fått bekreftet ved forespørsel, at de er underlagt utvidet kontroll under soning av varetekt eller rettskraftig dom.

For øvrig har PST selv god saksbehandling og notoritet i samarbeidet med kriminalomsorgen generelt og INFOFLYT. Det er egne systemer for dette i en egen møte- og notoritetslogg. Saksbehandlingen er elektronisk.

7.4.2 Kriminalomsorgens oppfatning av nytteverdi og potensiale for INFOFLYT

Gjennom møter med lokalt og regionalt nivå og med de ansattes organisasjoner har utvalget fått et bilde av hvordan man i kriminalomsorgen ser på INFOFLYT. Det uttrykkes noe forskjellige oppfatninger av nytteverdien i dag. Noen mener at INFOFLYT er nyttig som en arena for utveksling av informasjon i forebyggingsøyemed. Andre betoner problemene og ser få fordeler med samarbeidet i dag. Særlig rettssikkerhetsmanglene, at informasjonen bruker for lang tid til å nå fram, at kvaliteten på sikkerhetsvurderingene er for dårlige og at det er for svak kompetanse og profesjonalitet i samarbeidet, fremheves.

Samtlige som utvalget har snakket med, ønsker et velfungerende INFOFLYT. Det er et stort udekket kunnskapsbehov. I framtiden forventes andelen utenlandske innsatte som er domfelt for alvorlig kriminalitet å øke, noe som sterkt øker behovet for kunnskap om kriminelle fra andre land. Dette bør framtvinge et INFOFLYT der regions- og distriktsskiller ikke hindrer informasjonsflyten og samarbeidet. Det er likevel noe ulike syn på hvor tett politiet og kriminalomsorgen bør integreres i samarbeidet. Noen er skeptiske til at politiet i for stor grad ber om opplysninger fra kriminalomsorgen og legger stor vekt på at kriminalomsorgens primære oppgave er å sikre en god straffegjennomføring som både gir god sikkerhet og bidrar til tilbakeføring til samfunnet.

7.5 Rapporteringsrutiner

Utvalget har ikke funnet noen rutiner for rapportering av hvordan INFOFLYT fungerer. INFOFLYT eller samarbeidet med politiet generelt er ikke nevnt i de årlige tildelingsbrev fra Justisdepartementet til KSF. Men i KSFs tildelingsbrev til regionene for 2012 er det tatt inn et punkt om satsing på samarbeid med politiet for å hindre alvorlig kriminalitet. INFOFLYT nevnes imidlertid ikke spesielt og tiltak for å oppnå dette er ikke nevnt utover at *«En slik utveksling må systematiseres og kvalitetssikres i størst mulig grad og (...) gjennomføres på alle nivåer.»*

INFOFLYT har ikke vært evaluert. De første årene etter at INFOFLYT ble etablert, ble det avholdt enkelte møter mellom KSF, KRIPOS og POD hvor samarbeidet ble gjennomgått. De siste årene har ikke utvalget registrert formalisert møtevirksomhet med dette formålet.

Utvalget har heller ikke registrert noen særskilt intern oppfølging i KSF av INFOFLYT som system. Andre enn de som daglig arbeider med INFOFLYT involveres bare ved juridisk behandling av klagesaker. Ekspedisjonssjefen i KSF involveres der det vurderes som nødvendig. For øvrig involveres de berørte seksjonslederne gjennom annenhånds behandling av brev som går ut. Det framstår som uklart i hvilken grad juridiske råd innhentes før det oversendes informasjon om innsatte til politiet.

7.6 Utvalgets oppsummering

Følgende ser ut til å fungere godt:

- Det er etablert et system for informasjonsutveksling på sentralt nivå
- INFOFLYT har forbedret notoriteten i sensitive saker
- God kontakt mellom sambandsmann og KRIPOS
- Det er en god oversikt over registrerte dokumenter i H-arkivet.
- Konfidensialiteten synes godt ivaretatt, i hvert fall sentralt og i enkelte regioner og lokale enheter

Utvalget har etter en gjennomgang av utvalgte saksmapper, samtaler med involvert personell på alle nivåer, samt fra KRIPOS imidlertid funnet en stor grad av uregulert praksis og ulike måter å behandle opplysningene og sakene på. Dette beror etter utvalgets oppfatning både på at instruksene ikke regulerer forholdet, og at instruksene ikke følges. Utvalget mener at systemet er underregulert, i liten grad kommunisert, lite strukturert og derfor preget av hvordan de involverte faktisk bruker det. Det har derfor dannet seg ulike måter og lokale varianter for hvordan INFOFLYT praktiseres. Utvalget mener at dette er uheldig.

Utvalget har fått flere tilbakemeldinger fra politihold om at både regelverk for innsyn, saksbehandlingen og kriminalomsorgens kompetanse må forbedres dersom politiet skal få tillit til at beskyttelsesverdig informasjon blir benyttet etter formålet for

utleveringen og ikke utleveres til uvedkommende. Utvalget fremmer derfor i kapittel 8 krav som bør stilles til et nytt regelverk, jf. regelforslagene i kapittel 11.

8 Krav som bør stilles til INFOFLYT - utvalgets vurderinger

Formålet med dette kapitlet er å redegjøre for utvalgets syn på de viktigste kravene til et nytt regelverk for INFOFLYT på bakgrunn av mandatet for utvalget og den kritikk som er framkommet mot INFOFLYT.

Informasjon fra politiet er nødvendig for at kriminalomsorgen skal kunne foreta gode risikovurderinger av enkeltindivider og grupper av innsatte og domfelte. Informasjon fra kriminalomsorgen til politiet kan bidra til å avdekke kriminalitet under straffegjennomføring og forebygge ny kriminalitet. Utvalget mener at et forbedret INFOFLYT kan bidra til å oppfylle disse målene.

8.1 INFOFLYT må forankres i et klart hjemmelsgrunnlag

8.1.1 Innledning

Kravet til hjemmelsgrunnlag er forankret i legalitetsprinsippet. Det innebærer at rettslige og faktiske inngrep fra det offentliges side overfor borgerne bare kan skje dersom det er hjemmel i lov.

Av mandatet fremgår at utvalget skal:

- foreslå regler for behandling av personopplysninger i kriminalomsorgen
- saksbehandlingsrutiner for kriminalomsorgens informasjonsutveksling
- vurdere om ny §§ 4c og 4 d i straffegjennomføringsloven gir en klar, tydelig og tilstrekkelig hjemmel for informasjonsutvekslingen med politiet
- sikre at regelverket både ivaretar formålet med informasjonsutvekslingen og rettssikkerheten til domfelte, innsatte og andre registrerte
- tilpasse regelverket til politiregisterloven.

Det synes å være uenighet om grensegangen mellom politioppgaver og kriminalomsorgens oppgaver og i hvilken grad kriminalomsorgen aktivt kan forebygge straffbare handlinger, jf. Prop. 151 L (2009-2010), se også omtalen av gjeldende rett etter straffegjennomføringsloven i punkt 4.4.

Utvalget har merket seg at departementet i lovproposisjonen fastholdt at «forebygging» av kriminalitet skulle tas inn i formålsbestemmelsen i ny § 4c. Begrepet «forebygging» ble likevel tatt ut i den endelige lovteksten og erstattet av «motvirke» kriminalitet (§ 4c bokstav c). Begrepet «motvirke» synes i hovedsak å omfatte det å forhindre kriminalitet i anstalten og bidra til rehabilitering, mens politiets oppgave er å etterforske, forebygge og hindre straffbare handlinger.

Utvalget mener at et nytt regelverk bør klargjøre i hvilken utstrekning kriminalomsorgen skal forebygge straffbare handlinger, herunder i samarbeid med politiet. Utvalget foreslår derfor at de rettslige uklarhetene fjernes for at INFOFLYT

skal kunne fylle sine formål slik de fremgår av utvalgets mandat og INFOFLYT-instruksen KSF 2/2005.

8.1.2 Legalitetsprinsippet krever klar hjemmel i lov

Utvalget legger til grunn at behandling av opplysninger INFOFLYT representerer et inngrep i den registrertes personvern og foreslår et regelverk som sikrer at de som er registrert i INFOFLYT nyter den samme personvernmessige beskyttelse som gjelder for de personer som er registrert i politiets registre.

Nødvendige opplysninger om den innsatte og personkretsen rundt vedkommende må registreres og gjøres tilgjengelig for de ansatte, herunder sensitiv informasjon knyttet til kriminelle for å unngå rømning og planlegging av ny kriminalitet. Dette kan føre til at enkelte innsatte underlegges et strengt kontrollregime. Opplysninger som innhentes vil kunne utgjøre en del av grunnlaget for nektelse av permisjoner, prøveløslatelse eller lettelser i straffegjennomføringen. Fengslet vil regelmessig kunne pålegge begrensninger i kontakt med andre personer og beslutte kommunikasjonskontroll. Disse tiltakene vil i enkelte tilfeller bli iverksatt uten at vedkommende kan ivareta sine interesser på en adekvat måte.

Jo mer inngripende tiltak mot den enkelte vil være, som kan være aktuelle som konsekvens av å være registrert i INFOFLYT, jo klarere må lovhjemmelen være. Forutsetningene og rammene for INFOFLYT må derfor komme tydelig fram i lov og forskrift. Det vises i denne sammenheng også til personopplysningsloven § 11 og politiregisterloven § 4, som stiller krav om at behandling av opplysninger må være begrunnet i konkrete formål. Dette krever klare anvisninger på systemets omfang og rammer for behandlingen slik at behandlingen ikke går ut over grensene for det definerte formålet.

Det er som nevnt usikkert om gjeldende § 7 første ledd c (innsyn) og d (unnlatt begrunnelse, jf. bokstav h (taushetsplikt) i straffegjennomføringsloven gir tilstrekkelig presis lovhjemmel for å regulere INFOFLYT.

Utvalget foreslår derfor et eget kapittel 1b om INFOFLYT med

- egen formålsparagraf i ny § 4f,
- hjemmel for utlevering av personopplysninger til politiet i ny § 4g, og
- hjemmel i ny § 4h for at behandlingen skal skje etter politiregisterlovens kapittel 8, §§ 55 første ledd nr. 3 og 59. Også politiregisterloven § 60 om Datatilsynets virkemidler, herunder til å gi pålegg, kommer etter § 4h til anvendelse for opplysninger som politiet har utlevert til kriminalomsorgen.

8.1.3 Spørsmålet om behov for et nytt tilsyns- eller kontrollorgan

Utvalget har vurdert om den registrertes interesser bør styrkes ved å opprette en uavhengig kontrollordning. Kravet om et uavhengig tilsynsorgan er nedfelt i både personverndirektivet og rammebeslutningen. Den europeiske

menneskerettighetsdomstolen (EMD) har slått fast at uavhengige kontrollorganer er en forutsetning for behandlinger der den registrerte ikke har innsynsrett.

Gjeldende kontrollordninger

Justisministeren har det konstitusjonelle og parlamentariske ansvaret for at KSF, som behandlingsansvarlig, og i kraft av sin instruksjonsmyndighet sørger for at ytre etat overholder personvernlovgivningen.

Datatilsynet har tilsynsmyndighet med kriminalomsorgens behandling av personopplysninger, også i INFOFLYT.

Sivilombudsmannens fører kontroll med forvaltningen.

Vurderinger av behovet for nye kontrollordninger

Spørsmålet er om gjeldende kontroll- og tilsynsordninger er tilstrekkelig for å ivareta den registrertes interesser. Utvalget har drøftet ulike ordninger, herunder om det bør opprettes et eget kontrollorgan for INFOFLYT, men tilrår at INFOFLYT baserer seg på gjeldende ordninger.

Utvalget har vurdert en ordning med skjult advokat etter mønster fra straffeprosessloven § 100a. En slik advokat oppnevnes ved rettslig behandling der retten har besluttet innsynsbegrensninger for parten. Advokaten representerer en rettsikkerhetsgaranti ved at vedkommende under taushetsplikt gjøres kjent med de opplysninger som parten ikke får se. Advokaten kan dermed angripe et vedtak fordi hemmeligholdte opplysninger kunne vært brukt som grunnlag for en mildere eller frifinnende dom. Utvalget finner det imidlertid problematisk å foreslå en slik ordning. Begrunnelsen er først og fremst at ordningen med skjult advokat ikke er innført i sivile saker. Videre er innsynssakene knyttet til INFOFLYT ikke av en slik art eller omfang at det tilsier å innføre en ny ordning bare for disse saker.

Utvalget er imidlertid opptatt av at det må sikres en løpende kontroll med saksbehandlingen i INFOFLYT. I tillegg til Datatilsynets og Sivilombudsmannens kontroll, foreslår utvalget å basere kontroll og tilsyn på en tydeligere lederforankring og på linjeansvaret i Justisdepartementet og KSF.

Som ledd i dette foreslås blant annet at Justisdepartementet skal være klageorgan for avgjørelser som treffes av KSF som behandlingsansvarlig, jf. forslag til § 14 i forskriften.

Det må også utvikles gode rutiner for internkontroll i forbindelse med behandling av opplysninger i INFOFLYT, se § 13 i forslaget til forskrift.

8.1.4 Behov for lovhjemmel for kriminalomsorgens adgang til å utlevere personopplysninger utenfor INFOFLYT

I hvilken utstrekning kriminalomsorgen har rett og plikt til å gi informasjon til og motta informasjon fra politiet, andre offentlige etater, forvaltningssamarbeidsparter og private bør utredes. Utvalget har gjennom sitt arbeid sett at mange ansatte i kriminalomsorgen

opplever at taushetsplikts grenser er vanskelige å trekke og at usikkerheten skaper problemer i praksis. Uklarhetene beror særlig på i hvilken grad kriminalomsorgen kan utlevere opplysninger til andre organer i mottakerorganets interesse, jf. forvaltningsloven § 13b nr. 5 og nr.6 som ikke omfatter dette.

I Ot.prp. nr.5 (2000-2001) om ny straffegjennomføringslov nevnes at departementet foreslo en klar hjemmel i høringsutkastets § 9. Departementet fant på bakgrunn av innvendinger fra høringsinstansene å trekke forslaget og henviste til at forvaltningsloven § 13 gir nødvendig hjemmel, sammenholdt med formålsbestemmelsen i straffegjennomføringsloven § 2. Det vises til omtalen av dette i proposisjonen på sidene 43-45.

Utvalgets mandat omfatter ikke dette spørsmålet, men utvalget tilrår at kriminalomsorgens informasjonsutveksling med politiet utenfor INFOFLYT og eventuelt med andre samarbeidsorganer gjennomgås med sikte på entydige regler i straffegjennomføringsloven. Utvalget tilrår at det i så fall vurderes om politiregisterloven så langt den passer, skal gjelde for all behandling av personopplysninger i kriminalomsorgen. Det vises til politiregisterloven §§ 30, jf. 27 og § 31, som setter klare rammer for politiets utlevering av opplysninger til andre offentlige organer og til private.

8.1.5 Innsyn i domstolsbehandling – tvisteloven § 22-3

Mandatet forutsetter at utvalget vurderer behovet for endringer innsynsreglene i tvisteloven § 22-3.

Dersom en innsatt bringer spørsmålet om nektelse av prøveløslatelse inn for domstolsapparatet, regulerer tvisteloven (lov 17. juni 2005 nr. 90) § 22-3 spørsmålet om adgangen til å føre bevis og til å forby bruk av bevis i den sivile saken. Utgangspunktet er at det ikke kan føres bevis som krenker lovbestemt taushetsplikt. Dette innebærer at heller ikke dommeren får forelagt opplysningene.

En forutsetning for utveksling av fortrolig informasjon er tillit til at mottakeren benytter opplysningene i samsvar med formålet for utleveringen og at opplysningene ikke blir eksponert for uvedkommende.

Faren for at sensitive opplysninger tilflyter partene under domstolsbehandling i sivile saker oppleves fra politiets side som reell og har også i praksis ført til en tilbakeholdenhet fra politiets side til å gi fra seg viktig informasjon om innsatte. Utvalget har fått flere tilbakemeldinger fra politihold om at risikoen for kompromittering utgjør en viktig hindring for å utlevere viktig informasjon om innsatte til kriminalomsorgen, se om dette i punkt 7.4.1.

Utvalget mener derfor at det bør vurderes om tvisteloven § 22-3 om bevisføring for retten, bør endres slik at mulighetene til å unnta sensitiv informasjon fra innsyn gjøres tilsvarende som i straffeprosessloven § 242a, (jf. tidligere tvistemålsloven § 204) om vitneforklaring. Dette innebærer at departementets begrunnelse for å nekte samtykke

til at beviset skal føres, ikke skal gjøres kjent for partene. I dag er det fare for at et begrunnet avslag vil være intetsigende eller vagt, nettopp av frykt for at en for konkret begrunnelse i seg selv kan bidra til å røpe en kilde, eller av andre grunner er sikkerhetsmessig uforsvarlig, noe som også er uheldig.

Tvisteloven § 22-3 er imidlertid ikke bare en utfordring for kriminalomsorgen. De samme problemstillingene kan gjøre seg gjeldende for andre offentlige organer, som for eksempel utlendingsmyndighetenes mulighet til å motta informasjon fra politiet. Utvalget mener derfor at bestemmelsen bør vurderes i en bredere sammenheng ut fra de erfaringer som de ulike etater har hatt etter lovendringen.

8.1.6 Bevisforbud etter straffeprosessloven § 117 og 118

I følge utvalgets mandat skal utvalget vurdere endringer også i disse bestemmelsene om forbud mot å ta i mot vitneforklaringer om forhold under lovbestemt taushetsplikt. I motsetning til tvisteloven § 22-3, antar utvalget at risikoen for at beskyttelsesverdig informasjon gjøres tilgjengelig for uvedkommende er langt mindre. Dette skyldes at partene og retten skal meddeles departementets begrunnelse for å nekte vitnet å forklare seg for stengte dører og under pålegg om taushetsplikt.

Det er i tillegg lite tenkelig at spørsmålet vil aktualiseres. De aktuelle opplysningene i INFOFLYT, vil bli utlevert til- og være en del av påtalemyndighetens bevisgrunnlag i straffesaken. Opplysningene vil dermed bli behandlet på samme måte som det øvrige bevismaterialet i straffesaken etter straffeprosessloven, herunder når det gjelder å hemmeligholde opplysningene. Utvalget mener derfor at det ikke er grunn til å vurdere endringer i disse bestemmelsene av hensyn til INFOFLYT.

8.1.7 Behandling av opplysninger om tredjepersoner i INFOFLYT

I Prop. 151 L (2009-2010) fremgår at departementet mener at registrering av tredjepersoner er en politioppgave. Det vises til omtalen av dette i punkt 4.4.1.

Utvalget mener likevel at kriminalomsorgen, i saker med risiko for alvorlig kriminalitet, bør få adgang til å registrere tredjepersoner i forebyggende øyemed. Opplysninger om utenforstående tredjepersoner som er i kontakt med den innsatte kan være sentrale for å forebygge alvorlig kriminalitet. Det vises til kriminalomsorgens etterretningssystemer i Sverige og Danmark, som også registrerer tredjepersoner i sine systemer.

Utvalget understreker likevel at registrering av tredjepersoner i forebyggende hensikt bare bør være aktuelt i saker der det er nærliggende grunn til å anta at en person i samarbeid med den innsatte, planlegger alvorlig kriminalitet, fysisk angrep på personer eller rømning, jf. forslaget til § 2 i bokstav a til c i forskriften. Opplysninger som gir særlig grunn til mistanke kan da stamme fra politiet, fra kriminalomsorgens egne ansatte eller fra kilder blant innsatte.

Utvalget understreker også at den nevnte forskriftsbestemmelsen ikke vil gi kriminalomsorgen adgang til å registrere tredjepersoner som ikke har kontakt med den innsatte, eller tredjepersoner som forsøker å oppnå kontakt med en innsatt.

Tredjepersoner uten en personlig relasjon med den innsatte har for øvrig ingen mulighet til å vite om at de er registrert i kriminalomsorgens systemer. Kriminalomsorgen kan dermed ikke registrere tredjepersoner bare fordi de tilhører det samme kriminelle miljøet som den innsatte, slik som politiet kan etter politiregisterloven § 5 nr. 2 hvis ikke de har andre konkrete opplysninger om at så er tilfellet.

Utvalget presiserer også at behandling av opplysninger om tredjepersoner må behandles på en betryggende måte med strenge krav til kvalitet og formålsbestemthet, i det opplysningene vil kunne bli brukt til å nekte besøk og annen kontakt med den innsatte. På denne bakgrunn vises til lovforslaget om formål for INFOFLYT i ny § 4f og forslaget til forskriften § 2 om nødvendighetskravet.

8.1.8 Lovhjemmelen bør tilpasses politiregisterloven

INFOFLYT skal være et system for informasjonsutveksling med politiet for å bekjempe kriminalitet. Siden formålet med behandlingen av opplysninger i INFOFLYT derved er sammenfallende med formålet for politiets behandling av opplysninger, er det nærliggende at det gjelder de samme behandlingsregler for henholdsvis kriminalomsorgen og politiet. Videre er store deler av de opplysninger som ligger i INFOFLYT opplysninger som kommer fra politiet. Dersom også slike opplysninger skulle reguleres av personopplysningsloven, vil man kunne risikere flere uheldige utfall. For eksempel kan man tenke seg at begjæringer om innsyn, retting, sperring og sletting får et annet utfall for den samme opplysningen, avhengig av om begjæringen rettes til kriminalomsorgen eller direkte til politiet.

En slik situasjon er verken ønskelig eller hensiktsmessig. Utvalget har i kapittel 6 gjort rede for de sentrale personvernrettslige bestemmelsene i både personopplysningsloven og politiregisterloven, herunder hva som er forskjellene. Som det fremgår der er forskjellene ikke store, slik at man ikke kan hevde at de som er registrert i INFOFLYT vil få svekket personvernet dersom man anvender politiregisterloven. Den mest markante forskjellen er at Datatilsynet ikke har påleggskompetanse i saker som gjelder innsyn, slik at en anvendelse av politiregisterlovens bestemmelser på dette punkt vil føre til at Datatilsynet heller ikke kan gi kriminalomsorgen pålegg om å gi den registrerte tilsyn. Betydningen av denne forskjellen må imidlertid ikke overdrives. Det vises her blant annet til at de fleste opplysninger i INFOFLYT er graderte, og da kan Datatilsynet heller ikke gi pålegg om innsyn.

Dernest vil man kunne hevde at politiregisterloven på enkelte områder innrømmer den registrerte bedre – eller i det minste klarere - rettigheter enn hva som følger av personopplysningsloven, jf. blant annet det tosporete system i klagesaker, jf. omtalen av dette i punkt 6.3.5.

Ved å anvende personvernreglene i politiregisterloven ved behandling av personopplysninger i INFOFLYT sikrer man en ensartet behandling av de samme opplysningene, enten de befinner hos politiet eller i INFOFLYT. Det må antas at et

felles regelverk vil gjøre det enklere for politiet å utlevere opplysninger til kriminalomsorgen, idet politiet da kan være trygg på at den videre behandlingen reguleres av de samme bestemmelsene som når politiet selv behandler opplysningene. Etter en helhetsvurdering har utvalget derfor kommet til at de beste grunner tilsier at man adopterer de aktuelle bestemmelsene i politiregisterloven for behandling av opplysninger i INFOFLYT, jf. forslaget til ny § 4h i straffegjennomføringsloven.

Som følge av dette foreslår utvalgets flertall, medlemmene Melander, Ellertsen og Sunde at forskriften om INFOFLYT ved enkelte henvisninger gir relevante bestemmelser i politiregisterforskriften tilsvarende anvendelse. Denne fremgangsmåten synes å være særlig hensiktsmessig fordi bestemmelsene det vises til utelukkende er saksbehandlingsregler.

Utvalget er enstemmig om at reglene i politiregisterloven om de registrertes rettigheter får anvendelse for INFOFLYT. Et mindretall, medlemmene Enger og Sand har imidlertid en lovteknisk dissens. De mener, som utvalgets flertall, at det er hensiktsmessig med rettslikhet på dette området for å ivareta politiets og kriminalomsorgens behov for å verne sensitiv informasjon i forbindelse med utveksling mellom etatene til grunn i forhold til INFOFLYT og at politiregisterloven derfor bør legges til grunn for INFOFLYT.

Under henvisning til at det bør være en målsetting å tilrettelegge for et godt og anvendelig regelverk for de som skal bruke det, som i størst mulig grad sikrer en ensartet og korrekt praksis på området, fremstår det for mindretallet som klokt å bearbeide og innarbeide de aktuelle bestemmelser i utkast til ny forskrift til INFOFLYT, fremfor alene å henvide til disse. Lovteknisk er begge løsninger fullt ut gangbare. Det er imidlertid viktig for, mener mindretallet, at et regelverk i størst mulig grad fremstår som selvstendig, uten parallellhenvisninger til andre regelverk. Dette gjør regelverket vesentlig mer anvendelig for dem som skal praktisere det og som ikke nødvendigvis har juridisk bakgrunn eller har full kunnskap om hvor rettskildene befinner seg, at rettskilder er gjenstand for endringer, analogisk anvendelse av rettsregler mv. Desto enklere, oversiktlig og klart forskriften utformes, desto bedre må det kunne antas at bestemmelsene håndteres korrekt av kriminalomsorgen.

Etter mindretallets syn bør ikke forslaget til forskrift vise direkte til en forskrift som på nåværende tidspunkt er til høring og som det er noe uenighet rundt, spesielt fra Politidirektoratets og KRIPOS' side. INFOFLYT er fullstendig avhengig av tillit fra politi- og påtalemyndigheten. Å koble håndteringen av INFOFLYT direkte til et utkast til regelsett som sentrale deler av politi- og påtalemyndighet er kritisk til, synes mindre klokt.

8.2 Saksbehandling og samarbeid

8.2.1 Kompetanse, tillit og samarbeidsfora

Utfordringene

Av mandatet fremgår at utvalget skal:

- kartlegge hvordan informasjonsutvekslingen skjer i dag
- foreslå regler for behandling av opplysninger
- foreslå hvilke saksbehandlingsrutiner som bør følges ved informasjonsutveksling

God informasjonsutveksling forutsetter et godt samarbeid og metodisk tilnærming og kompetanse. Både Stortingsmelding nr. 37 (2007-2008) «Straff som virker» og Meld. St.7 (2010-2011) om organisert kriminalitet fremhever dette som viktig. Det vises også til Riksrevisjonens undersøkelse som nevnt i kapittel 3. Politiloven § 2 nr. 5 og 6 forutsetter at politiet samarbeider med andre organer og bistår dem for at organene skal kunne løse sine oppgaver.

Utvalgets inntrykk etter besøk og intervjuer er at det samarbeides for lite på alle nivåer, med store variasjoner og i for stor grad uformelt. Imidlertid har det vært samarbeidet godt i enkelte saker. Et eksempel er NOKAS-ranet som utløste et tett og godt samarbeid mellom kriminalomsorgen og politiet. Utvalget mener at dette viser at et operativt og profesjonelt samarbeid er mulig, noe som er en sentral forutsetning for å videreføre og videreutvikle INFOFLYT.

Et godt samarbeid vil avhenge av det utvikles felles arenaer for gjensidig informasjonsutveksling og drøfting av forhold knyttet til enkeltsaker. Dette kan bidra til at man får et felles mål for samarbeidet og felles forventninger til hva samarbeidet skal gi begge parter. Utvalget foreslår at samarbeidet forankres på høyt ledernivå og fremgår av de årlige tildelingsbrev og øvrige styringsdokumenter.

Kriminalomsorgen vurderer i dag selv om innsyn helt eller delvis bør gis. Av hensyn til kriminalitetsbekjempelse og kildebeskyttelse bør opplysningene som mottas fra politiet beskyttes bedre enn i dag. Det må sikres at kriminalomsorgen først forelegger innsynsbegjæringer for politiet, se forslaget til forskrift i § 5.

Streng tilgangsstyring, sikker informasjonsutveksling og færrest mulige nivåer

Når politiet utleverer beskyttelsesverdig informasjon må politiet ha tillit til at kriminalomsorgen behandler den på en betryggende måte. Opplysningene må holdes skjult når det er nødvendig – også for den innsatte selv - og bare benyttes til de formål politiet har utlevert dem for.

For å ivareta kravet om sikker tilgangsstyring, informasjonsutveksling, lagring, logging og kontroll vil utvalget understreke behovet for et moderne saksbehandlingsverktøy og utvalget anbefaler at departementet prioriterer dette i det videre arbeidet.

Som ledd i å øke tilliten til at sensitiv informasjon kun brukes til det formål de er utlevert for, foreslår utvalget å ta bort regionenes rolle i konkrete saker, med mindre de som førsteinstans har beslutningsmyndighet, jf. straffegjennomføringsloven § 11, og derfor har behov for å få utlevert beskyttelsesverdig informasjon om den innsatte. Det vises til forslaget til forskrift § 8 som legger opp til en to-nivå saksbehandling i innsynssaker. Hensikten er dels å redusere antallet personer med tilgang til informasjon, og dels at en tre-nivåmodell som i dag, blir for omstendelig. I tillegg vil ikke regionenes ansatte ha en nærhet til og kunnskap om de aktuelle innsatte som forsvarer bruken av regionale ressurser til dette arbeidet.

Flagget i KOMPIS

Tilbakemeldinger fra politiet viser at systemet med den synlige eksistensen av “flagg” i det felles fangesakssystemet KOMPIS, i seg selv har ført til svekket tillit fra politiets side til at kriminalomsorgen behandler opplysningene de får med tilstrekkelig konfidensialitet. Det at alle ansatte med tilgang til en person i KOMPIS kan se flagget, anses i seg selv som en sikkerhetsrisiko og kan føre til at politiet blir tilbakeholdne med å utlevere opplysninger gjennom INFOFLYT-kanalen.

Utvalget mener at flaggingen bør erstattes med et system der bare de autoriserte ansatte vet at det er opplysninger om en innsatt som har særlig grad av beskyttelsesinteresse og som ikke skal framgå av KOMPIS. Samtidig må det markeres i merknadsfeltet at ledelsen ved det enkelte fengsel kontaktes før det treffes vedtak om permisjoner, soningsprogresjon mv. for vedkommende. Informasjonen må gjøres mest mulig nøytral av hensyn til at kun autoriserte ansatte skal kjenne til at det dreier seg om sensitiv etterretningsinformasjon.

Kompetanse

I dag er det ingen felles metodikk eller systematikk i håndtering, analyse og bruk av informasjon. St. meld nr. 37 (2009-2010) «Straff som virker» forutsetter som nevnt i kapittel 3 at kriminalomsorgen i framtiden må arbeide etter en felles metodikk og systematikk. Også tildelingsbrevet til regionene stiller krav om dette men uten at tiltakene for bedre arbeidsmåter konkretiseres. Behovet for å utvikle et nytt metodisk system som kan gjøre kriminalomsorgen bedre til å håndtere og bruke denne type informasjon på en måte som ivaretar rettssikkerhetsmessige og sikkerhetsmessige hensyn, gjelder i høyeste grad også for INFOFLYT.

Krav til kvalitet på opplysningene er nødvendig for å treffe riktige vedtak overfor denne gruppen innsatte. Kompetanse, grundighet og likebehandling ved saksbehandlingen og vedtaket er avgjørende for å oppnå kvalitet. De innsatte må gjøres kjent med sine rettigheter og mulighetene til å klage. De som skal arbeide med disse sakene må derfor både ha kompetanse til å håndtere sensitiv informasjon og ha juridisk kompetanse.

Utvalget tilrår at det blir brukt betydelig ressurser på kompetansebygging. Kriminalomsorgen har i dag et vel utbygd opplæringsprogram i informasjonssikkerhet, som bør utbygges til å omfatte den særlige behandlingen i INFOFLYT.

Autorisasjon for tilgang til etterretningsinformasjon bør imidlertid kreve opplæring utover det som kriminalomsorgen i dag tilbyr. Det bør derfor sikres en egen opplæringspakke for behandling av slike opplysninger, herunder opplæring i analyse og kvalitetsvurdering av etterretningsinformasjon og bruk av slik informasjon i kriminalomsorgen. En slik opplæring bør gjennomføres i samarbeid med politiet. Det vises som eksempel til politiets metode for trusselvurderinger, omtalt i 4.6 og ordningen med opplæring i Danmark, som omtalt i punkt 5.2 ovenfor.

Det vises også til kravene i Danmark til fengselsfaglig eller juridisk kompetanse, samt ledererfaring for å arbeide med slike saker. I tillegg kreves det sertifisering i «Risk-Management» og kurs hos politiets etterretningstjeneste. Utvalget mener at tilsvarende krav bør innføres for personell som skal arbeide med INFOFLYT. Kompetansekravene for kunnskap og bevissthet i de rettslige normene og etiske standarder for behandling av sensitive personopplysninger bør reguleres i en instruks for INFOFLYT.

Det vises til forslaget til § 8 annet ledd i forskriften.

Forpliktende samarbeid

Utvalget har vurdert om det bør opprettes en rådgivende samarbeidsgruppe bestående av personer fra kriminalomsorgen og politiet.

Utvalget understreker at det fortsatt vil være viktig å opprettholde skillet mellom de to etaters ulike roller og med klare ansvarslinjer. Utgangspunktet bør derfor være at oppgaveløsningen følger linjeansvaret i begge etater.

Dette forhindrer imidlertid ikke at tverretatlige strukturer bør opprettes. Utvalget mener det bør etableres en samarbeidsgruppe mellom KRIPOS og KSF for å utveksle informasjon, gjennomgå erfaringer og samarbeide om behandlingen av konkrete saker mv. Det vises til sammenligning til det operative teamet for å effektivisere soningsoverføring fra Norge til utlandet. Teamet ble opprettet i oktober 2010 og består av medlemmer fra KSF, Politidirektoratet, Oslo Politidistrikt og UDI. Erfaringene fra dette samarbeidet synes gode etter det utvalget kjenner til.

INFOFLYT må følges opp med rapporteringsrutiner og med sterk forankring i ledelsen i kriminalomsorgen. Det må sikres at systemet blir underlagt tilstrekkelig kontroll og styring.

I forskriftsutkastet i § 5 foreslår utvalget at departementet plikter å sørge for gode rutiner for samarbeid.

Utvalget tilrår at et nytt INFOFLYT bør evalueres av kriminalomsorgen og politiet i samarbeid når det har vært i drift i 2-4 år. Dette for å se om det har virket etter forutsetningene og som grunnlag for forbedringer.

8.2.2 Hvem som kan registreres, kvalitet på opplysninger og bruken i en risikovurdering

Utfordringene

Utvalget mener at dagens rundskriv er for vagt i forhold til å regulere hvilke innsatte som kan registreres inn i systemet og etter hvilke kriterier og hvor lenge de bør være i systemet. Utvalgets oppfatning er at mange som er i INFOFLYT burde vært tatt ut, se omtalen i punkt 7.2. Samtidig er det mange innsatte som ikke er registrert i INFOFLYT som utfra farlighetsgrad burde vært det.

Et spesielt problem, som også har vært trukket fram av flere tilsatte i kriminalomsorgen som arbeider med disse sakene, er at kriminalomsorgen mangler både verktøy og kompetanse til å risikovurdere innsatte og til å vurdere kvaliteten i den informasjonen de utveksler, jf. punkt 7.4. Dette gjelder særlig den informasjon kriminalomsorgen selv innhenter, men kan også i en viss grad omfatte opplysninger de mottar fra politiet.

Informasjon fra innsatte kan være av så vidt varierende sannhetsgehalt og kvalitet at det trengs innsikt i hvordan opplysningene bør vurderes og følges opp. I tillegg bør det være innebygd en vurdering av hvilke motiver disse kildene kan ha av å gi kriminalomsorgen informasjonen.

Flere tiltak bør vurderes. På kort sikt må kvaliteten i saksbehandlingen bedres og her er kompetansehevning viktig. Det bør også innføres rutiner som sikrer at det jevnlig undersøkes om opplysningene om innsatte er oppdaterte og korrekte. Som ledd i dette bør informasjonsflyten så snart som mulig gjøres elektronisk. Det kan være vanskelig å sikre god notoritet og oppfølging av hver enkelt sak, bl.a. jevnlig revurderinger av risiko, kun ved hjelp av manuell behandling. Det fremstår som en særlig utfordring at den mest komplette opplysningssamlingen ligger sentralt lagret, og ikke tilstrekkelig tilgjengelig for dem som antakelig skal gjennomføre revisjon av innholdet. I tillegg kan hensynet til sikker håndtering av dokumentene bli skadelidende med manuell behandling, oppbevaring, forsendelse, mv. Det vises her til beskyttelsesinstruksen § 12, som krever at graderte dokumenter «så langt det passer» behandles elektronisk i samsvar med sikkerhetslovens forskrift om informasjonssikkerhet. Se også forslaget til retningslinjer om behandling av gradert informasjon i punkt 10.3.2.

Utvalget mener at opplysninger ideelt sett bør kategoriseres etter en kriminalitetstype eller område som ikke kan knyttes til en bestemt person. Dette kan suppleres med en egen "VIC"-liste (Very Important Criminal), slik det gjøres i Sverige. Utvalget ser likevel at dette forutsetter et elektronisk register eller registre, slik at opplysningene kan kobles opp mot hverandre. Det vises også til at kriminalomsorgen både i Sverige og Danmark har gode elektroniske systemer og bruker betydelige personellressurser på dette. Se omtalen om dette i kapittel 6.

Det tar for lang tid fra det bes om en risikovurdering til vurderingen foreligger, se omtalen i kapittel 7. Ofte haster det med en vurdering for å hindre alvorlig kriminalitet,

eller for å sikre den innsatte en rask behandling av en søknad om permisjon eller prøveløslatelse mv, basert på ny informasjon. Det trengs derfor et tettere samarbeid med klare regler for oppfølging slik at frister settes og holdes.

Kvalitetssikring av opplysninger og system for risikovurdering

Personopplysningsloven § 11 bokstav e) krever at personopplysningene som behandles er korrekte og oppdaterte. I visse tilfeller vil kriminalomsorgen måtte basere beslutninger på opplysninger som er uverifiserte, for eksempel for å sikre liv og helse til en informant. Utvalget har fått tilbakemelding fra sine møter med anstaltene og regionene at kvaliteten på informasjonen, både innhentet internt og fra politiet, ofte er for dårlig som grunnlag for tiltak. Det er også et problem at politiets sikkerhetsvurderinger fort kan bli foreldet og utdaterte.

For å oppfylle lovgivningen og formålet med behandlingen på en god måte, bør det sikres et nærmere samarbeid og hyppigere vurderinger basert på kunnskap om de farligste innsatte og personkretsen rundt disse.

Man må skille mellom faktaopplysninger, opplysninger fra kilder med god pålitelighet og rykter basert på etterretning. Det trengs derfor et system for kvalitetssikring av etterretningsinformasjon som sikrer at bruken av opplysningene skjer etter en nøye vurdering av kvalitet på informasjonen. Politiets "4X4" system for å vurdere opplysningenes sannhetsgehalt som grunnlag for risikovurdering kan være et egnet verktøy.

Det kan være fornuftig å benytte politiets maler for kvalitetsvurdering. Kriminalomsorgen har derfor behov for en vesentlig kompetanseoppbygging på dette feltet og et eget verktøy for sikkerhetsvurderinger og mulighet for å kunne ettergå opplysninger de mottar eller selv innhenter.

I situasjoner der det haster og det antas å være høy risiko, bør kriminalomsorgen og politiet vurdere risikonivået i felleskap. Dersom de to etater har felles oppfatning av sikkerhetstrusselen, vil det sikre riktige vurderinger og vedtak. Det kan være tvil om kildenes troverdighet og sannferdighet, noe som trolig øker behovet for at begge etaters vurderinger inngår med basis i en nær dialog. Se forslaget til § 5 i forskriften om å sikre rutiner for samarbeid

8.2.3 Samarbeid internt i kriminalomsorgen

Utvalget mener at KSFs samarbeid med lokalt nivå bør baseres på lokale sambandsmenn ved enhetene som kan registrere i systemet, men ikke ha tilgang. Det vises til tilsvarende ordning i Sverige, omtalt i punkt 5.1.

Utvalget har registrert at svar på henvendelser og saksbehandling ofte tar for lang tid, særlig innad i kriminalomsorgen. Telefon og e-post brukes for å få rask tilbakemelding, særlig når tiltak haster. INFOFLYT-instruksen legger opp til at det kan ringes når det haster. De som arbeider med sakene i et nytt INFOFLYT bør få klare frister å forholde

til for å nedtegne opplysningene og registrere dem i saken. I tillegg må det sikres at gradert informasjon forsendes på en betryggende måte, ved bud, rekommanderte postsendinger mv. I disse sakene er notoritet, god saksbehandling og dialog viktig. Opplysningene må gjenfinnes i skriftlig form, være ordnet og av god kvalitet. Kompetanseutvikling vil også være sentralt, jf. utvalgets forslag til kompetansekrav i forskriften § 8 annet ledd. Et fremtidig rundskriv bør for øvrig stille klare krav til kvalitet på saksbehandlingen, se punkt 10.3.

8.2.4 Internasjonalt samarbeid

I dag har ikke kriminalomsorgen noe avtalefestet samarbeid med andre lands kriminalomsorgsmyndigheter, verken generelt eller i INFOFLYT om bestemte innsatte eller grupperinger av disse med forgreininger på tvers av landegrensene. Unntaket er saker med soningsoverføring. All informasjon om bestemte innsatte må utveksles via politimyndighetene med hjemmel i avtaler om politisamarbeid over landegrensene.

Ofte får ikke norske fengsler viktig informasjon om utenlandske innsatte som skal sone her. Stadig flere innsatte i norske fengsler er utenlandske og har tidligere sonet i hjemlandet. Mange av disse har også sonet tidligere i Danmark og Sverige. Antallet utenlandske innsatte i nordiske fengsler antas å øke vesentlig i årene som kommer. Dette kan tilsi et formalisert samarbeid mellom de nordiske landenes fengselsmyndigheter.

Både i og utenfor INFOFLYT vil kriminalomsorgen ha behov for opplysninger om personer som tidligere har sonet i et annet land. Det kan dreie seg om kunnskap om en person som kan være relevant i forhold til hvem vedkommende eventuelt ikke bør sone sammen med. Som eksempel kan nevnes krav til å forebygge organisert kriminalitet og hensynet til liv og helse til andre innsatte. Informasjon fra politiet vil ofte være mangelfull eller fengselet får ingen informasjon overhode. Derfor kan det være hensiktsmessig om fengselsmyndighetene kunne henvende seg direkte til det andre landets tilsvarende myndighet og få trusselvurderinger og andre opplysninger om personer direkte. Taushetsplikten vil som regel hindre at slik informasjon kan utveksles. Det vil være et brudd på taushetsplikten om norsk kriminalomsorg gir svenske myndigheter taushetsbelagt informasjon om en innsatt, bortsett fra tilfeller der en innsatt skal overføres til soning i Sverige. I sistnevnte tilfelle må de to land utveksle trusselvurderinger av sikkerhetsmessige årsaker.

Dette kan tilsi bilaterale avtaler eller konvensjoner som gir hjemmel til å gi informasjon til et annet avtaleland om personer som har soningstilknytning til flere avtaleland og som driver grenseoverskridende kriminalitet. Representanter fra kriminalomsorgen i Sverige og Danmark har gitt uttrykk for et ønske om et formelt samarbeid. Utvalget mener at spørsmål om et slikt internasjonalt samarbeid er et spørsmål som bør utredes i en annen sammenheng da mandatet ikke nevner dette særskilt. En slik utredning bør omfatte all informasjonsutveksling med utenlandske kriminalomsorgsmyndigheter, ikke bare INFOFLYT.

9 Økonomiske og administrative konsekvenser

9.1 Økonomiske konsekvenser

9.1.1 Tiltak på kort sikt

Mandatet forutsetter at det også foreslås en ordning uten at det tilføres ressurser. Utvalget mener det vil være svært vanskelig å få til et velfungerende INFOFLYT uten noe tilførsel av personell, betydelig kompetanseoppbygging og etablering av strukturerte samarbeidsfora. I tillegg er det et stort behov for å innføre et databasert saksbehandlingssystem med tilstrekkelig sikkerhet.

Utvalget antar likevel at noe kan oppnås ved å innføre rutiner og gi skikkelig opplæring, uten at det medfører store økonomiske merkostnader. Det vil imidlertid uansett være behov for en betydelig kompetanseoppbygging på kort sikt og noe merbemanning for å redusere sårbarheten. Minimumsbehovet er vanskelig å anslå. Sårbarhetsproblemet og merkompetansebehovet tilsier etter utvalgets mening at det må ansettes 1-2 ekstra personer på sentralt nivå i KSF. Videre bør det vurderes om det er behov for 1 person som er dedikert til INFOFLYT i enkelte fengsler og avdelinger med høyt sikkerhetsnivå. Avhengig av omfanget av arbeidet i et fremtidig INFOFLYT kan ressurstilførselen kunne tilsvare om lag 6-10 årsverk i økt bemanning i kriminalomsorgen. Dette vil kunne gi en styrking også til det generelle sikkerhetsarbeidet i kriminalomsorgen fordi INFOFLYT-sakene på lokalt nivå neppe vil kunne fylle en 100 prosent stilling. Inkludert kostnader til kompetanseoppbygging tilsvarer dette på usikkert grunnlag en merkostnad på om lag 8-10 mill. kroner per år i forhold til i dag.

9.1.2 Tiltak på lengre sikt

Det bør anskaffes et moderne databasert saksbehandlings- og arkivsystem. Det bør utredes om det kan inngå som en modul i kriminalomsorgens saksbehandlings- og arkivsystem og/ eller integreres i det elektroniske fangesakssystemet KOMPIS, men med sikkerhetsmessige barrierer og med sikker tilgangsstyring. Behandlingsmåten forutsettes fortsatt å skje etter beskyttelsesinstruksen, som i § 12 slår fast at graderte dokumenter skal behandles elektronisk i samsvar med sikkerhetslovens forskrift om informasjonssikkerhet.

Kriminalomsorgen arbeider nå med et tilgangsstyringssystem – IAM. Dette styrker sikkerheten og det bør vurderes å legge INFOFLYT inn som en modul i DocuLive, tilknyttet KOMPIS. IAM forutsettes å bli satt i verk i 2012.

Ved utveksling av informasjon mellom KSF og KRIPOS, og mellom KSF og regionene og videre ut til anstaltene bør det være krypterte linjer, noe som øker kostnadene.

Utvalget mener at et prosjekt bør utrede et INFOFLYT i et databasert saksbehandlings- og arkivsystem der både politiet, påtalemyndigheten og kriminalomsorgen har direkte

tilgang. Det må avklares om eierskapet til et slikt INFOFLYT bør ligge hos politiet eller kriminalomsorgen, eventuelt i et felleskap.

Det er vanskelig å anslå kostnadene til dette og årsverksbehovet. Dette vil avhenge av utformingen og omfanget. Et elektronisk system for sikker utveksling av informasjon internt, utveksling med politiet og eventuell felles tilgang, anslås avhengig av omfanget av løsninger og sikkerhetssystemer å koste mellom 20-40 mill. kroner.

I dag er Justisdepartementets behandling av alt gradert materiale fullt ut papirbasert, dvs. også utenfor INFOFLYT og kriminalomsorgen. Kostnaden kan derfor bli påvirket av en eventuell innpassing i en prosess mot elektronisk samhandling i hele justissektoren.

Det vises for øvrig til punkt 5.2 om den danske kriminalomsorgens etterretningssystem. Det arbeider 6 personer i kriminalomsorgen etterretningssenter. Senterets databaseverktøy kostet 1,5 mill. kroner i anskaffelse.

9.2 Administrative konsekvenser

Et forbedret manuelt system for utveksling av informasjon vil måtte få kostnader i form av kompetanseoppbygging og til ny organisering av arbeidet i kriminalomsorgen for å sikre at de fastsatte kravene til personvern og effektivitet etterlevs.

Utvalget tilrår at et nytt INFOFLYT undergis en grundig evaluering når det har vært i drift i 2-4 år.

10 Merknader til forslaget til regelendringer

Utvalget har i regelutformingene søkt å balansere de til dels motstridende hensyn på en god måte. Kravene til personvern, innsynsrett, forvaltningsmessige krav til saksbehandlingen og klagerett må ivaretas, samtidig som sikkerheten i straffegjennomføring, taushetsplikt, forebygging av alvorlig kriminalitet og andre personers sikkerhet ivaretas gjennom et nært samarbeid mellom politiet og kriminalomsorgen. I lovforslagene om den registrertes rettigheter kommer politiregisterloven til anvendelse.

10.1 Merknader til forslaget til lovbestemmelser

Det foreslås et nytt kapittel 1b i straffegjennomføringsloven som regulerer behandling av opplysninger i INFOFLYT. Kapitlet består av tre bestemmelser om henholdsvis formål, utlevering av opplysninger til politiet og den registrertes rettigheter.

Til § 4f. Formål med behandlingen av personopplysninger

I følge mandatet skal “..utvalget vurdere om (...) ny §§ 4c og 4d i straffegjennomføringsloven (...) gir en klar, tydelig og tilstrekkelig hjemmel for informasjonsutvekslingen med politiet.”

Utvalgets forslag til ny § 4f gir kriminalomsorgen en eksplisitt hjemmel til å kunne behandle personopplysninger i for å forebygge, hindre og bekjempe alvorlig kriminalitet. En slik hjemmel er nødvendig av flere årsaker. Det er behov for mer klarhet enn den gjeldende § 4c, som er mer rettet mot straffegjennomføringen, sikkerhet i fengsel og å forhindre rømning. Dernest sikrer den at kriminalomsorgen kan samarbeide med politiet og påtalemyndigheten i saker med alvorlig kriminalitet.

Hva som er «alvorlig» kriminalitet foreslås ikke entydig definert. Det synes hensiktsmessig gi et betydelig rom for fleksibilitet. Begrepet er også vanlig i ulike bestemmelser i lovgivningen uten å ha et entydig innhold. Begrepet angir derfor en retning i samsvar med gjeldende INFOFLYT-instruks og den praksis som har utviklet seg i de årene INFOFLYT har vært i funksjon. Dette innebærer at INFOFLYT også i fremtiden skal konsentreres om å bekjempe organisert kriminalitet, terror, vold, grove overgrep, rømning og hindre fare for liv og helse for innsatte, ansatte og andre personer. Dette betyr at mer hverdagslig kriminalitet med lavere strafferammer normalt ikke vil kvalifisere til registrering i INFOFLYT.

Det er likevel viktig å understreke at bestemmelsen ikke er ment å representere endringer i forhold til hva som er kriminalomsorgens kjerneoppgaver. Det er fortsatt politiet som skal bekjempe kriminalitet, men kriminalomsorgen må ha mulighet til å bidra til politiets kriminalitetsbekjempende virksomhet når saken involverer innsatte.

Til § 4g. Utlevering av personopplysninger til politiet og påtalemyndigheten

Gjeldende rett for kriminalomsorgens adgang til å utlevere opplysninger til politiet og påtalemyndigheten er omtalt i punkt 4.4.3. Siden gjeldende rett kan skape tvil om

omfanget av kriminalomsorgens adgang til å kunne utlevere opplysninger til politiet, foreslås det en egen hjemmel for utlevering av opplysninger til politiet med tilknytning til INFOFLYT.

Bestemmelsen fastslår at taushetsplikten ikke hindrer utlevering av opplysninger i INFOFLYT til politiet og påtalemyndigheten. Utleveringen kan bare skje for å ivareta formålene for straffegjennomføringen i § 4c, og de særskilte formålene i INFOFLYT i forslaget til ny § 4f. Utleveringen kan skje uavhengig av om den er i politiets interesse eller i kriminalomsorgens interesse.

Bestemmelsens siste alternativ sikrer at det også kan utleveres opplysninger som ennå ikke er registrert i INFOFLYT, så lenge de er nødvendige som ledd i en risikovurdering som skal foretas av politiet.

Til § 4 h. Den registrertes rettigheter ved behandling av personopplysninger i INFOFLYT

Kriminalomsorgens behandling av personopplysninger reguleres av personopplysningsloven. Utvalget foreslår imidlertid at man for behandling av opplysninger i INFOFLYT adoperer bestemmelsene i kapittel 8 og §§ 55 og 59 i politiregisterloven. Kapittel 8 i politiregisterloven regulerer informasjonsplikt, innsyn, retting, sperring og sletting, mens §§ 55 og 59 regulerer henholdsvis den registrertes klageadgang over vedtak om innsyn mv og adgang til å be Datatilsynet om kontroll av opplysninger som behandles om vedkommende. Forslaget er først og fremst begrunnet i at det fremstår som den beste løsningen at kriminalomsorgen og politiet må forholde seg til det samme regelverk hva gjelder de omtalte forhold, særlig hensett til at hovedformålet med behandling av opplysninger i INFOFLYT er kriminalitetsbekjempelse. Anvendelsen av de nevnte bestemmelsene i INFOFLYT svekker heller ikke den registrertes personvern og rettigheter. Politiregisterlovens bestemmelser om innsyn, retting, sperring og sletting er i det alt vesentlige sammenfallende med de tilsvarende bestemmelsene i personopplysningsloven, men er i større grad innrettet på de særlige behov som gjør seg gjeldende i politiet. Bestemmelsene i politiregisterloven §§ 55 og 59 derimot sikrer den registrerte bedre rettigheter. Personopplysningsloven inneholder ingen regler om klage på vedtak om innsyn, retting og sletting. Den registrertes adgang til å be om kontroll kommer til uttrykk i lovens § 42 tredje ledd nr. 7, hvoretter tilsynet etter henvendelse eller av eget vedtak skal gi uttalelse i spørsmål om behandling av personopplysninger. I politiregisterloven opereres det med et tosporet system. Den registrerte kan både klage over vedtak om innsyn, retting, sletting mv samtidig som vedkommende kan be om Datatilsynets kontroll av de samme forholdene, jf. omtalen om dette i punkt 6.3.5 i rapporten.

I bestemmelsens annet ledd foreslås det i tillegg at politiregisterloven § 60 om Datatilsynets kompetanse gis tilsvarende anvendelse for opplysninger som politiet har utlevert til kriminalomsorgen. Som det fremgår av omtalen i punkt 6.3.6 har Datatilsynet ikke påleggskompetanse hva gjelder spørsmålet om innsyn i politiets

opplysninger. For å etablere ensartethet foreslås det derfor at også denne bestemmelsen i politiregisterloven kommer til anvendelse. Dette gjelder dog bare opplysninger som er mottatt av politiet. For kriminalomsorgens egne opplysninger vil Datatilsynet fortsatt ha full påleggskompetanse i henhold til personopplysningsloven.

10.2 Merknader til forslaget til forskrift

Til § 1. Formålet med forskriften

Formålet er å ivareta kriminalomsorgens oppgaver etter forslaget til § 4f som er å forebygge, forhindre og bekjempe alvorlig kriminalitet. I tillegg henviser bestemmelsen til hensynene i straffegjennomføringsloven § 4c bokstavene a-e. Som eksempel nevnes hensynet i § 4c bokstav b om ro og orden og sikkerhet for innsatte, domfelte og samfunnet for øvrig.

Samtidig slås det fast at personvernet til den registrerte skal ivaretas.

Formålsbestemmelsen omfatter bare behandling av beskyttelsesverdige opplysninger. I et papirbasert INFOFLYT vil slik informasjon normalt bare inngå i gradert materiale etter beskyttelsesinstruksen og i få tilfeller etter sikkerhetsloven (rikets sikkerhet mv.).

Til § 2. Nødvendighetskravet

Bestemmelsen begrenser behandlingen til det som er nødvendig ut fra formålet. Det stilles krav til at behandlingen er saklig begrunnet, at det er sannsynlig at behandlingen faktisk bidrar til å oppnå formålet, og at behandlingen av personopplysningene er forholdsmessige etter en avveining av hva man kan oppnå, sett opp mot konsekvensene for den registrertes personvern.

I *første ledd* angis hvem det kan behandles personopplysninger om. Dette er innsatte, ansatte, besøkende og andre personer som nevnt i straffegjennomføringsloven § 4d.

Når det gjelder «andre personer» er det ikke tvilsomt at straffegjennomføringsloven § 4 d hjemler behandling av opplysninger om familiemedlemmer, venner og kolleger og andre den innsatte har et forhold til og som ønsker kontakt med den innsatte, samt personer som søker tilgang til fengselsområdet.

Spørsmålet er om personkretsen også kan omfatte personer som den innsatte har en relasjon til og som kan føre til at den innsatte alene eller sammen med personen begår ny kriminalitet. Som nevnt i punkt 4.4 og 8.1.7 gir neppe gjeldende kapittel 1a om behandling av personopplysninger i straffegjennomføringsloven tilstrekkelig hjemmel til å behandle personopplysninger, herunder tredjepersoner i kriminalitetsbekjempende øyemed.

Utvalget mener at forslaget til ny § 4f som utvider formålet til å omfatte forebygging og kriminalitetsbekjempelse, sammenholdt med at formålsbestemmelsen her også viser til behandling etter formålsbestemmelsen § 4c, gir tilstrekkelig hjemmel til å

forskriftsfeste at kriminalomsorgen kan behandle opplysninger i INFOFLYT om tredjepersoner som har eller prøver å få kontakt med den innsatte i den hensikt å begå alvorlig kriminalitet. Det vises også til at lovens § 4d bokstav b, som omhandler behandling av opplysninger om «*andre som har eller prøver å oppnå kontakt med den domfelte (...)*», henviser til § 4c.

Det må imidlertid kreves at den innsatte har tilknytning til den aktuelle tredjepersonen. Det kan ikke behandles opplysninger om andre, for eksempel i et gjengmiljø som den innsatte har kontakt med, uten at det er en personlig kontakt eller tilknytning mellom den innsatte og den aktuelle personen. Kriminalomsorgen kan dermed ikke registrere tredjepersoner utelukkende fordi de tilhører det samme kriminelle miljøet som den innsatte.

I *annet ledd* gis det anvisning på at bestemmelsen også gjelder for personer som gjennomfører straff i regi av friomsorgen eller ved elektronisk kontroll.

I *tredje ledd* stilles det krav om at det må foreligge objektive holdepunkter for å anta at vilkårene i første ledd er oppfylt, dvs. forhold som indikerer kriminell virksomhet, i motsetning til en ren subjektiv vurdering. Kravet er sammenfallende med nødvendighetskravet i politiregisterloven § 5 første ledd nr. 2 a om vilkårene for behandling av opplysninger til kriminalitetsbekjempelse utenfor den enkelte straffesak.

Til § 3. Krav til opplysningenes kvalitet

Bestemmelsen regulerer hvilke krav som stilles til opplysningenes kvalitet og er i samsvar med kravene som stilles i personopplysningsloven § 11 første ledd bokstavene b og politiregisterloven § 6 første og annet ledd, men det er tilføyd en nærmere forklaring i annet ledd om hva kvalitetskravene innebærer. Det vises også til utkast til politiregisterforskriften kapittel 5.

Første ledd lister opp hvilke krav som stilles til opplysningenes kvalitet. Opplysningene må være tilstrekkelige, relevante, korrekte og oppdaterte. De må slettes når de ikke lengre er nødvendige for behandlingen.

I *annet ledd* gis det en nærmere forklaring av kravene om tilstrekkelighet og relevans. Bestemmelsen er identisk med utkast til § 5-1 i politiregisterforskriften.

Etter *tredje ledd* kan ikke-verifiserte opplysninger behandles dersom dette er nødvendig utfra formålet. Bestemmelsen tilsvarer politiregisterloven § 6 annet og tredje ledd. Som politiet vil kriminalomsorgen ha behov for å kunne behandle ikke-verifiserte opplysninger i INFOFLYT, og denne adgangen bør komme frem i forskriften.

Til § 4. Behandlingsansvaret

Bestemmelsen regulerer behandlingsansvaret. Behandlingsansvaret er omtalt og definert i omtalen av personopplysningsloven i punkt 4.3.2.

I første ledd foreslås at det er KSF som er behandlingsansvarlig for opplysninger i INFOFLYT. Selv om ny §§ 4b og 4e i straffegjennomføringsloven legger opp til at behandlingsansvaret kan legges på et lavere nivå enn KSF ved behandlingen av personopplysninger i kriminalomsorgen, bør ikke dette gjelde for INFOFLYT. Informasjon i INFOFLYT er av særlig sensitiv karakter og ansvaret bør derfor plasseres hos sentral myndighet.

I annet ledd omtales den behandlingsansvarliges plikter. Bestemmelsen er identisk med utkast til § 2-2 i politiregisterforskriften.

I tredje ledd gis det anvisning på at det daglige behandlingsansvaret kan delegeres, jf. tilsvarende utkast til politiregisterforskriften § 2-3. Det er viktig å understreke at det her ikke er tale om å delegere behandlingsansvaret som sådan. Behandlingsansvaret vil alltid være plassert hos den øverste lederen i det organet som har behandlingsansvaret. Det er derimot tale om å delegere ansvaret for å løse de løpende oppgavene som er nødvendige for å ivareta behandlingsansvaret. I praksis vil det være nødvendig at det daglige behandlingsansvaret delegeres både til ansatte hos den behandlingsansvarlige og til underordnede organer.

Til § 5. Samarbeid mellom politiet og kriminalomsorgen

Utvalget mener at utveksling av personopplysninger i INFOFLYT må struktureres og formaliseres i større grad enn i dag. Justisdepartementet og KSF skal legge til rette for at informasjonsutvekslingen med politiet formaliseres og forbedres. Det foreslås derfor en plikt for departementet til å legge til rette for dette ved å etablere gode rutiner. I tillegg skal samarbeidet skape tillit til at mottakerens bruk av opplysningene er i samsvar med de pålegg eller vilkår som er gitt av avsenderen av opplysningene. Selv om kvaliteten av et samarbeid ikke kan regelfestes, mener utvalget at en forskrift som pålegger departementet å sørge for gode rutiner og tillit gir en forpliktelse for kriminalomsorgen til å legge til rette for faste samarbeidsformer med politiet og påtalemyndigheten.

Samarbeidet omfatter viktige områder som å effektivisere informasjonsutvekslingen og saksbehandlingen i vanskelige innsynssaker. Det er også viktig å sikre at de to etater sammen kan analysere enkeltsaker og vurdere praksis. På denne måten kan man i størst mulig utstrekning oppnå en felles forståelse av hvordan regelverket skal håndteres.

Til § 6. Fremgangsmåte ved registrering

Utvalget mener at bestemmelsen kan være et viktig bidrag for å presisere kravene til saksbehandling.

I første ledd slås det fast at det er den behandlingsansvarlige som beslutter om opplysninger skal behandles i INFOFLYT. Beslutning om registrering kan være en del av det daglige behandlingsansvaret og kan derfor delegeres. Videre skal slik beslutning være skriftlig og begrunnet. Pålegget om skriftlighet og begrunnelse sikrer ikke bare

notoritet men gir også en viss garanti for at en beslutning om registrering er veloverveid. Annet punktum om at begrunnelsen skal angi hvilke holdepunkter avgjørelsen bygger på og hva som er formålet med behandlingen, er ment som et absolutt minstekrav til hva begrunnelsen skal inneholde. Utover dette bør begrunnelsen også inneholde en nærmere beskrivelse av nødvendighetskravet, men utvalget finner ikke at dette bør være obligatorisk i hvert tilfelle.

I *annet ledd* er det lagt opp til at opplysningene i hovedsak skal registreres etter standard opplysningskategorier. På denne måten sikrer man ensartet praksis, at de nødvendige opplysningene blir registrert og bedre oversikt over hvilke opplysninger som registreres. At kravet skal gjelde i ”hovedsak”, er begrunnet i at INFOFLYT foreløpig er et papirregister og at det kan være vanskelig å innføre krav om kategorisering for slike papirregistre. Bestemmelsen tar derfor i større grad sikte på et fremtidig elektronisk system.

Til § 7. Utlevering av opplysninger til politiet og påtalemyndigheten

Etter *første ledd* kan behandlingsansvarlige beslutte utlevering av opplysninger til politiet og påtalemyndigheten for formål som nevnt i § 1 og for å hindre hendelser som nevnt i § 2 (nødvendighetskravet).

Annet ledd tilsvarende politiregisterloven § 27 siste ledd, annen og tredje setning om kravene til skriftlig utlevering og nedtegning av det som utleveres. Unntaket fra kravet om skriftlighet før utlevering vil være særlig aktuelt i de tilfeller opplysningene er nødvendige for å avverge et nært forestående lovbrudd eller rømning. Unntaket er imidlertid ikke permanent, idet den behandlingsansvarlige etter utleveringen skal foreta nedtegning.

Det vises for øvrig til den utførlige reguleringen i utkastet til politiregisterforskrift kapittel 9.

Til § 8. Tilgang til opplysningene

I *første ledd* gis for det første anvisning på at det kun er ansatte i kriminalomsorgen som kan få tilgang til INFOFLYT, jf. tilsvarende krav for tilgang til opplysninger i fangesakssystemet KOMPIS. Det vises til tilsvarende regulering i politiregisterloven § 21, som regulerer adgang til direkte søk i elektroniske registre. For det andre kreves det for tilgang at vedkommende ansatte blir særskilt bemyndiget. På denne måten kan den behandlingsansvarlige utpeke de personer som skal gis tilgang samtidig som et krav om særskilt bemyndigelse er egnet til å hindre og oppdage uautorisert tilgang til opplysningene.

I tillegg til de formelle kravene om ansettelsesforhold og bemyndigelse forutsetter tilgang at vedkommende har tjenestemessig behov, det vil si at tilgang er nødvendig for å utøve virksomheten i samsvar med regelverket.

I *annet ledd* stilles det krav om opplæring og at vedkommende i tillegg må sikkerhetsklareres. Selv om det normalt bare arbeides med opplysninger som er

gradert FORTROLIG eller STRENGT FORTROLIG etter beskyttelsesinstruksen, kan det også være aktuelt å arbeide med saker som angår rikets sikkerhet. Den autoriserte vil da arbeide med dokumenter som er graderte etter sikkerhetsloven og som dermed fordrer sikkerhetsklarering etter lovens § 19. I tillegg sikres at vandelen til de autoriserte ansatte er oppdatert slik at man kan fange opp at en ansatt er ilagt straffereaksjoner eller er under straffeforfølgning. I slike tilfeller må det her som ellers vurderes om vedkommende likevel skal sikkerhetsklareres.

I *tredje ledd* slås fast at det er den behandlingsansvarlige som gir bemyndigelse (autorisasjon). Bestemmelsen i annet punktum indikerer at antallet personer, som skal gis tilgang INFOFLYT, skal holdes så lavt som mulig. Sistnevnte er dels begrunnet i den registrertes personvern, og dels i at man på denne måten reduserer faren for spredning av opplysningene.

Til § 9. Nærmere om innsyn

Bestemmelsen gir ikke nærmere anvisning på innholdet i innsynsretten, men er utelukkende begrunnet i pedagogiske hensyn. Begrepet «innsyn» har for det første ulikt innhold i de lovene som gjør seg gjeldende i forbindelse med innsyn i INFOFLYT. Dernest kan det være hensiktsmessig at det tydeliggjøres hvilke lover som kan komme til anvendelse i forbindelse med saker knyttet til innsyn. Når personvernlovgivningen, herunder personopplysnings- og politiregisterloven, gir rett til innsyn, innebærer dette utelukkende at vedkommende kan få innsyn i opplysninger om seg selv. Dette i motsetning til såkalt partsinnsyn, slik som man finner det i forvaltningsloven, der vedkommende har rett til å gjøre seg kjent med sakens dokumenter. Partsinnsyn er således ikke begrenset til opplysninger om en konkret person, men omfatter i utgangspunktet alle opplysninger som ligger i saken.

Når det gjelder innsyn i opplysninger i INFOFLYT kan det tenkes at spørsmålet må løses i henhold til forskjellige lover. Det er dette bestemmelsen gjør oppmerksom på.

Dersom den registrerte utelukkende ber om innsyn i opplysninger om seg selv, gjelder politiregisterloven § 49, jf. bestemmelsens *første ledd*.

Dersom opplysningene er graderte, skal de behandles etter sikkerhetsloven eller beskyttelsesinstruksen, jf. *annet ledd*. Dette innebærer blant annet at det må foretas en vurdering om å nedgradere opplysningene før det gis innsyn, jf. også forskrift til sikkerhetsloven § 2-13.

Dersom opplysningene i INFOFLYT er brukt som grunnlag for et avslag på en søknad om permisjon, vil opplysningene også være en del av permisjonssakens dokumenter. I så fall gjelder forvaltningslovens regler om partsinnsyn med de begrensninger som fremgår av straffegjennomføringsloven § 7 første ledd bokstav c, jf. *tredje ledd*.

Til § 10. Retting, sperring, og sletting av opplysninger

Utvalget foreslår at politiregisterloven §§ 50 og 51 skal gjelde, jf. lovforslaget til ny § 4h. § 50 regulerer sperring og sletting av opplysninger som ikke lenger er nødvendige for formålet, mens § 51 regulerer retting, sperring og sletting av opplysninger som er mangelfulle. Anvendelsen av politiregisterloven §§ 50 og 51 er av pedagogiske grunner nevnt i *første ledd*. I tillegg foreslås at også bestemmelsene i utkastet til politiregisterforskrifter kapitlene 14, 15 og 16 kommer til anvendelse, jf. nærmere om dette nedenfor, med mindre ikke noe særskilt er bestemt i nærværende forskrift.

I *annet ledd* foreslås det slike særlige regler ved at det gis regler om hvilke rutiner som skal gjelde for å oppfylle bestemmelsene om retting, sperring og sletting. Utvalget mener at det er viktig at opplysningene i INFOFLYT gjennomgås med jevne mellomrom for å kontrollere om de fortsatt er nødvendige og eller ajourførte mv. Det foreslås derfor et krav om minst én gang i året å gjennomgå opplysningene med sikte på sletting av opplysninger som er ukorrekte, ufullstendige, ikke lenger er oppdaterte eller nødvendige for formålet. Dette sikrer at opplysningene som behandles har tilstrekkelig kvalitet og fortsatt er nødvendige for formålet med behandlingen. Utvalget mener at en slik rutine ivaretar den registrertes personvern på en god måte. Bestemmelsen i *tredje ledd* er en videreføring av annet ledd. Mens den behandlingsansvarlige etter annet ledd kan nøye seg med en gjennomgang, kreves det i henhold til tredje ledd at det må gis en skriftlig begrunnelse for oppbevaring av opplysningene utover 3 år. En slik rutine sikrer ytterligere at den behandlingsansvarlige har et bevisst forhold til spørsmålet om fortsatt registrering er nødvendig.

Bestemmelsen i *fjerde ledd* tilsvarer politiregisterloven § 51 annet ledd

I siste ledd gis det anvisning på at politiregisterforskriften kapittel 14, 15 og 16 om henholdsvis retting, sperring og sletting gjelder tilsvarende så langt de passer.

I det følgende foretas en kort gjennomgang med henblikk på hvilke bestemmelser i kapitlene 14 – 16 som passer eller som ikke passer.

Kapittel 14 regulerer retting av opplysninger.

§ 14-1 gir anvisning på at bestemmelsene i kapittel 14 bare gjelder så fremt ikke noe annet er bestemt i del 11 om politiets registre, noe som innebærer at eventuelle særlige bestemmelser om retting i forskriftene til de ulike registre går foran. § 14-1 vil således ikke kunne brukes direkte for INFOFLYT, men den vil kunne ha indirekte betydning. Dersom det for eksempel er aktuelt at en opplysning i INFOFLYT skal rettes, og angjeldende opplysning kommer fra politiet, må opplysningen rettes på samme måte som politiet ville rette den. Slike tilfeller vil bli fanget opp, idet nærværende forskrift § 12 annet ledd siste punkt legger opp til at KSF må forelegge saken for politiet før det treffes vedtak om bl.a. retting.

§ 14-2 regulerer hvilke feil som kan rettes. Bestemmelsen vil kunne anvendes i sin helhet, men annet ledd nr. 3 må leses slik at retting kan finne sted dersom behandlingen av opplysningene er i strid med straffegjennomføringsloven eller INFOFLYT-forskriften.

§ 14-3 om retting av feil etter begjæring eller av eget tiltak og § 14-4 om hvordan uriktige eller mangelfulle opplysninger skal rettes, kan anvendes i sin helhet.

Kapittel 15 regulerer sperring av opplysninger.

Den generelle bestemmelsen i § 15-1 vil bare være av interesse, dersom politiet har utlevert opplysninger til INFOFLYT fra et register, der det er gitt særskilte bestemmelser om sperring av opplysninger.

§ 15-2 om sperring av opplysninger vil kunne anvendes i sin helhet.

§ 15-3 om hvilke opplysninger som skal sperres kan anvendes i sin helhet, med unntak av annet ledd nr. 4 som ikke passer for INFOFLYT-forskriften.

§ 15-3 om videre behandling av sperrede opplysninger kan anvendes med unntak av første ledd nr. 2.

Kapittel 16 regulerer sletting av opplysninger.

Den generelle bestemmelsen i § 16-1 vil bare være av interesse, dersom politiet har utlevert opplysninger til INFOFLYT fra et register, der det er gitt særskilte bestemmelser om sletting av opplysninger.

§ 16-2 første ledd definerer begrepet sletting og vil kunne få tilsvarende anvendelse for INFOFLYT. For INFOFLYT vil kriminalomsorgens bevarings- og kassasjonsrundskriv gjelde, der det fremgår at INFOFLYT-dokumenter som oppbevares hos KSF skal bevares. Slettingen betyr i disse tilfellene at opplysningene ikke lenger skal være tilgjengelig for bruk for det formål de ble samlet inn for, men må fortsatt oppbevares inntil de avleveres til Riksarkivet.

§ 16-3 om sletting av opplysninger som ikke lenger er nødvendige for formålet, § 16-4 om sletting av opplysninger som er rettet eller som er mangelfulle og § 16-4 om sletting av sperrede opplysninger vil kunne anvendes i sin helhet på INFOFLYT.

§ 11. Bruk av opplysninger som er sperret

Bestemmelsen slår fast at opplysninger som er sperret bare kan brukes til de formål som gjorde at de ikke ble slettet, og er derved sammenfallende med politiregisterloven § 52 første punktum. Den videre bruken av sperrede opplysninger er nærmere regulert i politiregisterforskriften kapittel 15, som § 10 siste ledd viser til.

I utgangspunktet skal kriminalomsorgen slette opplysninger som ikke lenger er nødvendige, eller som er mangelfulle eller uriktige. Sperring skal skje når sletting vil

kunne frata den innsatte muligheten til å dokumentere sitt krav ved en for eksempel en senere søknad om erstatning.

§ 12. Saksbehandling i saker om innsyn, retting, sperring og sletting

Bestemmelsen regulerer hvilke saksbehandlingsregler som skal gjelde i forbindelse med begjæringer om innsyn, retting, sperring og sletting. Utvalget foreslår at man også her adopterer de tilsvarende bestemmelsene i politiregisterforskriften, men det er likevel nødvendig med enkelte særbestemmelser.

I første ledd gis det anvisning på at begjæringer om innsyn mv. skal leveres til den enhet der vedkommende soner, idet dette fremstår som den mest hensiktsmessige fremgangsmåten, jf. også behandlingsreglene i annet ledd. Bestemmelsen kan imidlertid ikke forstås slik at en begjæring blir å avvise dersom den registrerte fremmer den for den behandlingsansvarlige eller et annet organ. I så fall må det organet som mottar begjæringen videresende den til enheten der den registrerte soner mv.

I annet ledd gis det nærmere regler om hvordan begjæringen behandles. Det er enheten der vedkommende soner som undergir begjæringen forberedende behandling. Dette innebærer for det første at enheten må undersøke om begjæringen oppfyller de formkravene som oppstilles i siste ledd. Videre er det lagt opp til at enheten skal gi en anbefaling til den behandlingsansvarlige om begjæringen bør tas til følge eller ikke. Avgjørelsen ligger imidlertid kun hos den behandlingsansvarlige, enten begjæringen tas til følge eller ikke. I siste punktum er det foreslått en sikkerhetsventil for de tilfellene der angjeldende opplysning ble utlevert fra politiet. Dersom den behandlingsansvarlige vurderer å etterkomme begjæringen, skal den i disse tilfellene alltid forelegges politiet for uttalelse før saken avgjøres. Begrunnelsen for dette er at politiet i disse tilfellene kan være nærmere til å vurdere om den registrerte bør få medhold.

Tredje ledd henviser til politiregisterloven § 54 annet og tredje ledd, samt politiregisterforskriften § 17-2 til § 17-4 så langt de passer.

Henvisningen til § 54 annet ledd innebærer at begjæringen skal avgjøres senest innen 30 dager, men henvisningen til tredje ledd innebærer at et avslag ikke skal tilkjennegi at det foreligger en registrering.

Henvisningen til § 17-2 innebærer at det stilles de samme formkravene til begjæringer om innsyn mv. i INFOFLYT som for tilsvarende begjæringer i politiets registre. Når det gjelder § 17-3 er det først og fremst dens tredje og fjerde ledd som er av interesse, idet tredje ledd gir anvisning på hvordan innsyn skal gis og fjerde ledd gir anvisning på hvordan negative vedtak skal utformes. Henvisningen til § 17-4 innebærer at begjæringer om retting, sperring og sletting forutsetter at vedkommende tidligere har fått innsyn i angjeldende opplysning.

Til § 13. Informasjonssikkerhet og internkontroll

Utvalget foreslår at det for ordens skyld vises til at bestemmelsene om informasjonssikkerhet og internkontroll, jf. personopplysningsloven §§ 13 og 14, gjelder for INFOFLYT.

Til § 14. Klage

I *første ledd* gis det anvisning på at avgjørelser som gjelder begjæring om innsyn, retting, sperring og sletting kan påklages til Justis- og beredskapsdepartementet, slik det fremgår av politiregisterloven § 55 første ledd nr. 3. Begrunnelsen for at det bare henvises til § 55 første ledd nr. 3 er at de øvrige forholdene som er listet opp i § 55 (taushetsplikt, vandelskontroll og erstatning) ikke er av interesse for INFOFLYT. Siden slike vedtak treffes av KSF som behandlingsansvarlig, er Justis- og beredskapsdepartementet som overordnet organ, rette klageinstans.

I *annet ledd* gis der uttrykk for at bestemmelsene i utkast til politiregisterforskrift kapittel 18 kommer til anvendelse så langt de passer. De bestemmelsene som passer er følgende:

§ 18-1 første ledd nr. 1 og 2 gir uttrykk for at vedtak om innsyn, retting, sperring og sletting er gjenstand for klagebehandling. Videre passer siste ledd, der det gis anvisning på at vedtaket i klageinstansen ikke kan påklages og hva som gjelder for klager over avvisningsvedtak.

§ 18-3 første ledd regulerer hvem som kan klage og bestemmelsen kan anvendes tilsvarende for INFOFLYT.

§ 18-5 regulerer nærmere forholdet mellom adgangen til å klage og til å begjære tilsynsmyndighetens kontroll. Denne bestemmelsen kan anvendes tilsvarende i sin helhet, jf. nærmere om innholdet i det tosporete system i punkt 6.3.5.

§ 18-6 regulerer klagefrist, klagens form og innhold, og kan anvendes tilsvarende.

§ 18-7 gir anvisning på saksbehandlingsregler i klagesaker og kan anvendes tilsvarende.

Til § 15. Ikrafttredelse

Forskriften vil kunne tre i kraft på samme tid som lovendringene. Utvalget tilrår imidlertid at det på forhånd utarbeides en ny saksbehandlingsinstruks, noe som er nødvendig for å gjøre INFOFLYT fullt ut operativt fra første dag.

10.3 Behov for regulering i rundskriv/ saksbehandlingsinstruks

10.3.1 Generelt

Mandatet forutsetter at utvalget skal foreslå retningslinjer for saksbehandlingen. Utvalget har valgt å gjøre forskriften detaljert og vil derfor begrense seg til å ta opp

viktige sider som bør reguleres i rundskriv. Det bør etter utvalgets oppfatning først tas standpunkt til lov- og forskriftsforslagene før detaljerte saksbehandlingsinstrukser utformes.

Det vil slik utvalget ser det, være et betydelig behov for regulering av de ulike elementene i en instruks. Når systemet har virket en stund vil det trolig melde seg behov for ytterligere regulering av saksbehandlingen. De regionale og lokale ledd kan eventuelt også få behov for egne retningslinjer, utfra deres varierende behov og bruk av INFOFLYT.

Rundskrivet bør struktureres og hjemles etter paragrafene i forskriftene. En ny instruks bør utformes i detalj av en egen prosjektgruppe i forbindelse med den videre behandlingen av lov- og forskriftsutkastet om INFOFLYT.

Et sentralt element som bør reguleres i rundskrivet er hvordan et tett samarbeid mellom politiet og kriminalomsorgen skal legges opp for å skape tillit. I dette samarbeidet bør KRIPOS og KSF ha faste kontaktpersoner som har en arena for faste møter, eventuelt gjennom en samarbeidsgruppe. Gruppen bør håndtere både samarbeidet generelt og opp mot konkrete saker. Det er også viktig med en instruksfestet arbeidsdeling mellom den sentrale samarbeidsgruppen og de lokale autoriserte.

Det vises her til samarbeidet i Sverige og Danmark, som har laget strukturer for samarbeidet mellom de ulike etater som berøres av organisert kriminalitet mv. Et velfungerende samarbeid er avhengig av at de ansatte i kriminalomsorgen har god opplæring, forståelse og kompetanse i å behandle etterretningsinformasjon. Også på dette området kan sertifiserings- og opplæringsordningene i Danmark og Sverige tjene som eksempel, se omtalen av dette i kapittel 5.

Informasjonen som behandles og utveksles vil i hovedsak være etterretningsinformasjon. Så lenge slik beskyttelsesverdig informasjon er papirbasert bør opplysningene graderes etter sikkerhetsloven eller beskyttelsesinstruksen. På sikt bør opplysningene behandles elektronisk og håndteres slik politiet gjør det, blant annet gjennom tilgangsstyring i stedet for gradering av papirdokumenter. Dette tilsier at graderingsregimet og det senere tilgangsstyringsregimet bør reguleres i instruks og ikke i forskrift.

Følgende hovedelementer bør inngå i et rundskriv/ instruks:

- Hvordan informasjonsflyten bør skje internt i kriminalomsorgen
- Krav til kompetanse og opplæring av personell
- Formalisering av det interne samarbeidet, herunder arbeidsfordeling mellom autorisert personell på sentralt og lokalt nivå
- Hvordan kriminalomsorgen skal håndtere mottatt informasjon fra politiet,

- Hvordan sikre at politiet alltid forespørres om avgradering og høres før innsyn gis i gradert informasjon
- Hvordan opplysningskvaliteten skal vurderes (bruk av "4x4")
- Hvordan kriminalomsorgen skal utlevere informasjon til politiet, herunder
- I hvilken grad den skal utleveres som råmateriale eller bearbeides
- Formalisering av samarbeidet med politiet regionalt og lokalt
- Graderingsregime og nedgradering
- Tilgangsstyring
- Regulering av antall nivåer som skal involveres generelt og i enkeltsaker spesielt, herunder regionenes eventuelle rolle som nivå for saksbehandling i enkeltsaker

10.3.2 Særlig om behandling av gradert informasjon

Det er i dag et problem at dokumenter er graderte uten at opplysningene ser ut til å være beskyttelsesverdige. Det kan også være et problem at ugraderte og graderte dokumenter oppbevares sammen. Det er viktig for et fungerende samarbeid at de opplysninger som registreres er relevante for formålet. Det blir også enklere å behandle innsynssøknader dersom beskyttelsesverdig informasjon i størst mulig grad kan klassifiseres og holdes atskilt fra informasjon som kan gjøres offentlig kjent eller kjent for parten.

Det skal ikke gis innsyn i gradert informasjon. Men også i slike saker skal graderende enhet vurdere innsynsbegjæringen konkret med sikte på mulig avgradering. Ved innsynsbegjæringer i gradert informasjon skal kriminalomsorgen forelegge politiet dokumentene som politiet har gradert før innsynsbegjæringen behandles. Dette følger av kravet i beskyttelsesinstruksen § 5 nr. 4 om at et dokument bare kan nedgraderes av den etat som har foretatt graderingen. Se også reguleringen av gradert materiale forskriftsutkastet om informasjonsplikt og innsyn i § 11. De særskilte hensyn som gjør seg gjeldende i INFOFLYT-samarbeidet, tilsier at innsyn etter utvalgets oppfatning bør reguleres særskilt for INFOFLYT-opplysninger.

I et papirbasert INFOFLYT vil de fleste dokumentene fortsatt graderes på grunn av sitt innhold. I det følgende beskrives derfor noen forutsetninger og elementer som må være på plass i en framtidig rutine for kriminalomsorgens behandling av graderte dokumenter i INFOFLYT:

I: Formål:

Kriminalomsorgen må behandle gradert informasjon i overensstemmelse med beskyttelsesinstruksen §§ 2-5 og § 6 og sikkerhetsloven, straffegjennomføringsloven § 7 første ledd h, jf. c og d, og politiregisterloven §§ 30 og 35. Taushetsplikten og personvernet må ivaretas for de registrerte personene. Politiet må ha tillit til at rutinene for dette følges.

II: Organisering:

Kriminalomsorgens sentrale forvaltning (KSF) er kontaktleddet med politi- og påtalemyndigheten. All utveksling av informasjon mellom etatene skal skje via KSF. Regionalt og lokalt nivå i kriminalomsorgen gis tilgang til gradert informasjon via KSF, og i det omfang KSF vurderer det som nødvendig og forsvarlig.

Personell som skal ha tilgang til gradert informasjon må være sikkerhetsklarert og gitt opplæring i behandling av slik informasjon.

III: Behandling av registrert informasjon

- Når KSF eller regionalt/lokalt nivå mottar gradert informasjon fra politiet, skal informasjonen straks analyseres, kvalitetssikres og nødvendige tiltak iverksettes. Internt registrert informasjon må også undergis en grundig analyse og kvalitetskontroll som ledd i sikkerhetstiltak og utlevering til politiet.
- Opplysningene skal sammenstilles med eventuelle andre relevante opplysninger som enheten besitter. All relevant informasjon skal nedtegnes skriftlig.
- Det markeres i fangesakssystemet KOMPIS at det finnes gradert informasjon knyttet til en innsatt for å sikre at den bemyndigete kontaktes før det blir tatt avgjørelser som berører den innsatte (prøveløslatelse, permisjoner mv.). Det bør også vurderes å hente inn ny oppdatert informasjon. Markeringen i KOMPIS må være nøytral for ikke å røpe at det dreier seg om gradert etterretningsinformasjon.
- Lokalt og regionalt nivå må straks overlevere den informasjon som de enten har utarbeidet selv eller som de har mottatt fra enheter i politiet, til KSF etter reglene i beskyttelsesinstruksen § 10. De originale saksdokumentene skal sendes med mindre tidsmessige hensyn forhindrer det.
- KSF avgjør om informasjonen skal videreformidles til politiet. KSF beslutter om informasjonen skal bearbeides før utlevering.
- Dokumentene skal oppbevares etter beskyttelsesinstruksen § 9.
- KSF – evt. via regionen - skal sørge for at lokalt nivå straks får underretning om gradert informasjon som angår den eller de innsatte som er plassert i enheten.
- Et fullstendig kopisett av sakens dokumenter skal beholdes på lokalt og regionalt nivå, jf. § 9 i beskyttelsesinstruksen.

IV: Særlig om behandling av gradert informasjon i KSF

KSF er koordinerende behandler av all gradert informasjon i kriminalomsorgen. KSF skal til enhver tid ha oversikt over all gradert informasjon i etaten og være ansvarlig for at gradert informasjon videreformidles i den grad det er nødvendig og forsvarlig.

KSF er behandlingsansvarlig for behandling, oppbevaring og videreformidling av gradert informasjon i INFOFLYT og skal på forespørsel fra lokalt og sentralt nivå gi bistand.

V: Behandling av søknader fra innsatte som er registrert med gradert informasjon:

Når lokalt nivå vurderer søknader fra innsatte som er registrert med gradert informasjon, må informasjonen leses grundig, herunder vurdere om det bør innhentes ny informasjon med betydning for søknaden. KSF skal alltid konfereres før lokalt nivå *innvilger* søknader om første permisjon, overføring til annen fengselsenhet, frigang, straffavbrudd eller løslatelse. Lokalt nivå bør også konferere med KSF i forbindelse med andre søknader, dersom dette kan ha sikkerhetsmessig betydning.

Tilsvarende behandlingsmåte gjelder for regionalt nivå når dette nivået har avgjørelsesmyndighet, jf. straffegjennomføringsloven § 6.

- a) Ved *søknad om første permisjon, overføring til annen fengselsenhet, frigang, straffavbrudd eller løslatelse*, skal lokal enhet orientere KSF om at det er framsatt søknad. KSF bør bes om å foreta ytterligere undersøkelser om den graderte informasjonens fortsatte relevans. KSF skal også bes om å foreta nye undersøkelser om den innsatte med relevans for søknaden.

Lokalt nivå må aldri avgjøre søknaden eller meddele for den innsatte eller dennes fullmektig om antatt saksutfall før KSFs vurdering er mottatt.

- b) Ved *søknad om overføring* til annen fengselsenhet må den enhet en innsatt skal flyttes fra, med innstillingen til mottakende fengsel, vedlegge et særskilt skriv der det orienteres om at det er registrert gradert informasjon om innsatte i INFOFLYT. Denne informasjonen skal gjøres kjent før overføringen effektueres.

Mottakende fengsel skal som ledd i en overføringssak, be KSF om tilgang til den graderte informasjonen før eventuell innvilgelse av søknaden.

- c) Ved *søknad om prøveløslatelse med møteplikt for friomsorgen* skal lokalt nivå snarest orientere KSF om saken og hvilket friomsorgskontor som skal forestå møteplikten. KSF skal ta stilling til i hvilket omfang friomsorgskontoret skal bli gjort kjent med den graderte informasjonen og gi lokalt nivå tilbakemelding om dette.

VI: Rutinemessig oppdatering av informasjon:

Lokalt nivå tillegges ansvar for rutinemessig å rette henvendelser til KSF, med anmodning om å foreta en oppdatering av mottatt gradert informasjon fra politiet. Informasjon som er innhentet internt skal oppdateres jevnlig, ikke sjeldnere enn årlig, jf. forslaget til forskrift § 10.

VII: Håndtering av innsynsbegjæringer:

Det nivå i kriminalomsorgen som har fått begjæringen, plikter å forelegge spørsmål om avgradering for graderende myndighet før det besluttes om innsynsbegjæringen skal innvilges. Der politiet er graderende myndighet skal foreleggelsen sendes via KSF. Politiet bør gradere alle dokumenter som inneholder særlig beskyttelsesverdig informasjon som utleveres til kriminalomsorgen.

VIII: Håndtering av gradert informasjon etter endt straffegjennomføring:

Informasjonen skal behandles etter kriminalomsorgens bevarings- og kassasjonsrundskriv. Dette innebærer at lokalt og regional nivå skal destruere informasjonen, mens KSF skal bevare denne for avlevering til Riksarkivet.

11 Forslag til lov og forskrift

Utvalgets mandat forutsetter at utvalget skal fremme forslag til hensiktsmessige regler for behandling av personopplysninger i INFOFLYT og at disse skal harmonere med tilsvarende regler for politiets informasjonsutveksling i politiregisterloven med forskrift og retningslinjer til loven.

Som nevnt i punkt 1.1 har arbeidet med forskriftene til politiregisterloven tatt lenger tid enn planlagt. Utvalgets forslag til forskrift baserer seg derfor på departementets høringsforslag.

Dersom høringsrunden medfører endringer i forskriftene til politiregisterloven som berører INFOFLYT, må dette reflekteres i den videre oppfølging av utvalgets forslag.

11.1 Utvalgets forslag til endringer i straffegjennomføringsloven

Nytt kapittel 1 b. Særlig om behandling av personopplysninger i INFOFLYT

§ 4f Formål med behandlingen av personopplysninger

Kriminalomsorgen kan behandle personopplysninger i INFOFLYT for å forebygge, forhindre og bekjempe alvorlig kriminalitet.

§ 4g Utlevering av personopplysninger til politiet og påtalemyndigheten

Kriminalomsorgen kan uten hinder av taushetsplikten etter § 7 første ledd bokstav h utlevere opplysninger til politiet og påtalemyndigheten til formål som nevnt i §§ 4c og 4f eller dersom det er nødvendig for at politiet skal kunne foreta en risikovurdering.

§ 4h Den registrertes rettigheter ved behandling av personopplysninger i INFOFLYT

Ved behandling av personopplysninger i INFOFLYT, kommer politiregisterloven kapittel 8, §§ 55 første ledd nr. 3 og 59 til anvendelse.

Politiregisterloven § 60 om Datatilsynets virkemidler kommer til anvendelse for opplysninger som politiet har utlevert til kriminalomsorgen.

11.2 Utvalgets forslag til forskrift

11.2.1 Innledende merknader

Rekkefølgen på temaene for bestemmelsene er gjort i stor grad etter mønster av politiregisterloven og politiregisterforskriftene.

Det er søkt å benytte like formuleringer og struktur som i politiregisterloven med forskrifter så langt det passer. I noen grad viser forskriften til bestemmelsene i politiregisterloven for å knytte forbindelsen til denne og gjøre det lettere å finne frem til det materielle innholdet i regelverket.

11.2.2 Utkast til forskrift

I utkastet til forskrift nedenfor reguleres:

- § 1 Formålet
- § 2 Nødvendighetskravet
- § 3 Krav til opplysningskvalitet
- § 4 Behandlingsansvaret
- § 5 Samarbeidet mellom kriminalomsorgen og politiet
- § 6 Fremgangsmåte ved registrering
- § 7 Utlevering av opplysninger til politiet
- § 8 Tilgang til opplysningene
- § 9 Innsyn
- § 10 Retting, sperring og sletting av opplysninger
- § 11 Saksbehandling i saker om innsyn, retting, sperring og sletting
- § 12 Bruk av opplysninger som er sperret
- § 13 Informasjonssikkerhet og internkontroll
- § 14 Klage
- § 15 Ikrafttredelse

Utvalget foreslår følgende forskriftsbestemmelser om INFOFLYT:

Forskrift om behandling av personopplysninger i INFOFLYT

§ 1 *Formålet med forskriften*

Formålet med forskriften er at kriminalomsorgen kan behandle beskyttelsesverdig informasjon for å ivareta sine oppgaver som nevnt i straffegjennomføringsloven §§ 4c og 4f, og samtidig ivareta personvernet til den registrerte.

§ 2 *Nødvendighetskravet*

Det kan behandles personopplysninger om innsatte, ansatte, pårørende og personer som har kontakt med eller prøver å få kontakt med den innsatte når behandlingen er nødvendig for å:

- a) forhindre rømning eller bistand til rømning,
- b) forhindre fysiske angrep på innsatte, ansatte, besøkende og andre som oppholder seg i enheten, eller
- c) bekjempe alvorlig kriminalitet.

Det kan også behandles personopplysninger om personer som gjennomfører straff utenfor fengsel for formål som nevnt i første ledd.

Behandling av personopplysninger i henhold til første og annet ledd kan bare skje dersom det foreligger objektive holdepunkter for å anta at vilkårene der er oppfylt.

§ 3 *Krav til opplysningenes kvalitet*

Personopplysninger som behandles, skal

- a) være tilstrekkelige og relevante for formålet med behandlingen
- b) være korrekte og oppdaterte, og

c) ikke lagres lenger enn nødvendig ut fra formålet med behandlingen.

Kravet om tilstrekkelighet innebærer at opplysningene må være fullstendige, det vil si utfyllende og detaljerte, og at man unngår at opplysningene gir et misvisende eller uriktig bilde av en person eller situasjon. Opplysningene er relevante når de har tilknytning til formålet og er nødvendige for behandlingen. Dersom formålet med behandlingen også kan oppnås ved å behandle færre eller mindre sensitive opplysninger, skal denne fremgangsmåten benyttes.

Opplysninger som ikke er verifiserte kan behandles dersom det er nødvendig ut fra formålet med behandlingen. Det skal fremgå at opplysningene ikke er verifiserte og de skal markeres med kildens pålitelighet og opplysningenes holdbarhet.

§ 4 *Behandlingsansvar*

Behandlingsansvaret for behandling av personopplysninger i henhold til denne forskriften ligger hos Kriminalomsorgens sentrale forvaltning (KSF).

Den behandlingsansvarlige har ansvaret for at behandling av personopplysninger skjer i samsvar med lov, forskrift og instruks, og at det utarbeides nærmere rutiner for å sikre at behandling av personopplysninger skjer i samsvar med gjeldende regelverk.

Den behandlingsansvarlige kan delegere det daglige behandlingsansvaret.

§ 5 *Samarbeid med politiet*

Departementet plikter å etablere rutiner som sikrer kontinuerlig samarbeid mellom den behandlingsansvarlige og politiet. Rutinene skal sikre at personopplysninger som utveksles, brukes i samsvar med pålegg gitt av politiet.

§ 6 *Fremgangsmåten ved registrering*

Avgjørelse om å behandle opplysninger tas av den behandlingsansvarlige. Beslutningen skal være skriftlig og begrunnet. Begrunnelsen skal angi hvilke holdepunkter avgjørelsen bygger på og hva som er formålet med behandlingen, jf. § 2 første ledd bokstav a – c.

Opplysningene skal i hovedsak registreres ved hjelp av standard opplysningskategorier som er felles for hele kriminalomsorgen.

§ 7 *Utlevering av opplysninger til politiet og påtalemyndigheten*

Den behandlingsansvarlige kan utlevere opplysninger til politiet når det er nødvendig for de formål som nevnt i § 2.

Opplysningene skal utleveres skriftlig. Utleveringen kan likevel skje muntlig dersom den behandlingsansvarlige antar at politiet trenger opplysningene så snart som mulig for å avverge lovbrudd. Det skal alltid nedtegnes hvilke opplysninger som utleveres, hvilket organ i politiet som mottar opplysningene og formålet med utleveringen.

§ 8 *Tilgang til opplysningene*

Tilgang til opplysninger som behandles i henhold til denne forskriften skal kun gis til ansatte i kriminalomsorgen som har tjenestemessig behov, og som har fått særskilt bemyndigelse.

Bemyndigelse skal bare gis til personer som har gjennomgått opplæring og som er sikkerhetsklarerte.

Bemyndigelse gis av den behandlingsansvarlige. Det skal ikke gis bemyndigelse til flere personer enn strengt nødvendig.

§ 9 *Nærmere om innsyn*

Innsyn i opplysninger i INFOFLYT reguleres av politiregisterloven § 49, jf. straffegjennomføringsloven § 4h.

Dersom opplysningene fremkommer i et gradert dokument, reguleres innsynsretten etter sikkerhetsloven eller beskyttelsesinstruksen.

Forvaltningsloven § 18 og 19 om partsinnsyn gjelder med de unntak som følger av straffegjennomføringsloven § 7 første ledd bokstav c

§ 10 *Retting, sperring og sletting av opplysninger*

Opplysninger skal rettes, sperres eller slettes etter politiregisterloven §§ 50 og 51, jf. straffegjennomføringsloven § 4h.

Opplysningene skal gjennomgås hvert år med sikte på å slette opplysninger som er ukorrekte, ufullstendige eller ikke lenger er oppdaterte eller nødvendige for formålet.

Avgjørelse om å opprettholde registreringen utover 3 år skal være skriftlig og begrunnet.

Dersom sletting vil kunne påvirke den registrertes legitime interesser, skal opplysningene sperres.

Utover dette kommer politiregisterforskriften kapittel 14, 15 og 16 til anvendelse så langt de passer.

§ 11 *Bruk av opplysninger som er sperret*

Opplysninger som er sperret kan bare brukes til de formål som gjorde at de ikke ble slettet, jf. politiregisterloven § 52 første punktum og straffegjennomføringsloven § 4h.

§ 12 *Saksbehandling i saker om innsyn, retting, sperring og sletting*

Begjæring om innsyn, retting, sperring og sletting skal leveres til den enhet der vedkommende gjennomfører straff eller varetekt.

Enheten undergir begjæringen forberedende behandling og sender den til den behandlingsansvarlige for avgjørelse. Gjelder begjæringen opplysninger som er mottatt av politiet, skal den oversendes politiet for uttalelse før det treffes vedtak.

Utover dette kommer politiregisterloven § 54 tredje ledd og politiregisterforskriften §§ 17-2 til 17-4 til anvendelse.

§ 13 *Informasjonssikkerhet og internkontroll*

Sikkerhetsloven, beskyttelsesinstruksen og bestemmelsene i personopplysningsloven §§ 13 og 14 med tilhørende forskrift, gjelder for personopplysninger som behandles etter denne forskriften. Bestemmelsene gjelder uavhengig av om behandlingen av personopplysninger skjer elektronisk eller manuelt.

§ 14 *Klage*

Den registrerte kan påklage avgjørelser om innsyn, retting, sperring og sletting, jf. politiregisterloven § 55 første ledd nr. 3. Klagen avgjøres av Justis- og beredskapsdepartementet.

Utover dette gjelder bestemmelsene i politiregisterforskriften kapittel 18 så langt de passer.

§ 15 *Ikrafttredelse*

Vedlegg 1:

Rundskriv G-3 2005 (det generelle samarbeidet om informasjonsutveksling)

Jnr.: 200506530 DUS OJH

Dato: 18.03.2005

Regiondirektørene i
kriminalomsorgen
Politidistriktene
Tingretter, Lagmannsretter,
Høyesterett
Påtalemyndighetens kontorer
Riksadvokaten
Liste D

Informasjonsutveksling mellom kriminalomsorgen og politiet/påtalemyndigheten

1. Formål og bakgrunn

Både kriminalomsorgen og politiet/påtalemyndigheten har som formål å forebygge kriminalitet og å trygge samfunnet, jfr straffegjennomføringsloven (strgjfl) § 2 og politiloven (politil) § 2. For å oppnå et best mulig resultat i sitt arbeid, er både kriminalomsorgen og politiet/påtalemyndigheten avhengig av gjensidig utveksling av opplysninger om både personer og andre forhold generelt. En slik utveksling må systematiseres og kvalitetssikres i størst mulig grad. Rundskrivet her angir tiltak og sentrale regler for å sikre et best mulig samarbeid.

2. Tiltak

Alle samarbeidende enheter på tilsvarende nivå innen kriminalomsorgen og politiet/påtalemyndigheten skal jevnlig utveksle informasjon om innsatte og dømte og personkretsen rundt disse, og om andre momenter av betydning for å forebygge kriminalitet og trygge samfunnet. Generell orientering om hverandres etater, organisering og systemer skal også gis. Det skal også tilstrebtes samarbeid om kompetanseutvikling.

Tiltakene skal gi kriminalomsorgen et bedre grunnlag for sin sikkerhetsvurdering av varetektsfengslede og dømte. Politiet/påtalemyndigheten skal få et bedre grunnlag for sin etterforskning og oppfølging. Utveksling av nødvendig og korrekt informasjon vil også forbedre de respektive etaters forebyggende arbeid.

3. Rutiner for informasjonsutveksling

Forvaltningsloven (fvl) § 13 b første ledd nr. 5 angir at opplysningene skal gis av forvaltningsorganet som sådan. Avgjørelsen ligger til organets leder- eller den han/hun har delegert avgjørelsen til. Tilsvarende gjelder for strpl § 61 c første ledd nr. 6.

For utveksling av informasjon om særlig alvorlige saker og med særlig høy risiko, skal INFOFLYT-systemet benyttes. For behandling av disse sakene vises det til særskilte, interne, saksbehandlingsinstruksjoner utarbeidet av Kriminalomsorgens sentrale forvaltning (KSF), Riksadvokaten, Politidirektoratet (POD) og Politiets sikkerhetstjeneste (PST).

4. Særlig om taushetsplikt og unntak fra denne

Av straffeloven § 139 og § 172 fremgår at kriminalomsorgen har plikt til å orientere politiet om/anmelde visse forhold. Av påtaleinstruksen § 5-3 fremgår at politiet skal orientere kriminalomsorgen om iverksatt etterforskning mot dømte. Videre skal kriminalomsorgen alltid orienteres hvis det fremstår som sannsynlig at domfelte under straffegjennomføring vil foreta eller delta i straffbar handling i nær fremtid.

For øvrig er utgangspunktet at både kriminalomsorgen, politiet og påtalemyndigheten har taushetsplikt om de fleste forhold. Informasjonsutveksling må hjemles i ulike unntaksregler.

1) Kriminalomsorgens avgivelse av opplysninger til politiet/påtalemyndigheten

Ved behov er unntakene fra taushetsplikten svært omfattende. I praksis settes det svært få skranker for kriminalomsorgens avgivelse av opplysninger.

a) Generelle unntak fra taushetsplikten

Fvl § 13 b, første ledd nr 5 gir unntak fra taushetsplikten for å gi "andre forvaltningsorganer opplysninger om en persons forbindelse med organet og om avgjørelser som er truffet og ellers slike opplysninger som er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningssgrunnlag". Avgiverorganets oppgaver etter strgfj § 2 er bl.a. å motvirke nye straffbare handlinger og trygge samfunnet. Dette innebærer f.eks. at kriminalomsorgen kan gi politiet/påtalemyndigheten opplysninger om hvilket fengsel og regime den innsatte/domfelte er underlagt, hvilke andre innsatte som er på samme avdeling, hvem som har kontakt med hverandre og lignende observasjoner. Videre kan det f.eks. gis opplysning om og hvorfor den innsatte/dømte er underlagt særskilte kontrolltiltak, om denne er forflyttet, ilagt reaksjoner på brudd (tidligere også kalt "refselser"), permisjoner, hvem som er gitt besøkstillatelser og når.

Opplysninger trenger ikke være knyttet til en konkret sak. Dette kan være f.eks. opplysninger om hvem som korresponderer og telefonerer med innsatte, og hva som sies (jfr f.eks. reglene om brev-, besøks- og telefonkontroll i fengsler). Opplysninger som fengselsbetjenter får i egenskap av å være medhjelper for helsepersonell (ved f.eks. medisinnutdeling), er imidlertid taushetsbelagte etter lov om helsepersonell.

b) Unntak fra taushetsplikten ved lovbrudd, anmeldelser og lignende

Fvl § 13 b, første ledd nr 6 hjemler unntak fra taushetsplikten når opplysningene gjelder lovbrudd, eller i forbindelse med en anmeldelse. Dette kan f.eks. være opplysninger fremkommet under brev-, telefon- og besøkskontroll, fra informanter eller observasjoner fra kriminalomsorgen forøvrig. Unntaket begrenser seg ikke bare til straffesanksjonerte lovbrudd. Det aktuelle forhold må ikke være bevist, mistanke er tilstrekkelig.

c) Unntak fra innsynsrett og krav til begrunnelse av vedtak

Etter strgfj § 7 bokstav c har en part (dvs en innsatt/dømt) ikke krav på innsyn i dokument som det anses utilrådelig at parten får kjennskap til av hensyn til en annen person, av sikkerhetsmessige hensyn eller av hensyn til etterforskning av straffbare forhold. I denne sammenheng likestilles partens advokat

med parten selv. Etter § 7 bokstav d kan det gjøres unntak fra begrunnelsesplikten ved vedtak dersom begrunnelse vil røpe opplysning som er unntatt fra adgangen til innsyn etter bokstav c.

2) *Politiets/påtalemyndighetens avgivelse av opplysninger til kriminalomsorgen*

Unntakene fra taushetsplikten er i praksis svært omfattende. Det må imidlertid skilles mellom opplysninger som er taushetsbelagt etter de alminnelige regler i politil § 24, jf. fvl §§ 13 flg. og straffeprosessloven (strpl) §§ 61 a flg, og registeropplysninger hvor taushetsplikten reguleres av strafferegistreringsloven § 8, og kommunikasjonskontrollopplysninger som reguleres av bestemmelsen i strpl § 216 i.

a) Kommunikasjon for å realisere formålet

For ordinær informasjon – dvs. alle andre opplysninger enn de politiet henter ut fra registre eller som er innhentet ved kommunikasjonskontroll – er ikke taushetsplikten "til hinder for at opplysningen brukes for å oppnå det formål de er gitt eller innhentet for, bl.a. kan de brukes i forbindelse med etterforskning, saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølging og kontroll", jfr strpl § 61 c første ledd nr. 2 og politil § 24, jf. fvl § 13 b første ledd nr. 2. Formålet er å sikre at innhentede opplysninger kan brukes slik det fremstår som nødvendig i den videre behandling av saken. Etter strpl § 226 første ledd er et av formålene med etterforskningen å fremskaffe opplysninger for fastsetting og fullbyrding av strafferettslige reaksjoner. Formidling av informasjon fra etterforskningen m.v. til kriminalomsorgen vil være å bruke informasjonen til dette formålet. Etter strpl. § 61 c første ledd nr. 2 er det derfor adgang til å gi kriminalomsorgen all informasjon (med unntak av KK-opplysninger) som er innhentet i anledning saken, og som kan antas å være av betydning for gjennomføringen av den fastsatte reaksjon.

b) Kommunikasjon til kriminalomsorgen for å fremme politiets oppgaver

Politiopplysninger som ikke er knyttet til saken som ledet fram til varetektsfengsling/dom kan også være av betydning for kriminalomsorgens avgjørelser. Dette kan f. eks være informasjon fremkommet under mer generell etterretningsvirksomhet eller i tilknytning til etterforskningen av andre straffesaker. Iflg strpl § 61 c første ledd nr. 6 og politil § 24, jf. fvl § 13 b første ledd nr. 5 er ikke taushetsplikten "til hinder for at det til andre offentlige organer blir gitt opplysninger om en persons forbindelse med politiet og om avgjørelser som er truffet og ellers slike opplysninger som det er nødvendig å gi for å fremme politiets oppgaver". Politiets viktigste oppgave er å forebygge og bekjempe kriminalitet, og å bidra til den alminnelig trygghet i samfunnet, jfr politil § 2. Hvis politiet gjennom å gi kriminalomsorgen opplysninger kan bidra til at innsatte/dømte ikke får adgang å fortsette sin kriminelle virksomhet under straffegjennomføringen, eller at domfelte hindres fra å unndra seg denne (f.eks. ved rømning eller uteblivelse), bidrar kommunikasjonen også til å "fremme politiets oppgaver".

Bestemmelsene inneholder et "nødvendighetskrav", men hvis politiet først sitter med opplysninger som antas å være av betydning for hvilket regime en varetektsfengslet/domfelt bør undergis, vil dette kravet normalt være oppfylt.

c) Registeropplysninger

Registeropplysninger er informasjon som hentes ut fra de registre som reguleres av strafferegistreringsloven. Hovedtrekkene i taushetspliktsreguleringen i denne loven og forskriften av 1974 vil også gjelde for de registre som i denne sammenheng vil være aktuelle.

For strafferegisteret inneholder loven og forskriften en generell bestemmelse om at kriminalomsorgen (fengslene og friomsorgskontorene og deres overordnede nivåer) kan gis tilgang til opplysninger.

I henhold til strafferegisterforskriften § 11 i.f. kan opplysninger fra politiregistrene også meddeles kriminalomsorgen.

d) Kommunikasjonskontrollopplysninger

Opplysninger fremkommet ved kommunikasjonskontroll reguleres av strpl § 216 i. Bestemmelsen etablerer en forholdsvis streng og omfattende taushetsplikt. Taushetsplikten er imidlertid ikke til hinder for at opplysningene bl.a. kan brukes for å avverge en straffbar handling som kan medføre frihetsstraff, f. eks rømning, voldsanvendelse i fengsel eller under permisjon/frigang, jf. § 216 i første ledd bokstav d.

Med hilsen

Kristin Bølgen Bronebakk
ekspedisjonssjef

Karen Alette Melander
ekspedisjonssjef

Vedlegg 2: Saksbehandlingsinstruks INFOFLYT, KSF 2/ 2005

Rundskriv KSF 2/2005

Jnr.: 200502697 D OJH/mha

Dato: 13.04.2005

Regiondirektørene
Direktøren for KRUS
Direktøren for KITT
Fengselslederne
Friomsorgslederne

INFOFLYT - Særskilt saksbehandlingsinstruks

1. Bakgrunn, formål og hjemmelsgrunnlag

INFOFLYT omfatter informasjonsutveksling om særlig alvorlige saker og med særlig høy risiko.

Riktige sikkerhetsmessige vurderinger i kriminalomsorgen er avhengige av et så godt informasjonsgrunnlag som mulig. Dette gjelder både de løpende sikkerhetsvurderinger på den enkelte enhet, men også ved nyinnsettelse og overføringer, samt i trusselsaker. Slik informasjon har til tider vært av varierende kvalitet. Det er derfor nødvendig med en sentral kvalitetssikring av slik informasjon og et formalisert operativt system som kan behandle den. Pga opplysningenes meget sensitive art, må systemet sikre minst mulig spredning av disse.

For å bedre informasjonsflyten mellom politiet og kriminalomsorgen om innsatte og dømte, deres tilhørighet til risikogrupperne og opplysninger om rømningsfare eller fare for anslag utenfra mm, har Kriminalomsorgens sentrale forvaltning (KSF) og Politidirektoratet (POD) og Politiets sikkerhetstjeneste (PST) utarbeidet en samarbeidsmodell for informasjonsflyt mellom politi og kriminalomsorg, kalt INFOFLYT.

Politi omfatter i denne sammenheng også påtalemyndigheten.

Retningslinjene her er gitt med hjemmel i straffegjennomføringsloven (strgjfl) §§ 10 og 11, forskriften § 7-1, justisdepartementets rundskriv G-3/2005 og øvrige bestemmelser i loven, forskriften og retningslinjene som innebærer sikkerhetsmessige vurderinger.

2. INFOFLYT er informasjonsutveksling på sentralt nivå

Informasjonsutvekslingen mellom politiet og kriminalomsorgen skal i INFOFLYT-sakene foregå mellom KSF og Nye Kripas, evt mellom KSF og PST. KSF skal ha et sentralt register over hvem som omfattes av INFOFLYT, med relevante opplysninger om disse. Personer registrert i INFOFLYT-registeret vil også være særskilt markert i KOMPIS.

Det sentrale INFOFLYT-samarbeidet mellom Nye Kripas/PST og KSF er ikke ment å tre istedenfor det

eksisterende og nødvendige samarbeid mellom kriminalomsorgens lokale enheter og lokalt politi, men vil være en kvalitetssikring av informasjon om visse innsatte, dømte og personkretsen rundt disse, og av informasjon om visse sakskomplekser av en viss alvorlighetsgrad, i tillegg til å gi ny informasjon om disse.

3. Målgruppe/personkrets som omfattes av INFOFLYT

Målgruppen er personer som etter en konkret vurdering av de ulike faktorer utgjør en særlig risiko for orden og sikkerhet i fengselet, for tjenestemennene der og for samfunnet for øvrig.

Dette er i hovedsak:

- innsatte (både på dom og varetekt), som antas å medføre
 - særlig rømningsfare, eller
 - fare for anslag utenfra for å bistå til rømning, eller
 - gisseltaking, eller
 - fare for ny særlig alvorlig kriminalitet
 - spesielle beskyttelsesbehov, f.eks. i forbindelse med vitnebeskyttelse *og som kan ha tilhørighet til*
 - organiserte kriminelle nettverk, eller
 - terrorister, eller
 - politiske ekstreme nettverk, eller
 - religiøse ekstreme nettverk

Videre kan det tas hensyn til

- type lovbrudd
- domslengde
- tidligere adferd i fengsel, som f.eks. nye alvorlige straffbare forhold

Denne gruppen vil i hovedsak sammenfalle med innsatte som kan være aktuelle å vurdere for innsettelse i "avdeling med særlig høyt sikkerhetsnivå" (strgjfl § 11, 2. ledd), i tillegg til innsatte som allerede sitter i slike avdelinger. INFOFLYT omfatter dermed også innsatte som ikke nødvendigvis skal innsettes på avdeling med særlig høyt sikkerhetsnivå, men som av andre årsaker ligger i "gråsonen" for denne kategorien, og som det vil være viktig å ha ekstra god kontroll på. Disse kan sitte på vanlig lukket avdeling, men kan om nødvendig få særskilte kontrollregimer- og oppfølging (innen rammen av regelverket).

Gruppen vil også omfatte innsatte tilknyttet særskilte kriminelle nettverk hvor de enkeltvis ikke anses som særlig risiko, men hvor to eller flere tilknyttet samme nettverk i samme fengsel kan anses som en risiko, f.eks. ransmiljøer, mc-kriminelle, visse torpedo/voldsmiljøer, særskilte narkotikaligaer, satanister og aktive gjengmedlemmer.

I tillegg omfattes

- den personkrets som er knyttet til disse innsatte, som f.eks.
 - besøkende,
 - telefoniske kontakter og
 - mottakere/avsendere av korrespondanse og annen kommunikasjon til og fra disse innsatte
- personkrets som ikke er innsatte, men som antas å ha tilhørighet til
 - organiserte kriminelle nettverk, eller
 - terrorister, eller
 - politiske ekstreme nettverk, eller
 - religiøse ekstreme nettverk

og som vil kommunisere eller kommuniserer med innsatte (i form av besøk, telefon eller annen korrespondanse), *også selv om* de innsatte i utgangspunktet ikke omfattes av målgruppen

En rekke personer (innsatte og andre) er tilknyttet særskilte kriminelle nettverk, og det bør derfor stilles bestemte krav til nettverket når det er spørsmål om dette. Et nettverk må ha formål utover "kameratskap". Det bør være en del av dagens trusselbilde og være en reell sikkerhetsrisiko når flere fra nettverket er samlet. Siden personkretsen også vil omfatte besøkende o.a. som har kontakt med den innsatte, begrenses ikke aktuell personkrets til bare å gjelde de tilfeller hvor flere innsatte av samme kategori sitter i samme fengsel.

4. Type opplysninger som skal omfattes av INFOFLYT

INFOFLYT skal være et system for behandling av:

- Opplysninger kriminalomsorgen trenger for å beslutte riktige sikkerhetsmessige tiltak. Dette kan være opplysninger om særskilte innsatte og særskilt personkrets fremkommet under politiets etterforskning eller etterretning og som politiet anser sensitive i forbindelse med fortsatt etterforskning eller etterretning, men som likevel kan gis kriminalomsorgen.
- Opplysninger politi og påtalemyndighet trenger for å bekjempe og forebygge kriminalitet. Dette er bl.a. opplysninger om forhold av sikkerhetsmessig art rundt soningssituasjonen til særskilte innsatte/dømte. Informasjon fra KSF til Nye Kripos evt PST vil basere seg på bearbejdede opplysninger hentet fra INFOFLYT-registeret, KOMPIS, innsatte informanter, brev-, telefon- og besøkskontroll samt andre egne observasjoner. Dette kan f. eks være opplysninger om regimet den innsatte er underlagt og årsak til dette, hvilke andre innsatte som sitter på samme avdeling, forflytninger, reaksjoner på brudd, permisjoner, hvem som er gitt besøkstillatelser og når, hvem innsatte korresponderer med og hva som sies, jf også pkt 7 om taushetsplikt.
- KSF vurderer om opplysningene ut fra sin art og alvorlighetsgrad skal registreres i infoflyt-registeret.

5. Forespørsel om og utveksling av informasjon

Forespørsel om informasjon og oversendelse av informasjon skal skje tjenestevei, dvs fra lokalt nivå til regionalt nivå til KSF og motsatt. Jf også pkt 6 om autorisering.

Utveksling av informasjon skjer mellom KSF og Nye Kripos, evt mellom KSF og PST, ved:

- Anmodning fra KSF til Nye Kripos eller PST om opplysninger for å vurdere om en innsatt eller annen person omfattes av målgruppen for INFOFLYT. Nye Kripos/PST har ansvaret for at detaljeringsnivået ved bruken av etterretningsopplysninger, såkalt "softinfo", blir vurdert i.f.m. utarbeidelse av svar til KSF. Når ikke verifiserte opplysninger utleveres, bør det gjøres oppmerksom på at deres korrekthet ikke er avklart. KSF viderefremidler informasjonen tjenestevei.
- Meldinger politiet av eget tiltak sender via Nye Kripos eller PST for evt vurdering i KSF, og som inneholder opplysninger politiet mener kan ha betydning for vurderinger innen INFOFLYT-systemet.

Opplysninger fra politiet til kriminalomsorgen om akutte problemer som opprør, overlevering av narkotika og lignende, som er av en viss alvorlighetsgrad, og hvor bruk av INFOFLYT-systemet vil medføre unødig forsinkelse, kan meldes direkte fra politiet til vedkommende lokale enhet. Kopi av meldingen sendes henholdsvis Nye Kripos eller PST og KSF. Her må det tas hensyn til tidsfaktor og om det er hensiktsmessig å benytte samme fremgangsmåte som beskrevet over.

- anmodning fra Nye Kripos eller PST til KSF om opplysninger om innsatte og dømte eller personkrets rundt disse.

6. Saksbehandling, registre og tilgangsnivå

Informasjon fra Nye Kripos/PST til KSF gis i bearbeidet form. Etter samråd med Nye Kripos/PST om videre avskalling av detaljopplysninger, gir KSF informasjon videre til region (evt i bearbeidet form), og den går deretter videre til fengselet (eventuelt ytterligere bearbeidet om dette fra politiets side anses nødvendig). Opplysninger som innebærer sikkerhetsrisiko rundt innsatte skal gis i sin helhet.

Saksbehandlingen skal være skriftlig, og skje iht. Beskyttelsesinstruksen. Informasjonen vil som hovedregel omfatte opplysninger som vil kunne skade offentlige interesser eller enkeltpersoner, også i betydelig grad. Dermed skal som hovedregel alle dokumenter i INFOFLYT som behandles i kriminalomsorgen graderes FORTROLIG eller STRENGT FORTROLIG (etter behov), og behandles, forsendes og oppbevares iht. Beskyttelsesinstruksen. Informasjonen oppbevares utilgjengelig for uvedkommende/andre enn de autoriserte og forsvarlig sikret i eget låst skap, atskilt fra fangesakene. Fangesakene merkes særskilt for å vise at det foreligger andre opplysninger om den innsatte. Det er naturlig at regionalt og lokalt nivå oppretter egne "INFOFLYT-mapper" om de enkelte innsatte. Dersom regionalt eller lokalt nivå utformer nye dokumenter i INFOFLYT-saken, eller mottar dette fra andre enn KSF/egen region (f. eks politi) skal det sendes kopi til henholdsvis regionalt nivå og KSF.

Ved oppretting av nye saker eller ved overføring, må de enkelte nivåer og enheter konferere muntlig på forhånd, slik at saken er kjent når saken og/eller innsatte ankommer.

Ved overføring mellom fengsler, skal den innsattes "INFOFLYT-mappe" iht. Beskyttelsesinstruksen følge den innsatte til nytt fengsel. Dersom mottakende fengsel ligger i en annen region, skal dokumenter i avgivende region sendes mottakende region. I KSF vil opplysningene lagres og bearbeides i eget register, INFOFLYT-registeret.

Alle nivå skal føre egen journal for dokumenter omfattet av INFOFLYT iht. Beskyttelsesinstruksen. Journalen skal være unntatt offentlighet. All bruk av dokumentene skal føres i egen logg, hvor det fremgår hvilke dokumenter som er brukt, hvem som har brukt dem og når.

Behandling etter Beskyttelsesinstruksen ivaretar behovet for tilgang til informasjon etter "need to know"-prinsippet. I KSF vil 3-4 personer være involvert, på regionsnivå 3-4 personer, og på lokalt nivå 2-4 personer (avhengig av enhetens størrelse). Det er behov for mer enn 1 person pr. nivå pga. fraværspromatikk. Disse vil være personlig autorisert. Regionene autoriserer personene på regionalt og lokalt nivå, og skal til enhver tid ha liste over autoriserte personer, hvor det også må fremgå i hvilken rekkefølge disse skal kontaktes. Også merkantilt personale (forværelse, arkiv o.l.) som skal håndterer dokumenter må autoriseres og fremgå av nevnte liste. Disse inngår ikke i gruppen på 2-4 personer nevnt over, men antallet må reduseres til et minimum. KSF skal fortløpende orienteres med kopi av nye eller endrete lister. Antallet autoriserte personer per nivå kan økes etter avtale mellom KSF og politiet. På regionalt nivå bør autoriserte personer ha beslutningsmyndighet i fangesaker.

På bakgrunn av opplysningene fra KSF vil regionene og fengslene beslutte nødvendige tiltak mot de aktuelle personene. Dette kan f.eks. være innsettelse på avdeling med særlig høyt sikkerhetsnivå, evt overføring til andre avdelinger eller lukkede fengsler, evt besøksnektelser eller skjerpet besøks-, brev- eller telefonkontroll, innsetting på enerom (f.eks. ved s.k. "selvisolering"), evt forflytting av andre innsatte for å skjerme en eller flere innsatte.

Når innsatte registreres av KSF i INFOFLYT, skjer en merking på innsattes personbilde i KOMPIS KIA, for å gjøre KOMPIS-bruker oppmerksom på at overordnet må kontaktes før ny beslutning tas. Beslutning tatt av fengsel eller region kan om nødvendig omgjøres av overordnet nivå, også til skade for innsatte, jf

straffegjennomføringsloven § 7 g). Det er for øvrig også alminnelig instruksjonsadgang for overordnet nivå.

Beslutning tatt på bakgrunn av politiinformasjon meldes tjenestevei tilbake til KSF, for videreformidling til Nye Kripes/PST.

7. Taushetsplikt

Taushetsplikten setter i praksis svært få skranker for kriminalomsorgens avgivelse av opplysninger til politiet, også i disse sakene. Opplysninger fengselsbetjenter får i egenskap av helsepersonells medhjelper (ved for eksempel medisindeling), er imidlertid taushetsbelagte etter lov om helsepersonell. Mest mulig åpen informasjon til politiet skal tilstrebes.

Utgangspunktet er at taushetsplikt også gjelder for opplysninger innenfor INFOFLYT. Informasjon til politiet forutsetter dermed at opplysningene faller innenfor et av unntakene fra taushetsplikten. De mest aktuelle unntakshjemlene er forvaltningsloven (fvl) § 13 b, 1.ledd nr 5 og nr 6:

- Fvl §13 b, 1. ledd nr 5 gir unntak for å gi "andre forvaltningsorganer" (dvs politiet) "opplysninger om en persons forbindelse med organet" (f.eks. hvilket fengsel og regime den innsatte er underlagt, hvilke andre innsatte som sitter på samme avdeling og lignende), om "avgjørelser som er truffet" (f.eks. om og hvorfor den innsatte er underlagt særskilte kontrolltiltak, om denne er forflyttet, ilagt reaksjon på brudd, permisjoner, hvem som er gitt besøkstillatelser og når), og "ellers slike opplysninger som er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningss grunnlag".

Avgiverorganets (dvs KSFs) oppgaver etter strgfvl § 2 er å ivareta at "Straffen skal gjennomføres på en måte som tar hensyn til formålet med straffen, som motvirker nye straffbare handlinger, som er betryggende for samfunnet..." Dette kan f. eks være å hindre rømning eller annen ny kriminalitet.

Opplysninger trenger ikke være knyttet til en konkret fangesak eller etterforsknings sak. Dette kan være f.eks. opplysninger om hvem som korresponderer og telefonerer og for øvrig er i kontakt med innsatte, og hva som sies (jfr hovedregel om stadig tilsyn, brev-, besøks- og telefonkontroll i lukkede fengsler).

- Fvl § 13 b, 1. ledd nr 6 hjemler unntak fra taushetsplikten når opplysningene gjelder lovbrudd, eller i forbindelse med en anmeldelse. Dette kan f.eks. være opplysninger fremkommet under brev-, telefon- og besøkskontroll, fra informanter eller observasjoner fra fengselet for øvrig. Unntaket begrenser seg ikke bare til straffesaksjonnerte lovbrudd. Det antas at det aktuelle forhold ikke må være bevist, men at mistanke er nok.

8. Innsynsrett i INFOFLYT-dokumentene kriminalomsorgen behandler (som forvaltnings sak)

Selv om taushetsplikten oppsetter få skranker for kriminalomsorgens ansatte mot å gi opplysninger, oppstår spørsmålet om innsattes og andres innsynsrett i dokumentene som ligger til grunn for vedtakene. Pga. opplysningenes sensitive karakter og dermed risiko ved spredning, er det naturlig å ha som utgangspunkt at det ikke må gis innsyn i disse spesielle opplysningene. Innsynsrettsspørsmålet oppstår både iht.:

- a. presse/øvrige offentlighet,
- b. innsatte selv og dennes tilknyttede personkrets, og
- c. prosessfullmektig (advokat/forsvarer) for den innsatte/dennes tilknyttede personkrets

a) innsynsrett for presse/øvrige offentlighet: Denne kan f.eks. avskjæres etter offvl §5a jfr fvl § 13 (personlige forhold), offvl § 6 (særlig 1.ledd nr 2)c) (offentlige kontrolltiltak), 5) (anmeldelse/dokument om lovovertrødelse) og 8) (personbilder i personregister). Presse vil dermed kunne nektes innsyn, og

likeledes de fleste organisasjoner/institusjoner. Sivilombudsmannen vil kunne kreve innsyn, jfr sivilombudsmannsloven § 7. Denne har imidlertid taushetsplikt.

b) innsynsrett for innsatte selv og dennes personkrets: Strgjfl § 7 c) avskjærer partens innsynsrett i "dokument som inneholder opplysninger som det av hensyn til en annen person må anses utilrådelig at parten får kjennskap til. Parten har heller ikke krav på å gjøre seg kjent med opplysninger i et dokument dersom innsyn er utilrådelig på grunn av sikkerhetsmessige hensyn, eller av hensyn til etterforskning av straffbare forhold". Denne hjemmelen vil i praksis kunne avskjære innsyn i de sakene som omfattes av INFOFLYT for innsatte og andre personer som måtte være omtalt i opplysningene (f.eks. besøkende, brev- og telefonpartnere).

c) innsynsrett for prosessfullmektig (advokat/forsvarer) for den innsatte/dennes tilknyttede personkrets:

1) Prosessfullmektig skal etter norsk rett likestilles med part dersom ikke annet er bestemt.

Prosessfullmektig har altså ikke en videre innsynsrett enn sin klient. Dermed er også prosessfullmektigens innsyn avskåret pga. sikkerhetsmessige hensyn, eller av hensyn til etterforskning av straffbare forhold etter strgjfl § 7 c).

2) Fvl § 19, 1.ledd c) gjør unntak fra innsynsretten for opplysninger om en parts helse eller hans forhold til personer som står ham nær, når det anses utilrådelig å gjøre opplysningene kjent for parten, og det er "særlige grunner" som taler mot å gi opplysningene til prosessfullmektigen. Også denne hjemmel kan brukes, men går ikke like langt som strgjfl § 7.

9. Innsynsrett i opplysninger gjennom domstolsbehandling

Selv om innsyn i politiopplysningene som brukes for å begrunne vedtaket kan nektes i selve forvaltningssaken (vedtaket om innsettelse, flytting, besøksnekt eller andre særskilte kontrolltiltak), kan parten gå til sivil sak for å få vedtaket prøvd for domstolen. Spørsmålet blir da om saksøker kan kreve at opplysningene legges frem som en del av bevisføringen, enten i form av dokumentet selv eller som vitneforklaring. Dette kan løses ved bruk av tvistemålsloven (tvml) § 250, eller ved forvaltningsmessig omgjøring av vedtaket.

Tvml § 250, 1. ledd: "Er ellers et skriftlig bevis i en parts besiddelse, kan det kræves fremlagt, naar det ikke indeholder noget, som parten efter reglerne om vidnesbyrd vilde være utelukket fra eller fritat for at gi forklaring om."

Spørsmålet er da om saksøkt part er utelukket eller fritatt fra å gi forklaring om disse opplysningene. Dette reguleres i tvml § 204 (strpl §§ 117 og 118 er parallelle bestemmelser). Etter § 204 nr 1 kan opplysninger om rikets sikkerhet ikke tas imot av retten uten Kongens tillatelse. Etter nr 2 kan ikke taushetsbelagte opplysninger (som det vil dreie seg om her) fremlegges uten samtykke av departementet (her: Justisdepartementet). Samtykke kan bare nektes dersom fremleggelse av opplysningene "vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold". Vilkåret for å nekte samtykke vil lett være oppfylt for de aktuelle opplysningene.

Tvml § 204, nr 2 annet ledd åpner imidlertid for at retten (etter en helhetsvurdering) ved kjennelse kan kreve opplysningene fremlagt selv om samtykke er nektet fra departementet. Departementet skal da kunne redegjøre for sitt standpunkt, uten at denne redegjørelsen meddeles motparten. En slik

redegjørelse kan overbevise retten, og kravet om fremleggelse av opplysninger avskjæres. Men det kan også være at retten, på tross av redegjørelsen, ved kjennelse beslutter at opplysningene må fremlegges. I dette tilfellet kan kjennelsen påkjæres til lagmannsretten og videre evt til Høyesteretts kjæremålsutvalg for ny prøving. Det kan antas at slik prøving kan ta noe tid.

10. Lagring og makulering av informasjon

Oppbevaring og makulering av dokumenter med informasjon omfattet av INFOFLYT-systemet skal skje i henhold til Beskyttelsesinstruksen.

- a. I fengslene/på lokalt nivå og på regionalt nivå skal dokumentene makuleres ved løslatelse.
- b. I KSFs INFOFLYT-register skal informasjon slettes/makuleres etter 10 år dersom ikke KSF bestemmer noe annet.
- c. Nye Kripos skal føre en oversikt over sakene som omfattes av INFOFLYT. Tilsvarende oversikt skal føres i PST i saker som omfattes av disses ansvarsområde.

11. Iverksettelse

Denne instruks trer i kraft straks.

Med hilsen

Kristin Bølgen Bronebakk

Ekspedisjonssjef

Andreas Skulberg

avdelingsdirektør

Vedlegg 3: Dokumentliste

1. Konvensjoner

- Personvernkonvensjonen 28.01.81 nr. 108
- EMK 4.11.50, art. 6, 8, 13
- Personverndirektivet 95/46 EF 24.10.95
- SP - FN-konvensjonen om sosiale og politiske rettigheter 16. desember 1966

2. Lover

- Forvaltningsloven 10.2.1967
- Menneskerettsloven 21.5.1999 nr. 30
- Offentleglova 19.5.06 nr. 16 §§ 11, 13
- Personopplysningsloven 14.4.2000 nr. 31,
- Politiloven 4.8.1995 nr. 53
- Politiregisterloven 28.5.2010 nr. 16
- Sikkerhetsloven 20.03.1998 nr. 10
- Straffeloven 22.5.1902 nr. 10
- Straffegjennomføringsloven 18.5.2001 nr. 21
- Straffeprosessloven 22.5.1981 nr. 25
- Strafferegistreringsloven 11.6.1971 nr. 52
- Tvisteloven 17.6.2005 nr. 90

3. Forskrifter

- Personopplysningsforskriften 15.12.2000 nr. 1265
- Straffegjennomføringsforskriften 22.2.2002 nr. 183
- Strafferegisterforskriften 20.12.1974 nr. 4
- Utkast til politiregisterforskrift

4. Rundskriv og instruks

- Påtaleinstruks 28.6.85 nr. 1679, kapittel 3 og § 5-3
- Rundskriv G-3/2005 (Det generelle samarbeidet om informasjonsutveksling)
- Saksbehandlingsinstruks for INFOFLYT - KSF 2/2005
- Rundskriv POD 2005/00319 – INFOFLYT
- Rundskriv G-111/2000 JD: Journalføring- registrering KOMPIS KIA
- Retningslinjer til straffegjennomføring 06. 08.2002
- Beskyttelsesinstruks 17.3.1972 nr. 3352
- Instruks for sambandsmann i INFOFLYT

5. Utredninger, rapporter, oppgaver

- NOU 2003:21: "Kriminalitetsbekjempelse og personvern."
- NOU 2009:15: "Skjult informasjon – åpen kontroll."
- Stortingsmelding nr. 37 (2007-2008): "Straff som virker. Mindre kriminalitet tryggere samfunn"

- Riksrevisjonens rapport 3:10 (2009-2010) *Riksrevisjonens undersøkelse av politiets innsats mot organisert kriminalitet*
- Masteroppgave INFOFLYT- 2010 av Heidi Hansen, Juridisk fakultet, Oslo
- FNs arbeidsgruppe for vilkårlig fengsling sin rapport til Norge 11. oktober 2007
- Policy for informasjonssikkerhet. "Elektronisk samhandling i justissektoren"

6. **Brev/notater**

- Sivilombudsmannen 2007/264, 2007/2274 – brev 5.6.09, 2006/1502
- KSFs svar til Sivilombudsmannen 21.9.2009 (ref. nr. 200904096)
- Datatilsynets pålegg etter tilsyn. Brev 25.1 2008 med kontrollrapport
- Datatilsynets brev til KSF 9.11.05 om vurdering av utvidet registrering i KOMPIS, som svar på KSFs brev 24.6.05, jf. Datatilsynets brev til KSF 16.2. 2004
- Notat fra KSF 11.6.2004 om utvikling av INFOFLYT
- Brev 29. juli 2004 fra KSF til regionene om tiltaksplan for straffegjennomføring for innsatte med tilhørighet til organisert kriminalitet.

Utgitt av:
Justis- og beredskapsdepartementet

Trykk:
Departementenes servicesenter 05/2012 - 150

