JUSTITSMINISTERIET

Vejledning om udveksling af personoplysninger som led i indsatsen mod radikalisering og ekstremisme

Med særligt fokus på infohusene

August 2020

Indhold

1. Indledning 2

2. De retlige rammer 3

3. Overblik: Sagsforløbet i infohuset 5
   - 3.1 Opstart 5
   - 3.2 Inden mødet i infohus kommune 5
   - 3.3 Møde i infohus kommune 6
   - 3.4 Efter møde i infohus kommune 6

4. Udveksling af personoplysninger i infohusene 7
   - 4.1 Generelle overvejelser, som deltagerne i infohuset skal gøre sig 7
   - 4.2 Hvilke kategorier af oplysninger kan videregives? 8
   - 4.3 Hvilke samarbejdsformer er omfattet af retsplejelovens § 115? 9
   - 4.4 Hvilke myndigheder og institutioner er omfattet af retsplejelovens § 115? 11
   - 4.5 Hvordan behandles opfølgning på indsatser og nye bekymringshenvendelser? 13
   - 4.6 Kan oplysninger benyttes i efterforskning? 14
   - 4.7 Er der en pligt til at videregive oplysninger efter retsplejelovens § 115? 14
   - 4.8 Registrering og journalisering af oplysninger 15
     - 4.8.1 Notatpligt 15
     - 4.8.2 Journaliseringspligt 16
   - 4.9 Oplysningspligt og partshøring 16
     - 4.9.1 Oplysningspligten 16
     - 4.9.2 Partshøring 19
     - 4.9.3 Øvrige rettigheder 20

5. Efterfølgende anvendelse af oplysninger fra infohuset 21

1. Indledning

En vellykket forebyggelsesindsats mod ekstremisme og radikalisering forudsætter et velfungerende samarbejde mellem de involverede myndigheder. Et centralt element i dette samarbejde består i udveksling af oplysninger mellem myndighederne.

Denne vejledning er målrettet offentlige myndigheders udveksling af personoplysninger som led i indsatsen mod ekstremisme og radikalisering. Vejledningen har særligt fokus på samarbejdet i infohusene, hvor landets 12 politikredse samarbejder med landets 98 kommuner om at forebygge og bekæmpe ekstremisme og radikalisering. De centrale aktører i infohusene er infohustovholderne fra politi og kommune. Andre aktører fra offentlige myndigheder inddrages i samarbejdet, hvor det er nødvendigt. Formålet med infohussamarbejdet er at sikre, at personer, der er i risiko for at begå kriminelle handlinger med ekstremistisk motiv, identificeres rettidigt med henblik på forebyggende indsatser. Infohussamarbejdet bygger videre på traditionerne fra det generelle kriminalitetsforebyggende samarbejde, hvor udvekslingen af personoplysninger primært er reguleret i retsplejelovens § 115.

Der er et bredt spænd i bekymringerne vedrørende ekstremisme og radikalisering, og vejledningen kan ikke ramme alle vinkler, men de centrale juridiske tvivlsspørgsmål, som kan opstå i forbindelse med udvekslingen af personoplysninger i infohusene, er forsøgt afdækket i denne vejledning.

Vejledningen er tænkt som et supplement til samarbejdsmodellen for infohusene og de tilhørende sagsgangsbeskrivelser, men kan samtidig fungere som et selvstændigt redskab i forbindelse med udveksling af oplysninger som led i forebyggelse af ekstremisme og radikalisering. Det bemærkes, at vejledningen er udarbejdet under inddragelse af Datatilsynet.

I vejledningen redegøres i afsnit 2 kort for de retlige rammer for samarbejdet i infohusene. Det vil sige primært retsplejelovens § 115, men også øvrige databeskyttelsesretlige regler. For overblikkets skyld skitseres overordnet i afsnit 3 sagsforløbet i infohuset. Under afsnit 4 beskrives udvekslingen af personoplysninger efter retsplejelovens § 115, hvor der sættes spot på centrale juridiske problemstillinger, som kan opstå i forbindelse med det ekstremisme og radikaliseringsforebyggende arbejde i infohusene. I afsnit 5 skitseres mulighederne for efterfølgende anvendelse af oplysninger fra infohusene.

2. De retlige rammer

Offentlige myndigheders udveksling af personoplysninger er hovedsageligt reguleret i databeskyttelsesforordningen[1] og databeskyttelsesloven[2]. For den behandling af personoplysninger, der foretages af de retshåndhævende myndigheder (politiet, anklagemyndigheden, kriminalforsorgen m.fl.) gælder dog retshåndhævelsesloven[3]. I forbindelse med offentlige myndigheders udveksling af personoplysninger i infohusene som led i indsatsen mod ekstremisme og radikalisering findes der dog også andre regelsæt af betydning.[4] Bestemmelsen i retsplejelovens § 115 er imidlertid helt central, fordi samarbejdet i infohusene bygger videre på de eksisterende kriminalpræventive samarbejder omfattet af retsplejelovens § 115.

Politiet og andre offentlige myndigheder kan udveksle oplysninger om enkeltpersoners rent private forhold – herunder om enkeltpersoner, der skønnes at være i risiko for at begå kriminelle handlinger med ekstremistisk motiv – efter retsplejelovens § 115, når det er nødvendigt af hensyn til det kriminalitetsforebyggende samarbejde (SSP-samarbejdet)[5], samarbejdet om indsatsen over for socialt udsatte (PSP-samarbejdet)[6] og samarbejdet om indsatsen over for personer, der løslades efter at have været frihedsberøvet (KSP-samarbejdet)[7]. Samarbejdet i infohusene hænger som nævnt tæt sammen med de eksisterende kriminalitetsforebyggende samarbejder i retsplejelovens § 115. Udveksling af oplysninger om enkeltpersoners rent private forhold mellem myndigheder i infohusene vil derfor ofte – men ikke altid – finde sted i medfør af retsplejelovens § 115. Derfor beskrives nedenfor i afsnit 4 primært rammene for udveksling af oplysninger efter retsplejelovens § 115. Dog bemærkes, at i de tilfælde udvekslingen af oplysninger ikke er dækket af retsplejelovens § 115, vil det i de fleste tilfælde alligevel kunne ske efter databeskyttelsesforordningen og databeskyttelsesloven. Det skyldes, at formålet med behandlingen af oplysninger om enkeltpersoner vil være at forebygge kriminelle handlinger med ekstremistisk motiv, hvilket vil være et legitimt og sagligt formål, som kan begrunde behandlingen af personoplysninger efter databeskyttelsesreglerne.

Generelt kan nævnes, at bestemmelsen i retsplejelovens § 115 skal give myndighederne mulighed for – inden en konkret indsats, f.eks. en kriminalitetsforebyggende indsats, og uden at indlede en egentlig sagsbehandling eller indhente samtykke – at begynde at udveksle oplysninger om rent private forhold og have uformelle og frie drøftelser om bestemte personers problemer. Drøftelserne forudsættes at ske på tværfagligt grundlag med henblik på at få klarlagt, om der er grundlag og behov for en indsats, herunder en ekstremisme- og radikaliseringsforebyggende indsats.

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

2 Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

3 Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer (retshåndhævelsesloven).

[4] Det omfatter bl.a. PET-lovens § 4, servicelovens § 49 a samt en række andre bestemmelser i særlovgivningen.

[5] Retsplejelovens § 115, stk. 1, nr. 1.

[6] Retsplejelovens § 115, stk. 1, nr. 2.

[7] Retsplejelovens § 115, stk. 1, nr. 2.

Bestemmelsen tilsigter at gøre det muligt for politiet at udveksle oplysninger med andre myndigheder, herunder kommunerne, om at man er bekymret for en bestemt person eller gruppe af personer med henblik på en forebyggende indsats.[8]

Det skal understreges, at retsplejelovens § 115 suppleres af databeskyttelsesreglerne. Retsplejelovens § 115 skaber et fælles hjemmelsgrundlag for udveksling af personoplysninger mellem myndigheder som led i samarbejderne omfattet af bestemmelsen. Behandlingen af de udvekslede oplysninger vil således fortsat være reguleret af de relevante regler herom i databeskyttelsesforordningen og databeskyttelsesloven. Hvis en behandling af personoplysninger er reguleret af retsplejelovens § 115, indebærer det, at databeskyttelsesreglerne – i det omfang det er relevant – finder anvendelse på forhold, der ikke er reguleret af retsplejelovens § 115. Det indebærer bl.a., at de databeskyttelsesretlige regler om den registreredes rettigheder, de grundlæggende behandlingsprincipper i databeskyttelsesforordningens artikel 5, reglerne om behandlingssikkerhed mv. finder anvendelse i det omfang, det er relevant, også for behandlinger af personoplysninger i infohusene i medfør af retsplejelovens § 115. Specifikt betyder det f.eks., at man kun må indsamle og behandle oplysningerne, hvis det er *nødvendigt* for ens arbejde, og at man skal huske at overveje oplysningspligten efter databeskyttelsesforordningen, selvom udvekslingen af personoplysningerne er sket under retsplejelovens § 115. Endvidere kan der – uanset at oplysningerne kan videregives efter retsplejelovens § 115 – være notat- og journaliseringspligt og andre forpligtelser efter de forvaltningsretlige regler. Se afsnit 4.

I forhold til efterfølgende anvendelse af oplysninger indsamlet og udvekslet i infohuset henvises til afsnit 5.

[8] Pkt. 3.5 i de almindelige bemærkninger til lovforslag nr. L 150 af 17. januar 1990 (LFF 1989-1990.1.150) (Dommeres habilitet, SSP-samarbejdet og advokatselskaber mv.)

3. Overblik: Sagsforløbet i infohuset

Infohusene er grundlæggende organiseret i *infohus kommune* og *infohus netværk*. Derudover findes også et nationalt forankret samarbejde i form af et nationalt sekretariat og en national styregruppe. Det er imidlertid på møderne i infohus kommune, som er det lokale samarbejdsforum mellem den enkelte kommune og den respektive politikreds, at den egentlige deling af personoplysninger mellem de deltagende myndigheder finder sted. I infohus netværk, som er et samarbejde mellem politiet og samtlige kommuner i politikredsen og andre relevante myndigheder, behandles der derimod ikke personoplysninger eller konkrete sager. Det samme gør sig gældende for det nationale samarbejde.

Begrebet "sagsforløb" anvendes i de følgende afsnit, selvom behandlingen af bekymringer i infohus kommune netop er kendetegnet ved, at der endnu ikke er startet en egentlig sagsbehandling op, jf. ovenfor i afsnit 2. For yderligere information om sagsforløbet ved håndtering af bekymringshenvendelser i infohus kommune henvises til vurderingsværktøjet til anvendelse ved bekymring for risiko for kriminalitet med et ekstremistisk motiv, som er udviklet i et samarbejde mellem Nationalt Center for Forebyggelse af Ekstremisme, Rigspolitiet Nationalt Forebyggelsescenter, Politiets Efterretningstjenestes Forebyggelsescenter og en række lokale praktikere fra kommune, politi m.fl.

Vurderingsværktøjet til anvendelse ved bekymring om ekstremisme kan tilgås her

3.1 Opstart

Sagsforløbet indledes typisk ved, at infohustovholderen i kommunen eller politiet modtager en bekymringshenvendelse vedrørende ekstremisme eller radikalisering. Det kan være en henvendelse fra en anden myndighed eller fra en privat aktør eller borger. Infohustovholderne i kommunen og politiet tager herefter kontakt til hinanden med henblik på at afklare, om bekymringshenvendelsen kan behandles på et møde i infohus kommune. I vurderingen indgår, om der er noget til hinder for, at henvendelsen behandles på et møde i infohus kommune. Hvis henvendelsen udgør en egentlig sikkerhedsmæssig trussel, håndteres henvendelsen af politiet og drøftes som udgangspunkt ikke i infohus kommune. Vurderes henvendelsen derimod eget til behandling på et møde i infohus kommune, vurderes det, hvilke relevante myndigheder der skal deltage på mødet. De relevante dele af den kommunale forvaltning inviteres med til mødet.

3.2 Inden mødet i infohus kommune

Forud for mødet i infohus kommune indsamler de deltagende myndigheder de oplysninger, der er nødvendige for en analyse og vurdering af bekymringshenvendelsen. Det vil som udgangspunkt være oplysninger, som de deltagende myndigheder har rådighed over – dvs. som eksempelvis fremgår af politiets registre, myndighedens sagsbehandlingssystemer eller lignende – men der kan også være behov for at indhente oplysninger fra andre myndigheder. Det vil eksempelvis være muligt at indsamle oplysninger fra en tidligere bopælskommune. Det er i den forbindelse

afgørende, at der ikke indhentes flere oplysninger, end hvad der er nødvendigt for at analysere og vurdere bekymringshenvendelsen, jf. afsnit 4.1. For så vidt angår indsamling af oplysninger fra private aktører henvises til afsnit 4.4. Se endvidere afsnit 5 om anvendelse af oplysninger uden for infohuset.

3.3 Møde i infohus kommune

På mødet i infohus kommune deltager infohustovholdere fra politikredsen og kommunen. Derudover deltager repræsentanter fra de relevante kommunale forvaltninger og andre relevante myndigheder, herunder kriminalforsorgen, den regionale behandlingspsykiatri m.fl. For så vidt angår privates deltagelse henvises til afsnit 4.4.

På mødet udveksles og deles de oplysninger, som hver myndighed er i besiddelse af og/eller har indsamlet om den pågældende inden mødet, og der foretages en analyse af personens situation, hvorefter der enten 1) udarbejdes en anbefaling om, hvad der bør arbejdes med for at skabe positiv udvikling hos personen, eller 2) det vurderes, at bekymringshenvendelsen ikke kan danne grundlag for at gøre yderligere i sagen. Det bemærkes, at der ikke træffes myndighedsbeslutninger i infohus kommune, men der er alene tale om en anbefaling. Iværksættelse af en eller flere konkrete indsatser over for den pågældende besluttes og iværksættes efterfølgende af myndigheden.

Det bemærkes, at man ved videregivelse af oplysninger om ekstremisme og radikalisering fra en myndighed til en anden, skal være opmærksom på, at kun de medarbejdere, der er udpegede til at håndtere sådanne oplysninger, gives oplysningerne. Der kan endvidere henvises til samarbejdsmodellen for infohusene og de tilhørende sagsgangsbeskrivelser, hvor det i en række tilfælde er specificeret, hvem blandt de involverede aktører der har ansvar for at udveksle oplysninger om ekstremisme og radikalisering.

3.4 Efter møde i infohus kommune

Myndigheden, som kan iværksætte en ekstremisme- eller radikaliseringsforebyggende indsats over for den pågældende person, træffer efterfølgende beslutning i overensstemmelse med den lovgivning, som myndigheden er underlagt. Det kan eksempelvis være en beslutning i kommunen om at tilbyde et mentorforløb eller samtaler med en psykolog. Der kan også iværksættes uddannelses- eller beskæftigelsesmæssige indsatser. Infohusets opfølgning på iværksatte indsatser samt behandling af nye bekymringshenvendelser om personer, der allerede er blevet drøftet i infohuset, er nærmere omtalt i afsnit 4.5.

4. Udveksling af personoplysninger i infohusene

4.1 Generelle overvejelser, som deltagerne i infohuset skal gøre sig

Udveksling af personoplysninger mellem myndigheder i infohusene er en *behandling af personoplysninger*. De databeskyttelsesretlige regler indeholder nogle generelle krav, som altid skal overvejes ved behandling af personoplysninger. En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Der skal være et retligt grundlag for at behandle personoplysningerne. Bestemmelsen i retsplejelovens § 115 giver det retlige grundlag for den behandling, der ligger i at udveksle personoplysninger inden for de omfattede samarbejder. Retsplejelovens § 115 suppleres af de databeskyttelsesretlige regler. Det vil således i langt de fleste tilfælde være muligt at behandle oplysninger som led indsatsen mod ekstremisme og radikalisering efter retsplejelovens § 115 eller efter de databeskyttelsesretlige regler. Retsplejelovens § 115 betyder også, at det ikke er nødvendigt at indhente et samtykke for at kunne påbegynde udvekslingen af oplysninger.

De deltagende myndigheder i infohussamarbejdet, der behandler personoplysninger, skal i løbet af samarbejdet generelt overveje om:

1. Behandlingen af oplysningerne om den enkelte sker *som led* i samarbejdsformerne i retsplejelovens § 115 med henblik på at forebygge ekstremisme og radikalisering. Hvis det ikke sker som led i samarbejdsformerne, skal der findes et andet grundlag for behandlingen af oplysningerne, f.eks. i databeskyttelsesreglerne eller anden lovgivning.
2. Behandlingen af oplysningerne er *nødvendig* for den kriminalitetsforebyggende indsats over for personer, der er i risiko for at begå kriminelle handlinger med ekstremistisk motiv.
3. Behandlingen af oplysningerne i øvrigt overholder databeskyttelsesforordningens artikel 5.

Når den deltagende myndighed skal foretage ovenstående vurdering, kan en række momenter have betydning. Myndigheden skal ved behandling af personoplysninger være opmærksom på, hvilken kategori oplysningen tilhører. Det skyldes, at oplysningens kategori har betydning for vurderingen af de tre betingelser. En personoplysning kan være ikke-følsom og følsom. Dertil er enkelte øvrige oplysninger særligt reguleret. Man bør være opmærksom på, at ikke-følsomme personoplysninger i *sammenhæng* med andre oplysninger efter omstændighederne kan være følsomme eller fortrolige personoplysninger. Se nedenfor i afsnit 4.2 om de forskellige kategorier af oplysninger.

Vurderingen af ovenstående betingelser skærpes ved behandling af følsomme og fortrolige oplysninger. Man kan sige, at de enkelte myndigheder skal være ekstra opmærksomme på at vur-

dere, om betingelserne ovenfor er opfyldt ved behandlingen af følsomme og fortrolige oplysninger. Er behandlingen i det lys nødvendig, er det dog tilladt at behandle oplysningen. Det kan i et typisk forløb i infohus kommune eksempelvis have betydning for vurderingen af en bekymringshenvendelse om en person, hvilken religion eller politisk overbevisning den pågældende har, ligesom helbredsoplysninger i form af eksempelvis psykisk diagnose kan have betydning. Myndigheden skal derfor konkret vurdere, om det er nødvendigt for samarbejdet i infohuset og vurderingen af bekymringshenvendelsen at behandle disse følsomme oplysninger om religion, politisk overbevisning og/eller helbred. Hvis myndigheden konkret vurderer, at det er nødvendigt at behandle oplysningen, må myndigheden dog godt det, selvom der er tale om en følsom oplysning.

Kravet om, at behandlingen af oplysningerne skal være nødvendig, betyder, at det altid bør overvejes, om det kan være tilstrækkeligt at behandle færre oplysninger for at kunne iværksætte den kriminalitetsforebyggende indsats. Hvis det er nødvendigt at behandle en given oplysning, vil oplysningen kunne behandles, når de øvrige betingelser er opfyldt.

Den myndighed, som i forbindelse med samarbejdet i infohuset *modtager* personoplysninger, bliver ved modtagelsen dataansvarlig for behandlingen af disse oplysninger, og myndigheden er derfor ansvarlig for at overholde de databeskyttelsesretlige krav. Det betyder bl.a., at myndigheden skal sikre sig, at myndigheden lever op til sin oplysningspligt, at der er et tilstrækkeligt sikkerhedsniveau ved behandlingen af oplysningerne mv. Modtager myndigheden oplysninger, der ikke er nødvendige for myndighedens opgaver i forhold til personen, eller modtages oplysninger ved en fejl, skal oplysningerne som udgangspunkt slettes. Det følger af principperne om dataminimering og opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5. Bemærk dog, at notat- og journaliseringspligten ofte fører til, at offentlige myndigheder ikke skal slette oplysninger, jf afsnit 4.8 nedenfor.

Når myndigheden som led i samarbejdet *videregiver* personoplysninger, skal myndigheden også sikre sig, at myndigheden overholder de databeskyttelsesretlige krav. Det betyder bl.a., at myndigheden skal sikre sig, at der alene videregives de nødvendige oplysninger.

Ved behandling af personoplysninger, herunder ved videregivelse, skal man sikre sig, at man lever op til kravene om behandlingssikkerhed. Det aktualiseres i høj grad, hvis man videregiver følsomme eller fortrolige personoplysninger via e-mail – særligt, hvis det sker til private. Det vil normalt være en passende sikkerhedsforanstaltning, hvis man anvender *kryptering*, når man sender følsomme og fortrolige oplysninger med e-mail.

Datatilsynets anbefalinger ved anvendelse af e-mails kan læses her

4.2 Hvilke kategorier af oplysninger kan videregives?

Deltagere i infohuset skal som nævnt ved behandlingen af personoplysninger være opmærksomme på, hvilke kategorier af oplysninger, der behandles. Det skyldes som nævnt, at kategorien af oplysninger har betydning for, hvilke krav der stilles til behandlingen af oplysningerne. Retsplejelovens § 115 gælder alene for oplysninger om enkeltpersoners rent private forhold. Rent

private forhold skal i denne forbindelse forstås som fortrolige oplysninger.[9] Retsplejelovens § 115 regulerer således ikke videregivelse af andre personoplysninger, men her kan videregivelsen af oplysningerne ske efter databeskyttelsesreglerne.

Følsomme personoplysninger, der er omfattet af databeskyttelsesforordningens artikel 9[10], vil utvivlsomt altid være fortrolige og dermed omfattet af retsplejelovens § 115. Det samme gælder for oplysninger om stafbare forhold omfattet af databeskyttelseslovens § 8.

Almindelige (ikke-følsomme) personoplysninger er primært ikke fortrolige og dermed ikke omfattet af retsplejelovens § 115. Visse almindelige personoplysninger kan dog være fortrolige, hvilket bl.a. gælder oplysninger om væsentlige sociale problemer, interne familieforhold eller selvmordsforsøg. Almindelige personoplysninger, der ikke er fortrolige, kan videregives med hjemmel i databeskyttelsesforordningens artikel 6[11]. Der er generelt en videre adgang til at behandle almindelige personoplysninger sammenlignet med følsomme og fortrolige personoplysninger. Det skyldes, at nødvendighedskravet skærpes ved behandling af følsomme og fortrolige personoplysninger, jf. ovenfor i afsnit 4.1. Det betyder, at der f.eks. er videre adgang til at behandle oplysninger om navn, adresse, fødselsdato og lignende almindelige oplysninger sammenlignet med oplysninger om seksualitet, religion, politisk overbevisning eller andre følsomme oplysninger.

For en oversigt over de forskellige typer af personoplysninger, se side 9 i Justitsministeriet vejledning om behandling af personoplysninger i SSP-samarbejdet**.**

4.3 Hvilke samarbejdsformer er omfattet af retsplejelovens § 115?

Det er afgørende for, om udvekslingen af personoplysninger kan ske inden for rammerne af retsplejelovens § 115, at udvekslingen af oplysningerne er *nødvendig* af hensyn til 1) det kriminalitetsforebyggende samarbejde, 2) samarbejdet om indsatsen over for socialt udsatte personer eller 3) samarbejdet om indsatsen over for personer, der løslades efter frihedsberøvelse. Afgrænsningen af de forskellige samarbejdsformer er nærmere beskrevet i den følgende.

Det kriminalitetsforebyggende samarbejde (SSP-samarbejdet)
Efter retsplejelovens § 115, stk. 1, *nr. 1*, kan politiet og offentlige myndigheder udveksle personoplysninger om rent private forhold, når det er nødvendigt af hensyn til det kriminalitetsforebyggende samarbejde. Kerneområdet for bestemmelsen er SSP-samarbejdet – det vil sige samarbejdet mellem skole, socialforvaltning og politi – men også andre samarbejder mellem politiet og kommunerne med henblik på kriminalitetsforebyggelse vil være omfattet.[12] Begrebet "det kriminalitetsforbyggende samarbejde" skal forstås bredt og omhandler udveksling af oplysninger for at forebygge kriminalitet. Det er derfor i vidt omfang muligt at videregive oplysninger efter bestemmelsen. Bestemmelsen i retsplejelovens § 115, stk. 1, nr. 1, om det kriminalitetsforebyggende

[9] Forvaltningslovens § 27 regulerer, hvad der er fortrolige oplysninger.

[10] Retshåndhævelseslovens § 10, hvis oplysningerne behandles af de retshåndhævende myndigheder (politi, anklagemyndighed mv.). Følsomme personoplysninger kan videregives, hvis det er *strengt nødvendigt* af hensyn til de formål, der er omfattet af loven.

[11] Retshåndhævelseslovens § 9, hvis oplysningerne behandles af de retshåndhævende myndigheder (politi, anklagemyndighed mv.). Ikke-følsomme personoplysninger kan videregives, hvis det er *nødvendigt* af hensyn til de formål, der er omfattet af loven.

[12] Pkt. 3.6 i de almindelige bemærkninger til lovforslag nr. L 150 af 17. januar 1990 om ændring af retsplejeloven (Dommeres habilitet, SSP-samarbejdet og advokatselskaber mv.)

samarbejde kan således benyttes til udveksling af personoplysninger mellem politiet og relevante offentlige myndigheder som led i indsatsen mod ekstremisme og radikalisering, når det er nødvendigt at hensyn til det kriminalitetsforebyggende samarbejde.

For yderligere vejledning omkring SSP-samarbejdet kan henvises til Justitsministeriet vejledning om behandling af personoplysninger i SSP-samarbejdet

Samarbejdet om indsatsen over for socialt udsatte personer (PSP-samarbejdet)
Efter retsplejelovens § 115, stk. 1, *nr. 2*, kan politiet og offentlige myndigheder udveksle personoplysninger om rent private forhold, når det er nødvendigt af hensyn til samarbejdet mellem politiet, de sociale myndigheder og social- og behandlingspsykiatrien om indsatsen over for socialt udsatte personer. Bestemmelsen kan bruges til udveksling af oplysninger mellem offentlige myndigheder om rent private forhold med henblik på en social eller psykiatrisk indsats som led i indsatsen mod ekstremisme og radikalisering.

Samarbejdet om indsatsen over for personer, der løslades efter frihedsberøvelse (KSP-samarbejdet)
Efter retsplejelovens § 115, stk. 1, *nr. 3*, kan politiet og offentlige myndigheder bl.a. udveksle personoplysninger om rent private forhold, når det er nødvendigt af hensyn til samarbejdet mellem politiet, kriminalforsorgen og de sociale myndigheder om indsatsen over for personer, der løslades fra frihedsberøvelse og skønnes at være radikaliserede eller i risiko for at blive det. Hvis kriminalforsorgen bliver bekendt med, at en indsat i en af kriminalforsorgens institutioner er radikaliseret eller ved at blive det, vil kriminalforsorgen f.eks. kunne videregive oplysninger herom efter retsplejelovens § 115, stk. 1, nr. 3, til kommunen med henblik på tilrettelæggelse af en forebyggende indsats, når den pågældende løslades. Oplysningerne kan f.eks. vedrøre den indsattes adfærd, udtalelser, litteratur, besøgende mv.[13] Det skal dog i hvert enkelt tilfælde vurderes, om videregivelse af bestemte oplysninger konkret er *nødvendigt* for samarbejdet, og for at de involverede myndigheder kan tilrettelægge en koordineret indsats over for den pågældende.

Eksempel om løsladelse

Der er opstået bekymring om radikalisering hos en person, der afsoner, men som står over for at skulle løslades. Kriminalforsorgen underretter politiet om bekymringen. Bekymringen vurderes at være egnet til en drøftelse på et møde i infohuset, hvor kriminalforsorgen bliver inviteret til at deltage. Kriminalforsorgen kan under mødet som udgangspunkt videregive oplysninger om afsoneren til infohustovholderen fra politiet og til den kommune, hvor den pågældende forventes at tage ophold i forbindelse med løsladelsen. Der kan videregives de oplysninger til kommunen, der er nødvendige for kommunens forebyggende indsats over for den pågældende. Der kan eksempelvis være behov for at videreføre et igangværende forløb (f.eks. et mentorforløb), eller der kan være behov for, at bopælskommunen iværksætter nogle nye indsatser over for den pågældende i relation til uddannelse og beskæftigelse.

[13] Pkt. 2.2.2. i de almindelige bemærkninger til lovforslag nr. L 78 af 9. december 2015 om ændring af retsplejeloven (Udveksling af oplysninger om tegn på radikalisering og ekstremisme).

Opsummering

Retsplejelovens § 115 finder kun anvendelse, når videregivelsen af personoplysninger om rent private forhold sker inden for rammerne af de nævnte samarbejdsformer. Uden for rammerne af de nævnte samarbejder skal der findes andre grundlag for videregivelse af oplysninger. Er udvekslingen af oplysninger ikke omfattet af samarbejdsformerne i retsplejelovens § 115, vil udvekslingen af oplysninger om enkeltpersoner typisk kunne ske inden for rammerne af databeskyttelsesreglerne (databeskyttelsesforordningen, databeskyttelsesloven samt retshåndhævelsesloven), hvor der er vide muligheder for at udveksle personoplysninger, når det er nødvendigt som led i indsatsen mod ekstremisme og radikalisering. Det skyldes, at behandling af oplysninger om en person med det formål at forebygge kriminelle handlinger med ekstremistisk motiv vil være et legitimt og sagligt formål, der kan begrunde behandling efter databeskyttelsesreglerne. Det er en forudsætning for at kunne benytte de databeskyttelsesretlige regler, at oplysningerne har været eller er under elektronisk behandling. Se endvidere afsnit 4.1 for generelle overvejelser man skal gøre sig.

4.4 Hvilke myndigheder og institutioner er omfattet af retsplejelovens § 115?

Bestemmelsen omfatter udveksling af personoplysninger om rent private forhold mellem politiet og offentlige myndigheder, der inddrages i de former for samarbejde, der er nævnt i retsplejelovens § 115, stk. 1, jf. stk. 2. Retsplejelovens § 115 omfatter som udgangspunkt alle offentlige forvaltningsmyndigheder.[14] Retsplejelovens § 115 indeholder ikke en begrænsning af, hvilke offentlige myndigheder personoplysninger kan udveksles med, men det vil altid være et krav, at der alene udveksles oplysninger med de myndigheder, der er nødvendige at inddrage i forhold til samarbejdet. Det er endvidere muligt efter retsplejelovens § 115, stk. 3, at udveksle oplysninger med selvejende institutioner, der løser opgaver for det offentlige på bl.a. socialområdet.

Bestemmelsen i retsplejelovens § 115 indeholder ikke en mulighed for at udveksle personoplysninger med *private aktører*. Det betyder imidlertid *ikke* nødvendigvis, at det er i strid med de databeskyttelsesretlige og forvaltningsretlige regler at udveksle oplysninger med en privat aktør. En udveksling af oplysninger vil så blot skulle ske efter reglerne i databeskyttelsesforordningen og databeskyttelsesloven og ikke efter retsplejelovens § 115.[15] En privat aktør vil i relation til bekymringer om radikalisering f.eks. kunne være et privat boligselskab eller en privat indkvarteringsoperatør på asylområdet. Er der tale om en selvejende institution, gælder dog retsplejelovens § 115, stk. 3.

For så vidt angår *ikke-følsomme (almindelige) personoplysninger*, kræver det enten, at den pågældende, som bekymringshenvendelsen retter sig imod, har givet samtykke til udvekslingen med den private aktør, eller at udvekslingen af oplysningerne f.eks. må anses for at være nød-

[14] Offentlige forvaltningsmyndigheder skal forstås i overensstemmelse med myndighedsbegrebet i forvaltningslovens § 1, stk. 1 og 2.

[15] For de retshåndhævende myndigheder (politi, anklagemyndighed mv.) gælder retshåndhævelsesloven, hvis udvekslingen sker til de formål, der er omfattet af loven.

vendig af hensyn til udførelsen af en opgave i samfundets interesse eller som led i offentlig myndighedsudøvelse eller er nødvendig for at overholde en retlig forpligtelse.[16] Udveksling af personoplysninger i infohussamarbejdet med private aktører vil i den forbindelse være udtryk for en udveksling i samfundets interesse.

Det er også muligt at udveksle *følsomme personoplysninger* i infohuset med private, men man skal her være mere opmærksom. Det vil enten kræve, at den pågældende har givet samtykke, eller at det er nødvendigt for at forfølge et retskrav for den afgivende eller modtagende myndighed/private aktør, eller at behandlingen er nødvendig for at beskytte den pågældendes vitale interesser, eller den pågældende tydeligvis har offentliggjort oplysningerne selv. Det kan eksem-

Eksempel om asylområdet

Der er bekymring om radikalisering hos en beboer under 18 år på et asylcenter. Asylcenteret drives af en *privat* indkvarteringsoperatør. Indkvarteringsoperatøren videregiver oplysninger om beboeren til Udlændingestyrelsen og til politiet. Endvidere orienteres kommunen, da beboeren er under 18 år, og kommunen har mulighed for at iværksætte indsatser efter sociallovgivningen over for den pågældende. Det vurderes, at bekymringshenvendelsen fra asylcenteret er egnet til behandling i infohus kommune. Kommunen og politiet har brug for at indsamle en række yderligere oplysninger om beboeren fra asylcenteret. Da der er tale om en privat indkvarteringsoperatør, vil retsplejelovens § 115 ikke kunne anvendes på kommunens og politiets indsamling af oplysningerne. Derimod vil indsamling af oplysningerne kunne ske efter databeskyttelsesreglerne. Kommunen og politiet må derfor gerne indsamle oplysninger fra den private, selvom det ikke er omfattet af retsplejelovens § 115.

Bekymringshenvendelsen skal efterfølgende behandles på et møde i infohus kommune. På mødet deltager politiet og kommunens infohustovholdere samt en medarbejder fra den kommunale socialforvaltning. En repræsentant fra Udlændingestyrelsen vil kunne deltage i mødet, hvis det findes nødvendigt. Udveksling af oplysninger med Udlændingestyrelsen vil kunne ske efter retsplejelovens § 115 eller i hvert fald databeskyttelsesforordningen og databeskyttelsesloven. Det vil sige, at hvis det falder uden for retsplejelovens § 115, vil det kunne ske efter databeskyttelsesreglerne. En repræsentant fra den private indkvarteringsoperatør vil kunne deltage i mødet i infohus kommune om den pågældende beboer på asylcenteret, men må kun gives de oplysninger om den pågældende beboer, som er nødvendige for, at indkvarteringsoperatøren kan hjælpe med den forebyggende indsats rettet mod den pågældende beboer. Det vil også være muligt efter databeskyttelsesreglerne at videregive følsomme oplysninger om beboeren til indkvarteringsoperatøren.

Det kan samtidig overvejes, om det er nødvendigt, at den private indkvarteringsoperatør deltager i hele mødet. Hvis det ikke er tilfældet, kan mødet planlægges sådan, at den private aktør alene får kendskab til visse oplysninger af nødvendighed for vedkommendes rolle i infohussamarbejdet, og den forebyggende indsats vedkommende skal stå for.

[16] Databeskyttelsesforordningens artikel 6, stk. 1, litra c og e.

pelvis være på sociale medier, der er offentligt tilgængelig for alle. Udveksling af følsomme personoplysninger med private vil kunne være nødvendigt for at forfølge et retskrav, idet retskrav i denne sammenhæng fortolkes bredt.[17]

Det vil – uanset oplysningens karakter som følsom eller ikke-følsom – herudover være væsentligt at se på, om det er *nødvendigt* at udveksle personoplysningen. Generelt kan det siges, at der alene kan udveksles de oplysninger, som den private har behov for at have kendskab til for at kunne hjælpe med den forebyggende indsats rettet mod den pågældende. Det vil generelt være nødvendigt og sagligt at videregive navn, fødselsdato og lignende ikke-følsomme oplysninger på den person, som den private skal indgå i et samarbejde om. Det vil også kunne være nødvendigt og sagligt at videregive meget følsomme oplysninger om eksempelvis den pågældendes religion, politiske overbevisning eller helbred. Myndighederne skal dog være mere påpasselige i forhold til følsomme oplysninger. Derfor skal myndighederne være særligt opmærksomme på, hvilke oplysninger der videregives.

I de tilfælde, hvor det er nødvendigt at udveksle visse oplysninger med private for at vurdere en bekymringshenvendelse om ekstremisme eller radikalisering i infohussamarbejdet, vil det ikke være i strid med tavshedspligten. Det skyldes, at videregivelsen af de fortrolige oplysninger må anses for berettiget. Overvej også behandlingssikkerheden ved videregivelse af følsomme og fortrolige personoplysninger til private, jf. afsnit 4.1 om videregivelse via e-mail.

Vurderingen af, om udvekslingen af oplysninger med den private er i overensstemmelse med de databeskyttelsesretlige regler og forvaltningsretten, kan også afhænge af, om den private aktør har fået et tavshedspålæg efter forvaltningslovens § 27, stk. 6. Tavshedspålægget indebærer, at der gives et forbud mod uberettiget af videregive oplysninger, omfattet af pålægget, og det øger sikkerheden omkring den privates behandling af oplysningerne. Tavshedspålægget skal være skriftligt meddelt den private forud for, at den private får kendskab til den fortrolige oplysning. Tavshedspålægget skal gives af den aktør, der videregiver den fortrolige oplysning. Der skal endvidere være et klart behov for at meddele tavshedspålægget. Tavshedspålægget kan dog ikke gives, hvis der er en pligt til at inddrage den private, eksempelvis for at kunne oplyse en konkret sag.

Vil du vide mere? Læs mere her om tavshedspålæg i vejledning om forvaltningslovens pkt. 159 ff.

4.5 Hvordan behandles opfølgning på indsatser og nye bekymringshenvendelser?

Udfaldet af et møde i infohus kommune vil være, at der enten 1) udarbejdes en anbefaling om, hvad der bør arbejdes med for at skabe positiv udvikling hos personen, eller 2) det vurderes, at bekymringshenvendelsen ikke kan danne grundlag for at gøre yderligere i sagen.

Hvis der er iværksat en indsats over for den pågældende person, må det antages, at man inden for rammerne af § 115 kan udveksle oplysninger for at effektuere indsatsen eller følge op på, om der fortsat er bekymring for ekstremisme eller radikalisering. Det afgørende er i den forbindelse,

[17] Betænkning nr. 1565 om yttelsesforordningen, s. 203 og 215.

at udvekslingen af oplysninger er nødvendig som led i den kriminalitetsforebyggende arbejde eller de øvrige samarbejder omfattet af retsplejelovens § 115. Hvis udvekslingen af oplysninger som opfølgning på iværksatte indsatser ikke sker som led i de samarbejder, der er omfattet af retsplejelovens § 115, kan oplysningen videregives, hvis der er et andet grundlag for videregivelsen. Det kan eksempelvis være, at en myndighed anmoder om at få tilsendt en oplysning, som er afgørende for myndighedens afgørelsessag, jf. forvaltningslovens § 31.

Ofte vil der i forbindelse med infohussamarbejdet være tale om langstrakte forløb, hvor der f.eks. med mellemrum modtages bekymringshenvendelser, men hvor der måske ikke tidligere har været grundlag for at iværksætte en indsats. Sådanne "tilbagevendende" bekymringer om samme person vil også kunne drøftes i infohuset efter retsplejelovens § 115. Men omfanget af henvendelserne vil dog kunne medføre, at der under alle omstændigheder er behov for at igangsætte en egentlig sagsbehandling hos de relevante myndigheder således, at sagen løftes ud af infohuset.

4.6 Kan oplysninger benyttes i efterforskning?

Det følger af retsplejelovens § 115, stk. 2, 2. pkt., at personoplysningerne i forbindelse med samarbejderne ikke må videregives med henblik på efterforskning af straffesager. Sker det i særlige tilfælde, at politiet gennem samarbejderne bliver bekendt med oplysninger, som kan have betydning for efterforskningen af en straffesag, vil politiet kunne benytte oplysningerne i forbindelse med efterforskningen. Bestemmelsen udelukker derimod, at politiet med henblik på efterforskning gennem samarbejderne indhenter oplysninger med det formål at bruge oplysningerne til efterforskning.[18]

Bestemmelsen er i øvrigt ikke til hinder for, at medarbejderne hos de myndigheder, der indgår i samarbejderne, vil kunne anmelde strafbare forhold til politiet. Dette skal i givet fald blot ske uden for samarbejderne. Bestemmelsen tilsigter således f.eks. ikke at ændre noget i de situationer, hvor det følger af f.eks. sociallovgivningen, at der består en anmeldelsespligt.

4.7 Er der en pligt til at videregive oplysninger efter retsplejelovens § 115?

Retsplejelovens § 115 indeholder ikke en pligt til at videregive fortrolige oplysninger. De myndigheder og institutioner, der indgår i samarbejderne, er ikke forpligtet til at videregive oplysninger. Det skal her bemærkes, at forvaltningslovens § 31, stk. 1, er fraveget med retsplejelovens § 115, hvorfor offentlige myndigheder ikke har en pligt til at videregive oplysninger i disse samarbejder på begæring af andre myndigheder. De databeskyttelsesretlige regler medfører heller ikke en pligt til at videregive personoplysninger.

Der kan dog i anden særlovgivning være en pligt til at videregive fortrolige oplysninger. Som eksempel på en sådan pligt kan nævnes PET-lovens § 4, hvorefter myndigheder har pligt til at videregive oplysninger til PET, hvis PET anmoder herom og betingelserne i bestemmelsen i øvrigt et opfyldt. I servicelovens kapitel 27 er der i visse tilfælde en underretningspligt. Endvidere kan

[18] Jf. stk. 4.2 i Vejledning 2009-07-10 nr. 60 om politiets samarbejde med de sociale myndigheder og psykiatrien som led i indsatsen over for socialt udsatte personer (PSP-samarbejdet) og om videregivelse af oplysninger i forbindelse med samarbejdet

nævnes er der undtagelsesvist efter straffeloven kan være en pligt til om fornødent at anmelde visse alvorlige forbrydelser til politiet.[19] I den forbindelse kan oplysningerne ikke anses for at være videregivet som led i samarbejdet om infohusene, jf. også retsplejelovens § 115, stk. 2, 2. pkt.

4.8 Registrering og journalisering af oplysninger

4.8.1 Notatpligt

Infohussamarbejdet er at betragte som et samarbejde om faktisk forvaltningsvirksomhed. I almindelighed er der derfor ikke et krav om, at mundtlige oplysninger, som udveksles som led i infohussamarbejdet, skal noteres ned. Det skyldes, at notatpligten efter offentlighedslovens § 13 alene gælder i afgørelsessager.

Det er dog muligt, at der efter omstændighederne vil påhvile myndighederne en notatpligt i den enkelte situation som følge af ulovbestemte forvaltningsretlige grundsætninger. Hensynet bag notatpligten er, at det efterfølgende kan fastlægges, hvad der er sket (dokumentationshensyn). Det vil endvidere kunne give mulighed for effektiv kontrol af, om myndigheden har handlet korrekt (kontrolhensyn). Det kan f.eks. blive relevant ved en senere erstatningssag.

Den ulovbestemte notatpligt vedrører *væsentlige sagsekspeditionsskridt*. Det kan på den baggrund være nødvendigt at notere væsentlige oplysninger i en lang række situationer omfattet af infohussamarbejdet. Det kan være om aftalte indsatser i infohussamarbejdet og aftaler om arbejdsfordelingen myndighederne imellem. Det kan eksempelvis være en aftale om en bekymringssamtale med borgeren. Et væsentligt sagsekspeditionsskridt kan efter omstændighederne også være en beslutning om at videregive oplysninger. Endvidere vil mundtlig opfyldelse af oplysningspligten efter de databeskyttelsesretlige regler kræve et notat, jf. afsnit 4.9. Der kan i regi af infohuset drøftes forhold af væsentlig betydning for den pågældende, og det kan være naturligt at notere visse væsentlige oplysninger ned for at kunne dokumentere disse senere. Det kan endvidere være et væsentligt sagsekspeditionsskridt at undlade at iværksætte yderligere indsatser. Det kan derfor være hensigtsmæssigt at notere, at der ikke er grundlag for at iværksætte en indsats på baggrund af en bekymringshenvendelse. Ved en senere ny bekymringshenvendelse vedrørende pågældende, kan det være nyttigt at se, hvilke overvejelser der indgik i den tidligere vurdering. Det bemærkes i den forbindelse, at notatpligten ikke betyder, at der skal foretages partshøring, jf. afsnit 4.9.2 om parthøring i afgørelsessager.

I visse særlige tilfælde følger det af god forvaltningsskik, at faktiske oplysninger skal noteres.

Der er ikke formkrav til notatet. Det kan ske i hånden (og evt. efterfølgende scannes), på computeren, ved at arkivere en e-mail sendt til egen e-mailadresse eller lignende. Noteringerne om de pågældende kan også være i et samlet dokument vedrørende flere personer. Det er dog et krav, at noteringen kan fremsøges igen, bl.a. med henblik på at give indsigt eller aktindsigt.

Læs mere om notatpligten i ombudsmandens myndighedsguide her.

[19] Straffelovens § 141.

4.8.2 Journaliseringspligt

Dokumenter, der er modtaget, afsendt eller oprettet af myndigheden som led i administrativ sagsbehandling, med betydning for en sag eller sagsbehandling skal journaliseres efter offentlighedslovens § 15. Det gælder også elektroniske dokumenter så som e-mails. SMS-beskeder kan ligeledes være omfattet. Journaliseringspligten gælder uanset titlen på dokumentet. Interne dokumenter skal forelægge i endelig form for at være journaliseringspligtige. Et dokument med titlen "arbejdsdokument", der er endeligt, kan derfor være omfattet af kravet om journalisering.

Journaliseringspligten gælder både i afgørelsessager og andre administrative sager. Pligten til at journalisere skal således overvejes i infohussamarbejdet. Dokumenter med notatpligtige oplysninger, som beskrevet under afsnit 4.8.1, skal ligeledes journaliseres.

Journalisering skal ske snarest muligt. Papirbaserede dokumenter bør i almindelighed være journaliseret 3-4 arbejdsdage efter modtagelsen eller afsendelsen. E-mails bør som udgangspunkt være journaliseret 7 arbejdsdage efter modtagelsen eller afsendelsen. Disse frister omfatter ikke interne dokumenter. Journalsystemet skal indeholde oplysninger om datoen for modtagelsen eller afsendelsen samt en kort, tematisk angivelse af dokumentets indhold. Journalisering skal foretages på en korrekt og systematisk måde, sådan at dokumentet ikke journaliseres på en forkert sag, og således at dokumentet kan fremsøges igen.

Læs mere om journaliseringspligten i ombudsmandens myndighedsguide her.

4.9 Oplysningspligt og partshøring

4.9.1 Oplysningspligten

Efter databeskyttelsesforordningens artikel 13 og 14 har den person, som der behandles oplysninger om, krav på at blive underrettet, hvis der behandles oplysninger om den pågældende.[20] Forpligtelsen påhviler den dataansvarlige myndighed. Ved udveksling af oplysninger i infohussamarbejdet vil de deltagende myndigheder hver især være dataansvarlige for deres behandling af personoplysninger om den pågældende.

De deltagende myndigheder skal overveje oplysningspligten efter databeskyttelsesforordningen og således overveje, om den person, som de behandler oplysninger om (og/eller forældremyndighedsindehaveren) bl.a. skal have oplysninger om, at myndigheden behandler personoplysninger om den pågældende, hvad formålene med behandlingen af personoplysningerne er, at personoplysningerne behandles efter bestemmelsen i retsplejelovens § 115 (eller databeskyttelsesreglerne), og hvilken kategori oplysningerne har mv.

Har den deltagende myndighed opfyldt sin oplysningspligt over for borgeren, vil det normalt ikke være nødvendigt for myndigheden at opfylde en ny oplysningspligt i forbindelse med videregivelsen af personoplysningerne til de øvrige deltagende myndigheder. Dette skyldes også, at de øvrige deltagende myndigheder, når myndighederne modtager personoplysningerne, som udgangspunkt har en oplysningspligt over for den pågældende borger.

[20] De retshåndhævende myndigheders oplysningspligt er reguleret i retshåndhævelseslovens §§ 13-14.

I mange tilfælde vil den forebyggende indsats, der skal iværksættes, kræve et samarbejde med den pågældende, hvorfor det under alle omstændigheder vil være naturligt at inddrage den pågældende.

Der er ikke formkrav til selve orienteringen. Det er således muligt at give orienteringen telefonisk (med telefonnotat herom), mundtligt ved et møde eller besøg (med notat herom), som en folder udleveret ved møder eller besøg, i et brev, via et link etc. Men det kan være en fordel at give orienteringen skriftligt, så det senere kan dokumenteres, at orienteringen er givet. Sker orienteringen mundtlig, er det af dokumentationshensyn derfor meget vigtigt, at myndigheden noterer ned, at den enkelte (og/eller forældremyndighedsindehavere) er orienteret. Myndigheden kan med fordel udarbejde nogle standard-oplysningsskemaer, der sikrer, at der gives alle de relevante oplysninger efter databeskyttelsesforordningen.

Vil du vide mere om oplysningspligten? Se Datatilsynets vejledning her.

Som *udgangspunkt* skal myndigheden således orientere om, at myndigheden nu behandler personoplysningerne. Når oplysningerne er indsamlet hos den pågældende selv, skal orienteringen gives snarest muligt og inden for 10 dage. Når oplysningerne er indsamlet fra andre end den pågældende selv, skal orienteringen gives inden for 10 dage og ikke senere end en måned efter modtagelsen af oplysningerne.

Det vil dog være muligt helt at *undlade* at orientere den pågældende (og/eller forældremyndighedsindehaverne) om behandlingen af personoplysningerne som følge af databeskyttelsesforordningen eller databeskyttelsesloven.[21] Den pågældende skal ikke orienteres, hvis pågældende allerede er bekendt med de oplysninger, der skal indgå i orienteringen. Myndigheden har derudover mulighed for efter bl.a. databeskyttelseslovens § 22 og databeskyttelsesforordningens 14, stk. 5, at undlade at orientere den pågældende.

Myndigheden *skal foretage en konkret vurdering* af, om der er grundlag for at undlade at orientere. Der skal foretages en interesseafvejning. I afvejningen skal indgå på den ene side den pågældendes interesse i at blive orienteret og på den anden side afgørende hensyn til private eller offentlige interesser.

I relation til samarbejdet i infohusene vurderes det, at underretning til den pågældende vil kunne undlades efter databeskyttelsesforordningens artikel 14, stk. 5, eller databeskyttelseslovens § 22, hvis:

1. Oplysning om behandling til den pågældende i alvorlig grad vil gøre det umuligt eller i alvorlig grad forhindre, at der iværksættes en forebyggende indsats over for den pågældende.
2. Oplysning om behandling vil være umulig eller kræve en uforholdsmæssig stor indsats, typisk ved (mange) bipersoner, jf. nedenfor.
3. Oplysning om behandling ikke bør ske af hensynet til den pågældende selv.

[21] De retshåndhævende myndigheder kan undlade at orientere i videre omfang, jf. retshåndhævelseslovens §§ 13-14

4. Oplysninger om behandling bør vige for afgørende hensyn til statens sikkerhed eller den offentlige sikkerhed.
5. Oplysning om behandling ikke kan ske, fordi det er nødvendigt af hensyn til forebyggelse og efterforskning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner.

Der findes andre undtagelsesmuligheder, men de ovennævnte er vurderet som de relevante i forhold til samarbejdet i infohusene. Oplysningspligten vil kunne indtræde på et senere tidspunkt, når eller hvis hensynene for at gøre undtagelse ikke længere gør sig gældende. Oplysningspligten vil bl.a. kunne undlades eller udskydes, hvis det konkret vurderes, at det vil hindre en efterforskning, eller hvis orientering om behandling til den pågældende vil betyde, at den pågældende vil ryge længere ud i et ekstremistisk spor. Orientering vil også kunne undlades, hvis det vil kunne hindre den rette hjælp eller indsats, hvis den pågældende orienteres om behandlingen.

Eksempel 1 om oplysningspligt

En kommune behandler en bekymring om en bestemt person med henblik på at forebygge radikalisering. Oplysningerne stammer bl.a. fra infohussamarbejdet. Kommunen skal som den dataansvarlige overholde oplysningspligten i databeskyttelsesforordningens artikel 14, stk. 1. Kommunen skal med andre ord som udgangspunkt give pågældende borger en række informationer om behandlingen af personoplysningerne, herunder bl.a. om formålet med behandlingen, kategorierne af oplysningerne, som kommunen behandler, og kontaktoplysninger til kommunen. Det er dog muligt, at kommunen ud fra en konkret vurdering kan undlade at oplyse den pågældende borger, hvis en af betingelserne i databeskyttelsesforordningens artikel 14, stk. 5, eller databeskyttelseslovens § 22 er opfyldt. I den konkrete sag ringer kommunen til politikredsen for at høre, om det er noget til hinder for at give personen oplysninger om behandlingen. Politiet er i gang med en efterforskning mod den pågældende person. Politiet oplyser derfor, at formålet med politiets behandling af oplysninger om den pågældende vil kunne forspildes, hvis kommunen på dette tidspunkt oplyser den pågældende om, hvilke oplysninger kommunen behandler om vedkommende. På den baggrund vurderer kommunen, at den pågældende borger på nuværende tidspunkt ikke skal underrettes om, at kommunen behandler personoplysninger om vedkommende, jf. artikel 14, stk. 5. Den kommunale sagsbehandler laver et notat herom på sagen, hvor kommunens sagsoplysning og vurdering fremgår.

Eksempel 2 om oplysningspligt

En bekymring om en person er modtaget i kommunen. Infohustovholderen i kommunen tager kontakt til infohustovholderen i politiet. Det vurderes, at bekymringen egner sig til drøftelse i infohus kommune. Der skal foretages en konkret vurdering af, om der skal gives underretning om behandlingen af oplysninger til den pågældende, jf. databeskyttelsesforordningens artikel 14. Det vurderes, at der er risiko for, at personen vil nægte at tage imod hjælp, hvis pågældende modtager underretning om, at kommunen og politiet nu behandler oplysninger om den pågældende. Man undlader derfor at orientere den pågældende på dette tidspunkt.

Bekymringen drøftes nu i infohus kommune. Man vurderer, at bekymringen ikke er tilstrækkelig begrundet, og der er derfor ikke grundlag for at gå videre med bekymringen. Man modtog dog 2 måneder tidligere en lignende bekymring om den pågældende. Man har tillagt det betydning, at personen har en række gode personlige forhold, der trækker i positiv retning. Man vælger derfor at se tiden an, men aftaler samtidig, at de involverede myndigheder skal være opmærksomme på, om der sker ændringer i pågældendes personlige forhold. Der skal foretages en konkret vurdering af, om der i forlængelse af mødet i infohuset skal gives underretning om behandlingen af oplysninger til den pågældende, jf. databeskyttelsesforordningens artikel 14. Det vurderes, at underretning til den pågældende skal undlades, fordi det vil kunne føre til unødig stigmatisering af den pågældende, ligesom at man fortsat er bange for, at pågældende vil nægte at tage imod eventuel senere hjælp.

Det skal endvidere overvejes, om eventuelle *"bipersoner"* skal underrettes. Bipersoner er ikke den egentlige genstand for myndighedens behandling af personoplysninger. De optræder derimod alene accessorisk i tilknytning til andre oplysninger. Det vil med andre ord sige, at oplysninger om en biperson "følger med" hovedpersonen, men oplysningerne er alene sekundære. Det kan f.eks. være pårørende eller fagpersoner som en læge eller lignende. Myndigheden har som udgangspunkt også en pligt til at orientere bipersonen om behandlingen af dennes personoplysninger, på samme måde som orienteringen af hovedpersonen. Der er samme mulighed for at undlade at oplyse om behandlingen af personoplysninger, som beskrevet ovenfor. Interesseafvejningen vil dog ofte falde anderledes ud, fordi hensynet til en biperson er mindre tungtvejende. I de fleste tilfælde er det således ikke nødvendigt at underrette en biperson.

Hvis den pågældende er under 18 år, er det i givet fald forældremyndighedsindehaverne, der skal orienteres. Det vil bero på en konkret modenhedsvurdering af den pågældende, hvorvidt den pågældende skal orienteres samtidig med forældremyndighedsindehaverne.

4.9.2 Partshøring

Forvaltningslovens § 19 om partshøring finder anvendelse på afgørelsessager. Da der i infohussamarbejdet som hovedregel ikke vil blive truffet afgørelser, finder parthøringsreglerne ikke anvendelse. Såfremt en af de deltagende myndigheder anvender oplysninger, som de har fået kendskab til som led i infohussamarbejdet, i en afgørelsessag, hvor myndigheden træffer beslutning om en forebyggende indsats, skal der som udgangspunkt ske parthøring over oplysningerne.

4.9.3 Øvrige rettigheder

Indsigtsretten og retten til berigtigelse

De personer, der udveksles oplysninger om, har i henhold til databeskyttelsesforordningens artikel 15 efter anmodning krav på at få indsigt i de udvekslede oplysninger.[22] En sådan indsigtsanmodning vil som udgangspunkt skulle imødekommes, medmindre der i henhold til databeskyttelseslovens § 22 efter en konkret vurdering gøres undtagelse fra indsigtsretten, jf. afsnit 4.9.1.

Personen har også ret til at få berigtiget oplysninger. Det følger af databeskyttelsesforordningens artikel 16. Det indebærer, at den pågældende har ret til at få *urigtige* (forkerte) personoplysninger om sig selv rettet, og ret til at få fuldstændiggjort ufuldstændige personoplysninger. Dog vil det for offentlige myndigheder ofte være sådan, at man af hensyn til dokumentation for faktuelle forhold, som en beslutning eller afgørelse er truffet på grundlag af, ikke kan kræve, at urigtige oplysninger slettes.

Aktindsigt

Den pågældende har ligeledes adgang til aktindsigt. Det vil særligt være reglen om egenacces – det vil sige adgangen for en person til at blive gjort bekendt med oplysninger om vedkommende selv – efter offentlighedsloven, der er relevant, fordi samarbejdet i infohusene som udgangspunkt ikke består af afgørelsessager. I det omfang oplysninger fra infohussamarbejdet indgår i en afgørelsessag, f.eks. fordi en deltagende myndighed har iværksat en indsats, som har ført til en afgørelsessag, skal retten til aktindsigt vurderes efter forvaltningslovens regler om partsaktindsigt. Parten har som udgangspunkt ret til aktindsigt i alle sagens dokumenter, medmindre dokumenterne eller oplysningerne efter en konkret vurdering kan undtages. Det kan f.eks. være en myndigheds interne arbejdsdokumenter.

Inddragelse af den myndighed, som oplysningerne er modtaget fra

Er oplysningerne modtaget fra en anden myndighed som led i samarbejdet i infohuset, er det som regel relevant at høre denne myndighed forud for eventuel orientering, indsigt, partshøring eller aktindsigt. Det sker med henblik på at få myndighedens opfattelse af, om der skal gøres undtagelse hertil. Hvis oplysningerne er modtaget fra politiet, herunder PET, bør politiet altid høres forinden.

[22] For de retshåndhævende myndigheder gælder retshåndhævelseslovens §§ 15-16.

5. Efterfølgende anvendelse af oplysninger fra infohuset

Det er ofte sådan, at der kører flere forskellige forløb sideløbende. Det er således ofte forekommende, at der foruden forløbet i infohuset er en administrativ sag eller en afgørelsessag hos en af de deltagende myndigheder. Det kan eksempelvis være flere forskellige sager i forskellige dele af den kommunale forvaltning. Hverken de databeskyttelsesretlige regler eller retsplejelovens § 115 udelukker, at oplysninger udvekslet i infohussamarbejdet, kan behandles i forbindelse med den anden sag. Der er således meget vide rammer for at genanvende oplysninger i anden sammenhæng. Det er dog et krav, at oplysningerne ikke anvendes til et formål, der er uforeneligt med det formål, som oplysningerne oprindeligt blev indsamlet til. Det er endvidere et krav, at oplysningen er nødvendig for den anden sag. Se dog afsnit 4.6 om anvendelse af oplysninger i politiets efterforskning. Endvidere bør myndigheden sikre, at oplysningerne er ajourførte og rigtige, før de træffer afgørelse.

Oplysninger modtaget i infohussamarbejdet er ofte relevante for *de deltagende myndigheder* for at kunne træffe en efterfølgende afgørelse om en særlig indsats over for den person, der er i risiko for at begå kriminelle handlinger med ekstremistisk motiv. Der træffes som nævnt ikke afgørelser i infohuset. Den efterfølgende behandling af oplysninger – som finder sted uden for infohuset og retsplejelovens § 115 – i afgørelsessagen hos myndigheden er således i orden. Men behandlingen vil skulle ske med hjemmel i databeskyttelsesreglerne eller anden særlovgivning (f.eks. serviceloven) og vil skulle overholde de almindelige regler for behandling af personoplysninger, herunder databeskyttelsesreglerne, samt forvaltningsretlige regler. Almindelige personoplysninger vil derfor kunne behandles efter databeskyttelsesforordningens artikel 6, stk. 1, litra c og e, mens følsomme oplysninger og eventuelle oplysninger om strafbare forhold vil kunne behandles efter henholdsvis databeskyttelsesforordningens artikel 9, stk. 1, litra f, og databeskyttelseslovens § 8.

Det kan forekomme, at oplysninger, som har været drøftet i infohuset, er relevante for *andre myndigheder, som ikke har deltaget i drøftelser i infohuset*. I en sådan situation er der også gode muligheder for at videregive oplysningerne til andre myndigheder, hvis de almindelige betingelser for videregivelse af personoplysninger fra en myndighed til en anden er overholdt. Det betyder bl.a., at oplysningen kan videregives, hvis det er nødvendigt. En myndighed må som udgangspunkt kunne gå ud fra, at de personoplysninger, som en anden myndighed anmoder om at modtage, også vil være nødvendige som led i dennes myndighedsudøvelse, medmindre der er forhold i forespørgslen, som konkret tyder på noget andet. I forhold til videregivelse af personoplysninger, som sker på en myndigheds eget initiativ, bør myndigheden i tvivlstilfælde kontakte den anden myndighed på forhånd for at få afklaret, om en eventuel videregivelse vil være nødvendig for myndighedens opgavevaretagelse.

Der kan endvidere være en pligt for de deltagende myndigheder i infohuset til på begæring at videregive oplysninger til en anden myndighed, fordi oplysningen er afgørende for en afgørelse, myndigheden skal træffe eller afgørende for dennes virksomhed, jf. forvaltningslovens § 31. Det er dog vigtigt, at politiet inddrages før videregivelse med henblik på at vurdere sikkerhedsaspekterne.

Eksempel om kriminalforsorgen

Infohus kommune har drøftet en bekymring om radikalisering vedrørende en person, der allerede er inde i en kriminel løbebane. Personen er tidligere dømt og har på tidspunktet for drøftelsen i infohus kommune en aktuelt sigtelse. Det vurderes i infohuset, at et arbejde vil give personen mulighed for at komme på et bedre spor. Der iværksættes en beskæftigelsesindsats i kommunalt regi. Nogle måneder efter bliver den pågældende dømt og skal afsone i en af kriminalforsorgens institutioner. Oplysninger om bekymringshenvendelsen vil i denne situation være relevante for kriminalforsorgen med henblik på at vurdere, hvor den pågældende skal indsættes til afsoning. Kriminalforsorgen har imidlertid ikke deltaget i infohuset, da den pågældende på tidspunktet for behandling i infohuset ikke stod over for afsoning. Der er gode muligheder i sagen for, at de deltagende myndigheder kan videregive oplysninger udvekslet i infohuset til kriminalforsorgen. Kriminalforsorgen skal være opmærksom på, at oplysningerne fra infohuset er ajourførte og rigtige, da der efterfølgende kan være sket ændringer i den pågældendes forhold.

Dato
August 2020

Justitsministeriet
Slotsholmsgade 10
1216 København K

Telefon
72 26 84 00

Email
jm@jm.dk

ISBN
978-88-98564-35-7

Foto
Scanpix