JUSTITSMINISTERIET

Betænkning om restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud

Betænkning nr. 1504

Kronologisk fortegnelse over betænkninger

2008

1494 Straffelovrådets betænkning om en torturbestemmelse i straffeloven
1495 Evaluering af forsøg med stiftsråd
1496 Retshåndhævelsesarrest i sædelighedssager
1497 Grønlandsk – Dansk selvstyre kommissions betænkning om selvstyre i Grønland
1498 Betænkning om modernisering af selskabsretten
1499 Ikke offentliggjort
1503 Ikke offentliggjort

2009

1500 Betænkning om udveksling af oplysninger indenfor den offentlige forvaltning
1501 Betænkning om konfliktsråd
1502 Betænkning om visse køberetlige regler om sikkerhedsmangler
1504 Betænkning om restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud
1505 Behandling af klager over politiet

IT- og Telestyrelsen
Holsteinsgade 63, 2100 København Ø
Telefon 35 45 00 00 Fax 33 37 92 91

Betænkning om restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud

Betænkning nr. 1504

København 2009

Betænkning om restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud

Betænkning nr. 1504

Publikationen kan bestilles
via Justitsministeriets hjemmeside (www.jm.dk)
eller hos
Schultz Distribution
Herstedvang 10
2620 Albertslund
Telefon: 4322 7300
Fax: 4363 1969
www.schultzboghandel.dk
schultz@shultz-Grafisk.dk

ISBN: 87-91851-60-2
ISBN: 87-91851-61-0 (internet)
Tryk: Schultz Grafisk
Pris: Kr. 100 pr. bog inkl. moms

Indholdsfortegnelse

KAPITEL 1. Indledning og sammenfatning 6
1. Indledning 6
1.1. Udvalgets nedsættelse og kommissorium 6
1.2. Udvalgets sammensætning 7
1.3. Udvalgets arbejde 7
1.4. Betænkningens opbygning 7
2. Sammenfatning af udvalgets overvejelser 9
2.1. Indledning 9
2.2. Individuel underretning af restauratøren 10
2.3. Oprettelse af et centralt register over personer med restaurationsforbud 11
2.3.1. Et centralt offentligt register 11
2.3.2. Et fælles privat register 12
2.4. Tilvejebringelse af en klar lovhjemmel for politiet til at videregive oplysninger om personer med restaurationsforbud til restauratøren 13
2.5. Forbud rettet mod restauratører 14
KAPITEL 2. Gældende ret 15
1. Restaurationsforbud 15
1.1. Forbud efter restaurationslovens § 31, stk. 2 15
1.2. Det strafbare forhold 15
1.3. Tilknytning til restaurationsbesøg 17
1.4. Tidsmæssig sammenhæng 17
1.5. Forbuddets proportionalitet 18
1.6. Forbuddets udstrækning 18
1.6.1. Den geografiske udstrækning 18
1.6.2. Forbud rettet mod restauratøren 19
1.6.3. Den tidsmæssige udstrækning 20
1.7. Håndhævelse af restaurationsforbud 20
1.7.1. Politiets rolle 20
1.7.2. Restauratørens rolle 21
1.7.2.1. Århus-modellen 22
1.8. Straf for overtrædelse af restaurationsforbud 23
2. Politiets optagelse, opbevaring og anvendelse af fingeraftryk og personfotografier i straffesager 24
2.1. Politiets optagelse af fingeraftryk og personfotografier 24
2.2. Politiets opbevaring af fingeraftryk og personfotografier 25
2.3. Politiets forevisning og offentliggørelse af fotografier mv. 26
2.4. Politiets interne forskrifter om fingeraftryk og personfotografier 27
3. Persondatalovgivningen 28
3.1. Lov om behandling af personoplysninger (persondataloven) 28
3.1.1. Baggrund 28
3.1.2. Persondatalovens anvendelsesområde 29
3.1.2.1. Direktiv 95/46/EF 29
3.1.2.2. Persondataloven 30
3.1.3. Behandlingsregler 31
3.1.3.1. Grundlæggende principper 31
3.1.3.2. Materielle behandlingsregler 33
3.1.3.3. Særlig om databeskyttelsesdirektivets regler om behandling af oplysninger om strafbare forhold 35

3.1.4. Registreredes rettigheder 36
3.1.5. Behandlingssikkerhed 38
3.1.6. Anmeldelse 38
3.1.7. Tilsyn mv. 41
3.2. Forvaltningsloven og straffeloven 42
3.3. Den Europæiske Menneskerettighedskonvention 42
KAPITEL 3. Fremmed ret 44
1. Norge 44
2. Sverige 45
3. Storbritannien 45
KAPITEL 4. Udvalgets overvejelser 47
1. Udvalgets grundlæggende overvejelser 47
1.1. Ønsket om en udvidelse af restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud 47
1.1.1. Beslutningsforslag B 112 47
1.2. Problemets omfang i praksis 48
1.2.1. Antallet af restaurationsforbud 48
1.2.2. Antallet af overtrædelser 50
1.2.3. Hvor opstår problemerne i praksis? 51
1.2.3.1. De større diskoteker 51
1.2.3.2. Forbudszoner 52
1.2.3.3. De små værtshuse og udskænkningssteder mv. 52
1.2.4. Politiets nuværende praksis vedrørende videregivelse af oplysninger 52
1.2.5. Restauratørers egen registrering af oplysninger 53
1.2.5.1. Nox Network og registreringssystemet MasterClub 53
1.2.5.2. Datatilsynets afgørelse i Crazy Daisy-sagen 55
1.2.5.3. Datatilsynets vilkår for sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger 57
2. Løsningsmodeller 60
2.1. Grundlæggende kriterier 60
2.1.1. Praktisk anvendelighed 60
2.1.2. Retssikkerhed 60
2.1.3. Persondatasikkerhed 61
2.1.4. Omkostnings- og ressourceeffektivitet 61
2.2. En decentral eller en central løsning 61
2.2.1. Den decentrale løsningsmodel 62
2.2.1.1. Grundlæggende idé 62
2.2.1.2. Hvilke oplysninger bør politiet videregive til restaurationerne ved den decentrale løsningsmodel? 63
2.2.1.2.1. Særlig om politiets videregivelse af personfotos 63
2.2.1.3. Hvordan skal videregivelse af oplysningerne ved den decentrale løsningsmodel ske 66
2.2.1.4. Hvem skal have adgang til oplysningerne 66
2.2.1.4.1. Indehavere og bestyrere 66
2.2.1.4.2. Dørmænd 67
2.2.1.4.3. Andre end næringsbrevsindehavere, bestyrere og dørmænd 68
2.2.1.5. Indførelse af en særlig tavshedspligt 70
2.2.1.6. Indførelse af særlige uddannelseskrav 70

2.2.1.7. Fordele ved den decentrale løsningsmodel 71
2.2.1.8. Ulemper ved den decentrale løsningsmodel 71
2.2.2. Centrale løsningsmodeller 72
2.2.2.1. Adgang til et centralt offentligt register med oplysninger om restaurationsforbud 72
2.2.2.1.1. Dataansvar 73
2.2.2.1.2. Registrets indhold og funktion 74
2.2.2.1.3. Hvem skal have adgang til registret 75
2.2.2.1.4. Tekniske løsningsmodeller 75
2.2.2.1.5. Biometribaseret register 76
2.2.2.1.6. CPR-baseret register 79
2.2.2.2. Oprettelse af et fælles privat register med oplysning om restaurationsforbud 80
2.2.2.2.1. Dataansvar 81
2.2.2.2.2. Registrets indhold 81
2.2.2.2.3. Hvem skal have adgang til registret 82
2.2.2.2.4. Registrets funktion 82
2.2.2.2.4.1. Registrering af oplysninger om interne karantæner mv. 83
2.2.2.2.4.2. Udveksling af oplysninger om restaurationsforbud og karantæner 83
2.2.2.2.4.4. Oplysninger fra politiet 84
2.2.2.3. Fordele ved de centrale løsningsmodeller 84
2.2.2.3.1. Generelt 84
2.2.2.3.2. Fordele ved et centralt offentligt register 85
2.2.2.3.3. Fordele ved et fælles privat register 85
2.2.2.4. Ulemper ved de centrale løsningsmodeller 85
2.2.2.4.1. Generelt 85
2.2.2.4.2. Ulemper ved et centralt offentligt register 86
2.2.2.4.3. Ulemper ved et fælles privat register 86
3. Udvalgets konklusioner 87
3.1. Alle restaurationer skal have adgang til oplysninger om restaurationsforbud 87
3.2. Der bør tilvejebringes en klar hjemmel for politiet til at videregive identitetsoplysninger til de berørte restaurationer 88
3.3. Individuel skriftlig underretning af berørte restaurationer 88
3.4. Tavshedspligt mv. 89
3.5 Ensretning af politiets praksis vedrørende meddelelse af restaurationsforbud til restauratører 90
3.6. Behovet for en central løsning 90
3.6.1. Et centralt offentligt register 91
3.6.2. Et fælles privat register 92
3.6.2.1. Politiets videregivelse af oplysninger til det fælles private register 93
3.6.2.2. Sikkerhed og tavshedspligt mv. 93
KAPITEL 5. Udkast til forslag til lov om ændring af lov om restaurations- og hotelvirksomhed mv. (Videregivelse og behandling af oplysninger om restaurationsforbud) 95
1. Lovudkast 95
2. Bemærkninger til lovudkastets enkelte bestemmelser 97
BILAG 100

KAPITEL 1. Indledning og sammenfatning

1. Indledning

1.1. Udvalgets nedsættelse og kommissorium

I sommeren 2008 nedsatte justitsministeren et sagkyndigt udvalg med repræsentation fra berørte myndigheder og organisationer, herunder restaurationsbranchen, som skulle foretage en samlet gennemgang og vurdering af, hvordan restaurationer mv. sikres adgang til identitetsoplysninger på personer med restaurationsforbud, uden at en sådan adgang til personfølsomme oplysninger om enkeltpersoner sætter grundlæggende hensyn til persondatabeskyttelsen over styr.

Nedsættelsen af udvalget skete på baggrund af Folketingets Retsudvalgs beretning af 1. oktober 2007 over beslutningsforslag nr. B 112 (Folketingstidende 2006-07, Tillæg B, side 1783).

Udvalgets opgaver blev i kommissoriet beskrevet således:

> ”Udvalget skal overveje, hvordan restaurationer mv. kan sikres adgang til identitetsoplysninger på personer med restaurationsforbud.
>
> Udvalget anmodes i den forbindelse om at overveje mulighederne for at registrere personer, der er meddelt restaurationsforbud, i et særskilt register, som i fornødent omfang kan stilles til rådighed for restauratører og dørmænd mv. Udvalget skal i den forbindelse gennemgå og vurdere de praktiske og retlige spørgsmål, som dette giver anledning til, herunder med hensyn til persondatabeskyttelse.
>
> Udvalget anmodes om at komme med forslag til ordningens nærmere praktiske og retlige udformning og gennemførelse.
>
> Udvalget skal i den forbindelse overveje, om en ordning af nævnte karakter kræver lovgivning. Hvis udvalget finder, at der er et sådant behov, anmodes udvalget om at udarbejde et lovudkast.
>
> Udvalget anmodes om så vidt muligt at færdiggøre sit arbejde inden udgangen af 2008, så der i givet fald kan gennemføres lovgivning i folketingsåret 2008-09.
>
> Medlemmerne af udvalget udpeges af justitsministeren […].

Udvalget vil kunne inddrage organisationer og personer med særlig indsigt på området i arbejdet."

1.2. Udvalgets sammensætning

Udvalget har haft følgende sammensætning:

Landsdommer Henrik Estrup, Vestre Landsret (formand)
Kontorchef Barbara Bertelsen, Justitsministeriet
Professor dr.jur. Peter Blume, Københavns Universitet
Kontorchef Jytte Tandrup Christensen, Erhvervs- og Selskabsstyrelsen
Advokatfuldmægtig Martin Jørgensen, Dansk Erhverv
Afdelingschef Birgit Kleis, Rigspolitiet
Direktør Lars Orlamundt, Horesta
Juridisk konsulent Christel Petersen, Kommunernes Landsforening
Advokat Hanne Rahbæk, Advokatrådet
Direktør Kasper Skov-Mikkelsen, Sikkerhedsbranchen

Fuldmægtig Rasmus Kieffer-Kristensen, Justitsministeriet, har varetaget hvervet som sekretær i forbindelse med udarbejdelsen af betænkningen.

1.3. Udvalgets arbejde

Udvalget har afholdt 5 møder og afgiver denne betænkning i enighed.

1.4. Betænkningens opbygning

I kapitel 1, afsnit 2, findes en sammenfatning af udvalgets overvejelser.

I kapitel 2 redegøres for gældende ret med hensyn til udstedelse og håndhævelse af restaurationsforbud. Der redegøres endvidere for de gældende regler om politiets optagelse, opbevaring og anvendelse af fingeraftryk og personfotografier i straffesager, idet disse regler har været af betydning for udvalgets overvejelser. Endelig redegøres for de relevante regler i persondatalovgivningen, forvaltningsloven, straffeloven og Menneskerettighedskonventionen, idet udvalgets forslag skal være forenelig med disse regler.

I kapitel 3 redegøres for fremmed ret.

I kapitel 4 redegøres for udvalgets overvejelser.

I kapitel 5 findes udvalgets forslag til ændring af restaurationsloven.

I betænkningen er medtaget en række bilag.

Et enigt udvalg afgiver herved betænkningen til justitsministeren.

København, den 12. marts 2009

Henrik Estrup (formand)	Barbara Bertelsen	Peter Blume
Jytte Tandrup Christensen	Martin Jørgensen	Birgit Kleis
Lars Orlamundt	Christel Petersen	Hanne Rahbæk
Kasper Skov-Mikkelsen		

Rasmus Kieffer-Kristensen

2. Sammenfatning af udvalgets overvejelser

2.1. Indledning

I medfør af restaurationslovens § 31, stk. 2, kan politiet forbyde personer, som i forbindelse med restaurationsbesøg har begået en strafbar handling, at opholde sig som gæster i bestemte virksomheder. De "virksomheder", der er tale om, er restaurationer i vid forstand, jf. restaurationslovens § 1, herunder værtshuse, diskoteker, natklubber mv.

De nærmere betingelser for, at politiet kan udstede et restaurationsforbud, og reglerne om restaurationsforbuds tidsmæssige og geografiske udstrækning mv., er gennemgået i kapitel 2.

Udvalgets opgave har bestået i at undersøge, hvordan det kan sikres, at en restauration får oplysning om det, når en person får et restaurationsforbud, og hvordan denne oplysning bedst kan gives.

Udvalget har taget udgangspunkt i en opfattelse af, at alle restaurationer uanset deres karakter, størrelse og geografiske placering bør have adgang til at få det at vide, når en person har fået et forbud efter restaurationsloven mod at komme det pågældende sted. Udvalget har herved lagt vægt på, at restaurationerne i praksis spiller en vigtig rolle i forbindelse med håndhævelsen af restaurationsforbud, herunder gennem adgangskontrollen på diskoteker og natklubber mv.

Udvalget har med dette udgangspunkt overvejet fordele og ulemper ved både en individuel underretningsordning, hvor oplysninger om restaurationsforbud sendes direkte til de berørte restaurationer, og ved en central registerordning, hvor oplysninger om restaurationsforbud stilles til rådighed for de restaurationer, der er tilsluttet registret. Udvalget anbefaler, som det fremgår af det følgende, en kombination af de to ordninger:

2.2. Individuel underretning af restauratøren

Efter udvalgets opfattelse bør politiet ved en individuel underretning orientere den eller de berørte restaurationer, når en person får et restaurationsforbud. Underretningen bør ske skriftligt, jf. nærmere kapitel 4, afsnit 2.2.1.3. En restauratør skal dog kunne fravælge at få individuel underretning, hvis restaurationen er tilsluttet et centralt register med oplysning om restaurationsforbud, jf. nedenfor.

Udvalget har ved anbefalingen af, at politiet skal give en restauration individuel underretning, når en person af politiet har fået forbud mod at komme der, lagt vægt på, at mange restaurationer ikke kan antages at have noget ønske om at blive tilsluttet et centralt elektronisk register, og at der derfor – uanset om der indføres et sådant register – vil være behov for, at de modtager oplysninger om restaurationsforbud direkte fra politiet

Der er i dag forskelle i den måde, hvorpå politiet orienterer en restauration, når politiet har givet en gæst forbud mod at komme på stedet. Udvalget forslår derfor, at der sker en ensretning af politiets underretningsprocedurer. Der henvises til kapitel 4, afsnit 3.5.

En oplysning om, at en person har fået et restaurationsforbud, er en fortrolig oplysning, idet en person kun kan få et restaurationsforbud, hvis vedkommende har begået (er sigtet for) et strafbart forhold. De oplysninger, som politiet efter forslaget skal give en restauration, når en person har fået forbud mod at komme der, bør derfor begrænses mest muligt. Udvalget foreslår på den baggrund, at politiet skal give restaurationen oplysning om den pågældendes navn og CPR-nummer og om forbuddets tidsmæssige udstrækning. Det kan derimod ikke anses for nødvendigt, at restaurationen f.eks. får oplysning om karakteren af den lovovertrædelse, der har ført til restaurationsforbuddet. Der henvises til kapitel 4, afsnit 2.2.1.2.

Oplysningerne skal efter forslaget gives til næringsbrevsindehaveren eller bestyreren, idet det er vigtigt, at der er en fysisk person i restaurationen, som er ansvarlig for den videre behandling af oplysningerne. Næringsbrevsindehaveren eller bestyreren vil

kunne videregive oplysningerne til restaurationens dørmænd og i fornødent omfang til andre ansatte, jf. nærmere kapitel 4, afsnit 2.2.1.4.

Udvalget foreslår, at der indføres særlige regler om tavshedspligt mv. med hensyn til de oplysninger, der modtages fra politiet, jf. nærmere kapitel 4, afsnit 3.4.

2.3. Oprettelse af et centralt register over personer med restaurationsforbud

Udvalget har overvejet, om der – udover den individuelle underretning af restauratøren, der er omtalt oven for – bør oprettes et centralt register over personer med restaurationsforbud, som den enkelte restauration kan få online adgang til i forbindelse med sin adgangskontrol.

Efter udvalgets opfattelse vil der for en række restaurationers vedkommende – herunder navnlig større diskoteker og natklubber – være væsentlige fordele forbundet med at oprette et sådant centralt register. Restaurationerne slipper derved for selv at skulle registrere de personer, der har forbud mod at komme i restaurationen. En del restaurationer har endvidere i forvejen gæsteregistreringssystemer mv., som vil kunne anvendes i tilknytning til et centralt register. Om fordelene ved at oprette et centralt register over personer med restaurationsforbud henvises i øvrigt til kapitel 4, afsnit 2.2.2.3.

Et centralt register vil kunne oprettes både som et centralt offentligt register og som et centralt (fælles) privat register. De to former for centrale registre omtales i det følgende:

2.3.1. Et centralt offentligt register

Et centralt offentligt register vil mest nærliggende skulle føres af Rigspolitiet, da det er politiet, der er i besiddelse af oplysningerne om udstedte restaurationsforbud.

Udvalget har overvejet, om et centralt offentligt register vil kunne baseres på elektroniske fingeraftryk som identifikation, men har afvist denne mulighed, jf. kapitel 4, afsnit 2.2.2.1.5. Da det heller ikke vil være muligt at lade et centralt offentligt register indeholde et foto af personer, der har fået et restaurationsforbud, jf. herved kapitel 4, afsnit 2.2.1.2.1, vil et centralt offentligt register i stedet skulle baseres på CPR-numre,

hvilket dog ville give anledning til betydelige kontrolproblemer. Det skyldes, at det vil være vanskeligt for restaurationerne at sikre, at det CPR-nummer, som en gæst oplyser, rent faktisk er det rigtige, eller at et sygesikringskort mv., der fremvises eller køres gennem en kortlæser ved adgangskontrollen, er vedkommendes eget kort og ikke et kort, som vedkommende har lånt eller stjålet.

Udvalget kan derfor og i øvrigt af de grunde, der er anført i kapitel 4, afsnit 2.2.2.1.1., ikke anbefale, at der etableres et centralt offentligt register over personer med restaurationsforbud. Der henvises også til kapitel 4, afsnit 3.6.1.

2.3.2. Et fælles privat register

Udvalget anbefaler i stedet, at der oprettes et fælles privat register, hvor de restaurationsvirksomheder, som ønsker det, kan få oplyst, om en bestemt person har restaurationsforbud det pågældende sted. Efter udvalgets opfattelse vil det være nærliggende at lade branchen selv stå for oprettelsen og driften af registret.

En væsentlig fordel ved et sådant fælles privat register vil være, at det – i modsætning til et centralt offentligt register – udover navn og CPR-nummer med samtykke fra gæsten også vil kunne indeholde billeder, fingeraftryk (såkaldte templates) og andre identitetsoplysninger, som kan anvendes til at sikre en hurtig, effektiv og ensartet adgangskontrol. Når restaurationen i forbindelse med adgangskontrollen anvender det fælles private register for at få svar på, om en person har et restaurationsforbud det pågældende sted, vil det således være muligt at sammenholde det CPR-nummer, som gæsten oplyser, med det foto eller fingeraftryk af den pågældende, som findes i systemet, hvorved mulighederne for at snyde ved hjælp af et forkert CPR-nummer eller fremvisning af et lånt eller stjålet sygesikringsbevis minimeres.

En anden ikke uvæsentlig fordel ved et fælles privat register vil være, at det – efter omstændighederne – også vil kunne anvendes til at registrere oplysninger om interne karantæner til gæster på grund af dårlig opførsel mv.

Registret vil kunne indrettes, så det i vidt omfang er kompatibelt med de gæsteregistreringssystemer, som en del restaurationer, navnlig større diskoteker og natklubber

mv., har i forvejen. Disse restaurationer vil herefter via deres eget system kunne søge i det fælles private registers oplysninger om restaurationsforbud.

Det vil ved anvendelse af det fælles private register alene være muligt for en restauration at få oplysning om, hvorvidt den person, der søges på, har forbud mod at komme i netop denne restauration. Det skal således ikke være muligt generelt at få oplysning om, hvorvidt en bestemt person har forbud mod at komme i en eller anden restauration. Det skyldes, at registret ellers vil få karakter af et såkaldt advarselsregister, hvilket ikke vil være i overensstemmelse med persondataloven. Tilsvarende skal restauratøren kun have adgang til oplysninger om interne karantæner, der vedrører den pågældende restauration.

Et fælles privat register med identitetsoplysninger på personer med restaurationsforbud vil skulle anmeldes til Datatilsynet og i øvrigt være i overensstemmelse med de krav, der følger af persondatalovgivningen og Datatilsynets vilkår m.v.

Det vil være en forudsætning, at Rigspolitiet udarbejder en teknisk løsning, som sikrer, at der fra politiets registre til det fælles private register løbende og i elektronisk form overføres opdaterede oplysninger om, hvilke personer der er omfattet af restaurationsforbud, og hvilke restaurationer forbuddene vedrører.

Som påpeget af repræsentanterne for Horesta og Dansk Erhverv vil det kunne overvejes, om det offentlige herudover bør yde økonomisk tilskud til etableringen af det fælles private register, da det også er i det offentliges interesse, og da der kan opstå risiko for, at etableringsudgifterne ellers bliver for høje for den enkelte restauration.

Der henvises i øvrigt til kapitel 4, afsnit 2.2.2.2. og 3.6.2.

2.4. Tilvejebringelse af en klar lovhjemmel for politiet til at videregive oplysninger om personer med restaurationsforbud til restauratøren

Restaurationsloven indeholder i dag ikke nogen klar hjemmel til, at politiet kan videregive oplysninger herom til restauratøren, når en person har fået et forbud mod at opholde sig som gæst i den pågældende restauration.

Udvalget finder, at der bør tilvejebringes en sådan klar hjemmel ved, at der i restaurationsloven indsættes en bestemmelse om, at politiet kan videregive oplysninger til næringsbrevsindehavere og bestyrere om, hvilke personer der har fået forbud efter restaurationsloven mod at opholde sig i den pågældende restauration. Det lovudkast, som udvalget har udarbejdet, findes i kapitel 5.

2.5. Forbud rettet mod restauratører

Efter restaurationslovens § 31, stk. 2, kan politiet ud over at forbyde en *gæst* at komme på en bestemt restauration give en *restauratør* forbud mod at modtage en bestemt person som gæst.

Der er i dag forskellig praksis i politikredsene med hensyn til at meddele forbud til restauratører. I nogle politikredse gives sådanne forbud stort set aldrig, mens der i andre kredse som udgangspunkt både meddeles forbud til gæsten og til restauratøren.

Udvalget foreslår, at politiets praksis vedrørende meddelelse af restaurationsforbud til restauratører ensrettes. Der henvises til kapitel 4, afsnit 3.5.

KAPITEL 2. Gældende ret

1. Restaurationsforbud

1.1. Forbud efter restaurationslovens § 31, stk. 2

Efter restaurationslovens § 31, stk. 2, kan politiet forbyde en person, der i forbindelse med restaurationsbesøg har begået en strafbar handling, at opholde sig som gæst i bestemte restaurationsvirksomheder (restaurationsforbud).

Forbuddet kan meddeles efter anmodning fra restauratøren, men også på politiets eget initiativ. Afgørelsen træffes på grundlag af en konkret vurdering af de oplysninger, der indgår i sagen.

1.2. Det strafbare forhold

Meddelelse af forbud forudsætter ikke, at der er begået flere strafbare handlinger i forbindelse med restaurationsbesøg. Ved lov nr. 1084 af 10. december 2002 blev restaurationslovens § 31, stk. 2, præciseret, således at det nu klart fremgår, at der er mulighed for at meddele et forbud allerede første gang, der konstateres en strafbar handling i forbindelse med restaurationsbesøg.

Det er efter restaurationslovens § 31, stk. 2, en betingelse for at meddele et forbud, at der i forbindelse med restaurationsbesøg er begået en strafbar handling. Det er dog ikke en forudsætning, at det strafbare forhold, som ligger til grund for forbuddet, er fastslået ved dom. Et forbud kan således meddeles, når den pågældende er sigtet for en strafbar handling i forbindelse med restaurationsbesøg.

Justitsministeriet (som indtil 2007, hvor opgaven overgik til Rigspolitiet, var rekursinstans i klagesager vedrørende meddelelse af restaurationsforbud) har ophævet forbud, hvor den sigtelse, som lå til grund for forbuddet, af bevismæssige årsager blev frafaldet, idet ministeriet i disse tilfælde ikke fandt, at det med tilstrækkelig sikkerhed kunne fastslås, at der var begået et strafbart forhold.

Det fremgår af forarbejderne til restaurationslovens § 31, stk. 2, at det er en forudsætning for at meddele et forbud mod at opholde sig som gæst i en bestemt restauration, at det må anses for nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden.

Bemærkningerne til forslaget til restaurationslovens § 31, stk. 2, må antages at forudsætte, at et forbud skal være nødvendiggjort af en forventning om, at den pågældende person i fremtiden vil forstyrre ro og orden i den konkrete restauration, såfremt vedkommende ikke meddeles forbud mod at tage ophold i restaurationen.

Bemærkningerne må endvidere antages at forudsætte, at ikke alle strafbare forhold begået i en restauration kan danne grundlag for et restaurationsforbud. Det er således ikke i sig selv tilstrækkeligt, at der er begået et strafbart forhold i en restauration. Det strafbare forhold skal tillige have en sådan tilknytning til eller sammenhæng med restaurationsbesøget, at det er nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden i restaurationen at meddele et forbud på baggrund af overtrædelsen. Der skal være tale om strafbare handlinger, som typisk begås i restaurationsmiljøet, eller som det er vigtigt at modvirke særligt i restaurationsmiljøet.

Justitsministeriet har i en konkret klagesag ophævet et restaurationsforbud, som var meddelt på baggrund af, at den pågældende var sigtet for overtrædelse af straffelovens § 279 ved i restaurationen at have forsøgt at benytte et stjålet dankort, idet ministeriet ikke fandt, at det strafbare forhold var af en sådan karakter, at det af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden i restaurationen var nødvendigt at meddele den pågældende et forbud efter restaurationsloven.

I praksis anvendes restaurationsforbud typisk i forbindelse med overtrædelse af våbenlovgivningen, overtrædelse af lov om euforiserende stoffer, vold samt overtrædelse af restaurationslovens § 32, stk. 1 (om støjende, voldelig, fornærmelig eller lignende adfærd, der er egnet til at forstyrre den offentlige orden eller medføre ulempe for andre tilstedeværende eller omboende), jf. herved også kapitel 4, afsnit 1.2.

For så vidt angår besiddelse af euforiserende stoffer må der foretages en konkret vurdering af bl.a. karakteren af den pågældende restaurationsvirksomhed for at fastslå,

om der er grundlag for et restaurationsforbud af hensyn til lovlighed, ædruelighed og opretholdelse af ro og orden. Dette indebærer, at der i situationer, hvor det strafbare forhold består i besiddelse af euforiserende stoffer, skal anlægges en vurdering af, om det i forhold til den konkrete restaurationsvirksomhed er nødvendigt at meddele et forbud. Besiddelse af euforiserende stoffer til eget forbrug, hvor de euforiserende stoffer ikke kan antages at være bestemt til at blive indtaget i forbindelse med restaurationsbesøget, vil således ikke i alle tilfælde kunne danne grundlag for et forbud efter restaurationsloven. I vurderingen af, om et forbud er nødvendigt i relation til den konkrete restaurationsvirksomhed, skal indgå karakteren af den pågældende restauration, omstændighederne i forbindelse med besiddelsen, samt om der er tale om en restaurationsvirksomhed, hvor der ofte konstateres overtrædelser af lov om euforiserende stoffer.

En vurdering af baggrunden for og karakteren af det strafbare forhold vil kunne føre til, at kravet om, at forbuddet skal være nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden, ikke kan anses for at være opfyldt, idet der ikke foreligger det fornødne grundlag for at antage, at den pågældende i fremtiden generelt vil forstyrre ro og orden i forbindelse med restaurationsbesøg.

1.3. Tilknytning til restaurationsbesøg

Det strafbare forhold skal have en vis nær og umiddelbar tilknytning til et restaurationsbesøg for at kunne danne grundlag for udstedelse af et forbud efter restaurationsloven.

Også strafbare forhold begået uden for en restaurationsvirksomhed kan dog danne grundlag for meddelelsen af et forbud efter restaurationsloven, blot det strafbare forhold har tilknytning til restaurationsbesøget. Der kan for eksempel være tale om strafbare forhold begået i køen til restaurationen eller strafbare forhold, som udspringer af en episode inde i restaurationen.

1.4. Tidsmæssig sammenhæng

Det skal være aktuelt nødvendigt at udstede et forbud, hvilket må antages at forudsætte, at et forbud skal udstedes i en vis tidsmæssig sammenhæng med det strafbare forhold, som ligger til grund for forbuddet.

1.5. Forbuddets proportionalitet

En afgørelse om udstedelse af et forbud efter restaurationslovens § 31, stk. 2, skal være i overensstemmelse med det forvaltningsretlige proportionalitetsprincip.

Det kan i den forbindelse nævnes, at Folketingets Ombudsmand i en udtalelse, som er optrykt i Folketingets Ombudsmands Beretning, 1986, s. 82, i forbindelse med en konkret sag har anført, at et restaurationsforbud generelt må anses som et indgreb af ringe intensitet i forhold til adressaten.

Et forbud, der udstrækkes til at omfatte flere restaurationer (såkaldte "zoneforbud"), jf. kapitel 2, afsnit 1.6.1. nedenfor, må dog anses for forholdsvis mere indgribende over for den pågældende, særligt hvor forbuddet omfatter størstedelen af restaurationerne i en by, således at forbuddet får karakter af en generel udelukkelse fra at deltage i byens restaurations- og natteliv.

Det må derfor også antages, at en vurdering af grovheden af det begåede strafbare forhold vil kunne føre til, at et forbud ikke kan udstrækkes til at omfatte andre restaurationer end den, hvor det strafbare forhold er begået.

1.6. Forbuddets udstrækning

1.6.1. Den geografiske udstrækning

Der er efter praksis ikke grundlag for at antage, at det strafbare forhold, som ligger til grund for forbuddet, nødvendigvis skal være begået i den eller de restaurationer, som forbuddet vedrører. Der er således mulighed for at udstede forbud, som omfatter andre restaurationsvirksomheder end den virksomhed, hvor det strafbare forhold er begået.

Et sådant bredere restaurationsforbud er i praksis bl.a. udstedt i tilfælde, hvor de restaurationer, som forbuddet gælder, er placeret inden for et snævert geografisk område – ofte side om side og med en tæt trafik af gæster mellem de forskellige restaurationer – eller hvor der er tale om restaurationer af samme karakter, som ligger inden for et begrænset geografisk område. For at kunne opnå den ønskede effekt af et forbud er

det i sådanne tilfælde således ofte nødvendigt at udstrække forbuddet til at omfatte alle restaurationer i området ("zoneforbud").

De nærmere betingelser for at udstrække et restaurationsforbud til at omfatte flere restaurationer er beskrevet i Justitsministeriets cirkulæreskrivelse af 21. december 2006, der er medtaget som bilag 1 til denne betænkning.

Rigspolitiet har oplyst, at man bl.a. hos Nordjyllands Politi har haft positive erfaringer med anvendelsen af "zoneforbud", hvilket har haft en øget præventiv effekt og har været medvirkende til et tryggere natteliv i Aalborgs bymidte. I øjeblikket er et betydelig antal personer således omfattet af restaurationsforbud, som gælder for både restaurationerne i Jomfru Ane Gade og de nærmeste omkringliggende gader i Aalborg bymidte, som i denne forbindelse betragtes som et samlet restaurationsmiljø. Der er for øjeblikket 41 restaurationer på denne forbudsliste, som alle er beliggende inden for en radius af ca. 200 meter fra Jomfru Ane Gade.

1.6.2. Forbud rettet mod restauratøren

Politiet har i dag mulighed for – i tilknytning til at en person er blevet meddelt et restaurationsforbud – tillige at meddele en restauratør forbud mod at modtage vedkommende som gæst, jf. restaurationslovens § 31, stk. 2, 2. pkt.

Der er i politikredsene forskellig praksis med hensyn til at meddele forbud til restauratører. I nogle politikredse gives stort set aldrig forbud til restauratøren, mens andre kredse som udgangspunkt meddeler forbud til såvel gæst som restauratør. I de sidstnævnte tilfælde er en væsentlig begrundelse for også at meddele forbud til restauratøren, at der herved gives denne en legitim adgang til at bortvise gæsten. Endvidere anvendes muligheden for at give restauratøren et forbud i tilfælde, hvor restauratøren tillader en gæst at opholde sig i restaurationen, uanset at restauratøren er bekendt med, at den pågældende er meddelt et restaurationsforbud.

1.6.3. Den tidsmæssige udstrækning

Restaurationslovens § 31, stk. 2, tager ikke stilling til den tidsmæssige udstrækning af forbud, som meddeles efter bestemmelsen. Det må dog forudsættes, at forbuddets tidsmæssige udstrækning skal begrænses til den periode, hvor forbuddet efter en konkret vurdering må anses for at være nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden på restaurationen.

I praksis udstedes et forbud efter restaurationsloven oftest for 2 år.

1.7. Håndhævelse af restaurationsforbud

1.7.1. Politiets rolle

Spørgsmålet om politiets rolle i forbindelse med håndhævelsen af restaurationsforbud efter restaurationslovens § 31, stk. 2, er ikke nærmere reguleret i restaurationsloven.

Det følger dog af politilovens § 2, at politiet bl.a. har til opgave at bringe strafbar virksomhed til ophør, efterforske og forfølge strafbare forhold samt at forebygge og afværge forstyrrelse af den offentlige fred og orden.

Rigspolitiet har oplyst, at politikredsene generelt prioriterer indsatsen for ro og tryghed i nattelivet højt. Politiet har bl.a. betydeligt fokus på den kriminalitet, som begås af rockere og kriminelle bander, herunder i restaurationsmiljøet, og der er i relation til disse grupperinger udarbejdet særlige strategier og initiativer for den politimæssige indsats. Politiet har også udarbejdet en strategi for indsatsen over for løst organiserede grupper af utilpassede unge, som giver anledning til uro og utryghed i lokalområderne, bl.a. i nattelivet.

I de fleste politikredse findes endvidere specialpatruljer, som særligt i weekenden patruljerer i restaurations- og nattelivsmiljøet. Blandt deres opgaver vil bl.a. være at kontrollere, om restaurationsforbud overholdes.

1.7.2. Restauratørens rolle

Restauratørens rolle i forbindelse med håndhævelse af restaurationsforbud meddelt til en gæst i medfør af restaurationslovens § 31, stk. 2, 1. pkt., er ikke nærmere beskrevet i restaurationsloven.

Det må dog antages, at restaurationsvirksomheder har en almindelig pligt til at sikre, at der ikke kommer uromagere og lignende ind på deres restaurationer. Denne pligt kan bl.a. udledes af forarbejderne til restaurationslovens § 19, hvoraf det fremgår, at en mangelfuld kontrol ved døren kan medføre fratagelse af alkoholbevillingen.

Det er endvidere anført i forarbejderne til ændringsloven fra 2002, at restauratøren har en pligt til at medvirke til restaurationsforbuds efterlevelse i det omfang, restauratøren kan identificere den pågældende og er bekendt med, at et forbud er meddelt.

Hvor langt denne forpligtelse rækker er dog uklart. Der vil således næppe kunne statueres strafansvar over for en restauratør, som uagtsomt eller forsætligt medvirker til, at en gæst, der er omfattet af et restaurationsforbud, jf. restaurationslovens § 31, stk. 2, 1. pkt., får adgang til restaurationen.

Det bemærkes i øvrigt, at det forhold, at restaurationsloven ikke indeholder nogen klar regel om, at politiet skal – eller må – videregive oplysninger til restauratører om, at en person er meddelt et forbud mod at opholde sig som gæst i restaurationen, også synes at underbygge, at restauratøren oprindelig kun er tiltænkt en begrænset rolle i forhold til håndhævelsen af restaurationsforbuddet.

I tilfælde, hvor politiet bliver bekendt med, at restauratøren tillader en gæst at opholde sig i restaurationen, uanset at restauratøren ved, at den pågældende er omfattet af et restaurationsforbud, kan der – som omtalt under afsnit 1.6.2. ovenfor - meddeles restauratøren et særskilt forbud mod at modtage vedkommende som gæst, jf. restaurationslovens § 31, stk. 2, 2. pkt. Overtrædelse af et sådant forbud kan straffes efter restaurationslovens § 37, stk. 1, nr. 3, jf. afsnit 1.8. nedenfor.

1.7.2.1. Århus-modellen

Et eksempel på, hvordan restaurationsvirksomheder kan bistå politiet i forbindelse med retshåndhævelsen i nattelivet, kendes fra Østjyllands Politi, hvor politiet i 2006 indførte den såkaldte "Århus-model" som reaktion på narkotikaproblemer på særligt ét diskotek i Århus.

"Århus-modellen", som i dag bl.a. er indført på 5 diskoteker i Århus, indebærer, at personale på diskoteker mv. tilbageholder narkotiske stoffer, som en gæst er fundet i besiddelse af, og overleverer dette til politiet i forbindelse med en anmeldelse af gæsten til politiet.

Modellen skal ses i lyset af, at personalet på diskotekerne ikke sjældent bliver opmærksom på personer, som er i besiddelse af narkotiske stoffer, idet de ofte afslører sig selv ved at tabe stofferne i forbindelse med betaling af entré eller ved betaling i baren. Hertil kommer tilfælde, hvor f.eks. to personer benytter det samme toilet.

Såfremt personale finder narkotiske stoffer hos en gæst, bliver denne bedt om at udlevere stoffet til personalet og om at følge med til kontoret, hvor den pågældende bliver bedt om at oplyse sin identitet og om at underskrive en blanket, der er udarbejdet af politiet. Den oplyste identitet bliver desuden kontrolleret ved opringning til politiets vagtcentral. Blanketten bliver sammen med stoffet, der placeres i aflåste skabe i særlige poser fra politiet, efterfølgende overgivet til politiet, der foretager den politimæssige behandling af sagen.

Både ledelse og personale på de pågældende diskoteker mv. har modtaget grundig instruktion fra politiet i, hvordan de skal forholde sig over for gæster, som mistænkes for besiddelse af narkotika. Østjyllands Politi har endvidere udarbejdet en vejledning til brug for personalet.

Østjyllands Politi vurderer, at erfaringerne med anvendelse af "Århus-modellen" overordnet er positive.

Siden indførelsen af modellen i 2006 har Østjyllands Politi modtaget ca. 80 anmeldelser, hvor modellen har været anvendt. Personalet på de relevante diskoteker mv. har

ikke haft problemer med at få gæster til at udlevere de narkotiske stoffer eller med at få gæsterne til at oplyse deres rette identitet. Hertil kommer, at ingen af de anmeldte personer efterfølgende har nægtet det påsigtede forhold i forbindelse med politiafhøring.

1.8. Straf for overtrædelse af restaurationsforbud

Efter restaurationslovens § 37, stk. 1, nr. 3, er straffen for overtrædelse af et restaurationsforbud meddelt i henhold til § 31, stk. 2, bøde. Under skærpende omstændigheder eller i gentagelsestilfælde kan straffen stige til fængsel indtil 4 måneder, jf. § 37, stk. 2.

Forud for 2007 var der ikke fastsat vejledende bødetakster for overtrædelse af restaurationsforbud efter § 31, stk. 2. Sager om overtrædelse af forbud efter § 31, stk. 2, blev indtil da typisk afgjort med bøder i niveauet 500 - 1.500 kr.

I Rigsadvokatens Meddelelse nr. 6/2007 af 12. juli 2007 er det – bl.a. i lyset af den øgede fokus på tryghed i nattelivet – fastsat, at anklagemyndigheden i sager om førstegangsovertrædelser af § 31, stk. 2, skal nedlægge påstand om en bøde på 1.500 kr., hvor der ikke foreligger skærpende omstændigheder. Bødeniveauet svarer bl.a. til bødeniveauet anvendt ved Retten i Ålborg.

Hvis der foreligger skærpende omstændigheder – f.eks. hvis vedkommende er til gene for personalet eller andre gæster, uden at dette er en overtrædelse af andre bestemmelser i straffeloven eller restaurationsloven mv. – skal bødepåstanden være 2.000 kr.

Bøden skal ifølge Rigsadvokaten søges forhøjet i gentagelsestilfælde, således at bøden i 2. gangstilfælde forhøjes med 500 kr. og i tredjegangs- og senere tilfælde med 1.000 kr. i forhold til bøden i førstegangstilfælde.

Vedrørende antallet af personer, der sigtes for overtrædelse af forbud henvises til kapitel 4, afsnit 1.2.2.

2. Politiets optagelse, opbevaring og anvendelse af fingeraftryk og personfotografier i straffesager

2.1. Politiets optagelse af fingeraftryk og personfotografier

Reglerne om foretagelse af legemsindgreb i forbindelse med efterforskning af straffesager findes i retsplejelovens kapitel 72.

Der sondres i retsplejeloven mellem legemsbesigtigelse (retsplejelovens § 792, stk. 1, nr. 1) og legemsundersøgelse (retsplejelovens § 792, stk. 1, nr. 2). Sondringen bygger på en vurdering af indgrebenes intensitet.

Optagelse af fingeraftryk og personfotografi er omfattet af reglerne om legemsbesigtigelse.

Efter retsplejelovens § 792 a, stk. 1, må legemsbesigtigelse af en sigtet kun foretages, såfremt den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og såfremt indgrebet må antages at være af væsentlig betydning for efterforskningen.

Herudover kan der optages fingeraftryk og personfotografi med henblik på senere identifikation, såfremt den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, eller for en overtrædelse af straffelovens § 235, stk. 2 (børnepornografi), jf. § 792 b, stk. 1.

Der kan endvidere i forbindelse med en efterforskning optages fingeraftryk og personfotografi af en person, der ikke er sigtet, hvis den pågældende meddeler samtykke hertil, jf. § 792 d, stk. 1 Samtykket skal så vidt muligt være skriftligt

Endelig kan optagelse af fingeraftryk og personfotografi af en ikke-sigtet person, der ikke har givet samtykke hertil, foretages, såfremt det er af afgørende betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover, jf. § 792 d, stk. 2.

Afgørelse om optagelse af fingeraftryk og fotografering træffes almindeligvis af politiet, jf. § 792 c, med adgang til domstolsprøvelse efter § 746, stk. 1. Dog træffer retten afgørelse om optagelse af fingeraftryk og personfotografi af en ikke-sigtet person, der ikke har givet samtykke hertil, jf. § 792 d, stk. 3.

Det følger af den almindelige proportionalitetsgrundsætning, som vedrørende legemsindgreb er fastslået i retsplejelovens § 792 e, stk. 1, at legemsindgreb ikke må foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og det ubehag, som indgrebet må antages at forvolde, ville være et uforholdsmæssigt indgreb.

2.2. Politiets opbevaring af fingeraftryk og personfotografier

De fingeraftryk, som politiet optager i medfør af retsplejelovens kapitel 72, opbevares i Fingeraftryksregistret, som administreres af Rigspolitiet. Oplysningerne om en registreret person skal slettes, når personen fylder 80 år, medmindre der er særlige forhold, der gør det nødvendigt at opbevare oplysningerne i længere tid.

Politiets opbevaring af personfotografier er indirekte reguleret i § 792 f. Det følger af denne bestemmelse, at politiet ikke må opbevare personfotografier med henblik på senere identifikation af personer, der ikke har været sigtet, eller som er frifundet, eller mod hvem påtale er opgivet. Fotografier, der er tilvejebragt ved indgreb, som retten i medfør af § 746, stk. 1, finder uhjemlede, skal straks tilintetgøres, jf. § 792 f, stk. 3.

Et personfotografi af sigtede, der er optaget i forbindelse med efterforskningen af et forhold, som den sigtede senere frifindes for, eller hvor påtale opgives, skal således destrueres, også selv om den pågældende findes skyldig i et andet forhold, medmindre dette andet forhold i sig selv kunne have begrundet optagelsen.

I praksis opbevares personfotografier optaget med henblik på senere identifikation af de pågældende dels i de lokale politikredse, hvor de er optaget, dels i en central samling under Rigspolitiet (fototeket).

2.3. Politiets forevisning og offentliggørelse af fotografier mv.

Retsplejelovens regler om forevisning af fotos sondrer mellem tre forskellige situationer: 1) hvor politiet foreviser et fotografi af en person, der konkret er mistænkt i den sag, der efterforskes, 2) hvor politiet foreviser et fotografi af forurettede eller andre vidner, og 3) hvor politiet foreviser fotografier fra fototeket (fotografier, der er optaget i forbindelse med en tidligere sag med henblik på senere identifikation af de pågældende), uden at de viste personer er konkret mistænkt i den sag, der nu efterforskes.

Politiets adgang til at forevise fotografier af *personer, der er mistænkt* i en sag, er reguleret i retsplejelovens § 812. Det fremgår af bestemmelsen, at fotografier af en mistænkt, som politiet er i besiddelse af, kun må forevises for personer uden for politiet, såfremt den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og indgrebet må antages at være af væsentlig betydning for efterforskningen.

Kompetencen til at beslutte, om der skal ske forevisning af fotografier ligger hos politiet, jf. § 812, stk. 2.

Det følger af retsplejelovens § 814, stk. 1, at forevisning af fotografier af *forurettede og andre vidner*, der ikke har samtykket i forevisningen, kun må ske, såfremt efterforskningen angår en forbrydelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, og indgrebet (forevisningen) må antages at være af afgørende betydning for efterforskningen.

Afgørelse om forevisning af fotografier efter § 814 træffes af retten ved kendelse, jf. bestemmelsens stk. 2.

Efter retsplejelovens § 815 må *forevisning af fotografier, som opbevares af politiet med henblik på senere identifikation*, jf. § 792 f (fototeket), uden for de tilfælde, der er omfattet af § 812 eller § 814, kun ske, såfremt efterforskningen angår en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, og den fotograferede inden for de seneste 5 år er fundet skyldig i en lovovertrædelse, der

efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, eller inden for de seneste 10 år er fundet skyldig i en lovovertrædelse, der kan medføre fængsel i 6 år eller derover.

Kompetencen til at beslutte, om der skal ske forevisning af fotografier efter § 815, ligger hos politiet, jf. bestemmelsens stk. 2.

Det følger af den almindelige proportionalitetsgrundsætning, jf. retsplejelovens § 816, at forevisning ikke må ske, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den, som det rammer, ville være et uforholdsmæssigt indgreb.

For så vidt angår politiets muligheder for at offentliggøre fotografier af en formodet gerningsmand følger det af retsplejelovens § 818, stk. 2, at offentliggørelse af et fotografi kun må finde sted, såfremt der er begrundet mistanke om, at den pågældende har begået en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder.

Herudover gælder reglen i retsplejelovens § 818, stk. 3, hvorefter offentliggørelse af et fotografi dog ikke må foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den, som det rammer, ville være et uforholdsmæssigt indgreb.

Kompetencen til at træffe afgørelse om offentliggørelse af et fotografi ligger hos politiet, jf. retsplejelovens § 818, stk. 4.

2.4. Politiets interne forskrifter om fingeraftryk og personfotografier

Den nærmere fremgangsmåde i forbindelse med politiets optagelse, opbevaring og anvendelse af fingeraftryk og personfotografier er reguleret i en række interne forskrifter hos politiet, herunder særlig Rigspolitiets kundgørelse B nr. 28 om fototeket hos Rigspolitiet og politikredsenes fotosamlinger og Rigspolitiets kundgørelse B nr. 24 om Kriminalteknisk Center (KTC).

De omtalte kundgørelser er af efterforskningsmæssige årsager ikke offentligt tilgængelige.

3. Persondatalovgivningen

3.1. Lov om behandling af personoplysninger (persondataloven)

3.1.1. Baggrund

Europa-Parlamentets og Rådets direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger blev vedtaget den 24. oktober 1995[1]. Direktivet indeholder en detaljeret regulering af såvel offentlige myndigheders som private virksomheders elektroniske behandling af personoplysninger. Direktivets formål er at sikre beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger samt at fjerne hindringerne for udveksling af personoplysninger inden for Fællesskabets område, jf. artikel 1. Direktivet er udarbejdet med hjemmel i artikel 100 A (nu artikel 95) i traktaten om oprettelse af Det Europæiske Fællesskab (EF-traktaten). Direktivet indeholder regler, som binder medlemsstaterne til at gennemføre en bestemt retstilstand, samt regler, der giver medlemsstaterne en videre adgang til at fastsætte regler til gennemførelse af direktivets intentioner.

Folketinget har i tilknytning til direktivet gennemført lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven), som er baseret på Justitsministeriets[2] betænkning nr. 1345/1997 om behandling af personoplysninger. Loven trådte i kraft den 1. juli 2000.

Ved loven gennemførtes en generel lovgivning om behandling af personoplysninger, som dels implementerede direktivet, dels erstattede de tidligere registerlove. Lovens formål er at sikre et fortsat højt beskyttelsesniveau i forhold til den enkelte borger, samtidig med at loven skal skabe de retlige rammer for en hensigtsmæssig udnyttelse af mulighederne for at behandle personoplysninger elektronisk.

[1] EF-Tidende nr. L 281 af 23. november 1995, s. 31 ff.
[2] Udvalget om registerlovgivningen.

3.1.2. Persondatalovens anvendelsesområde

3.1.2.1. Direktiv 95/46/EF

Direktivets anvendelsesområde afgrænses positivt i artikel 3, stk. 1, hvorefter direktivet gælder for behandling af personoplysninger, der helt eller delvis foretages ved hjælp af elektronisk databehandling, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

En negativ afgrænsning af direktivets anvendelsesområde findes i artikel 3, stk. 2, hvorefter direktivet ikke gælder behandling af personoplysninger, som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten. Undtaget er endvidere behandling, som vedrører den offentlige sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område, samt behandling som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.

Direktivet er således baseret på en funktionel afgrænsning, dvs. en afgrænsning af anvendelsesområdet via de relevante behandlingsaktiviteter. Derimod indeholder direktivet ikke nogen organisatorisk afgrænsning, og anvendelsesområdet omfatter derfor al behandling, uanset for hvem behandlingen måtte blive foretaget, og dermed såvel den offentlige som den private sektor.

Til brug for nærmere afgrænsning af anvendelsesområdet er bl.a. begreberne i artikel 3, stk. 1, defineret i direktivets artikel 2.

Ved "behandling af personoplysninger" forstås enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som personoplysninger gøres til genstand for, f.eks. registrering, opbevaring og videregivelse af oplysninger, men også indsamling, systematisering, tilpasning, ændring, udvælgelse, søgning, brug, formidling, sammenstilling, samkøring, elektronisk overførsel, samt blokering, sletning og tilintetgørelse mv., jf. artikel 2, litra b.

Ved "personoplysninger" forstås enhver form for information om en identificeret eller identificerbar fysisk person, jf. nærmere artikel 2, litra a. Det er ikke et krav, at perso-

nen direkte kan identificeres. Også den, der indirekte kan identificeres ved et CPR-nummer, en kode eller på anden måde, er omfattet af direktivet. Omfattet af begrebet personoplysninger er således også oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til et registreringsnummer, medlemsnummer, journalnummer eller lignende. Ved afgørelsen af, om en person er identificerbar, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den dataansvarlige eller af enhver anden, tages i betragtning, jf. præamblens betragtning 26.

Ved "register med personoplysninger" forstås enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag, jf. artikel 2, litra c.

3.1.2.2. Persondataloven

Persondataloven regulerer behandling af personoplysninger, som foretages af offentlige myndigheder og private, når behandlingen helt eller delvist foretages ved hjælp af elektronisk databehandling. Den omfatter ligeledes ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. persondatalovens § 1, stk. 1.

Persondatalovens regler gælder endvidere for anden ikke-elektronisk systematisk behandling af personoplysninger, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden, jf. persondatalovens § 1, stk. 2.

Ved personoplysninger forstås ifølge lovens § 3, stk. 1, enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Både ved indsamling (indrollering) af fingeraftryk og den efterfølgende brug (matchning) af templaten af aftrykket, jf. det biometribaserede register omtalt i kapitel 4, afsnit 2.2.2.1.5., er der tale om behandlinger af personoplysninger omfattet af persondataloven.

Det følger af persondatalovens § 2, stk. 1, at regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Af bemærkningerne til persondatalovens § 2, stk. 1, fremgår det, at bestemmelsen indebærer, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling.

Det fremgår imidlertid også, at dette ikke gælder, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod direktivet om behandling af personoplysninger.

Der er således adgang til at fravige persondatalovens regulering ved lov. Dette forudsætter dog som nævnt, at reguleringen ikke strider mod databeskyttelsesdirektivet.

3.1.3. Behandlingsregler

Direktivet angiver i kapitel 2 betingelser for lovlig behandling af personoplysninger. Der er regler om, hvornår behandling kan finde sted (artikel 6-9), om den registreredes rettigheder (artikel 10-15), om behandlingernes fortrolige karakter og behandlingssikkerhed (artikel 16-17) og om anmeldelse af behandlinger samt disses offentlige tilgængelighed (artikel 18-21). Ifølge artikel 5 skal medlemsstaterne i henhold til disse bestemmelser præcisere, på hvilke betingelser behandling af personoplysninger er lovlig. Ligeledes fremgår det af præamblens betragtning 22, at medlemsstaterne i deres lovgivning skal fastsætte nærmere bestemmelser om, på hvilke generelle betingelser en behandling er lovlig, og at medlemsstaterne har mulighed for uafhængigt af de generelle regler at fastsætte særlige betingelser for databehandling på specifikke områder og med hensyn til de særlige kategorier af de oplysninger, der omhandles i artikel 8. I overensstemmelse med direktivets regler indeholder persondataloven i kapitel 4-7 regler for, under hvilke betingelser behandling af oplysninger må finde sted.

3.1.3.1. Grundlæggende principper

I persondatalovens § 5 er fastsat en række grundlæggende principper for den dataansvarliges behandling af oplysninger, herunder regler om indsamling, ajourføring, op-

bevaring mv. Reglerne giver ikke et selvstændigt retligt grundlag for at foretage en bestemt behandling af oplysninger, idet hjemmel hertil skal søges i de øvrige behandlingsregler i §§ 6-13, kapitel 5-7 eller eventuelt i anden lovgivning. Reglerne i § 5 skal derimod altid iagttages, når der i medfør af de øvrige regler er hjemmel til at foretage behandlingen. Reglerne i § 5 følger af direktivet og kan derfor ikke fraviges for så vidt angår behandlinger, som er omfattet af direktivets anvendelsesområde.

Det påhviler ifølge lovens § 5 den dataansvarlige at overholde følgende regler:

- Behandling af personoplysninger skal ske i overensstemmelse med "god databehandlingsskik". Heri ligger, at behandlingen skal være rimelig og lovlig, men i øvrigt er det overladt til Datatilsynet at udfylde den retlige standard "god databehandlingsskik".

- Indsamlingen og registreringen af personoplysningerne skal efter § 5, stk. 2, ske til udtrykkeligt angivne og saglige formål. Om et bestemt formål med en indsamling af personoplysninger er sagligt afhænger først og fremmest af, om indsamlingen sker til løsning af en opgave, som det ligger inden for den pågældende myndigheds, virksomheds mv. område at varetage. I kravet om udtrykkelighed ligger, at den dataansvarlige i forbindelse med indsamlingen skal angive et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen, og formålet skal defineres med en vis præcision.

- Senere behandling må ikke være uforenelig med de formål, hvortil oplysningerne er indsamlet. Indsamlede oplysninger kan efterfølgende principielt godt anvendes til et andet end det oprindelige formål, blot den senere anvendelse ikke er uforenelig med det formål, som oplysningerne oprindeligt blev indsamlet til.

- Der må ikke indsamles flere oplysninger, end formålet tilsiger (proportionalitetsprincippet).

- Oplysningerne skal undergives fornøden ajourføring og fornøden kontrol med henblik på at sikre, at der ikke behandles urigtige eller vildledende oplysnin-

ger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller rettes. Endelig skal indsamlede oplysninger slettes eller anonymiseres, når det ikke længere er nødvendigt for den pågældende myndighed eller person at være i besiddelse af oplysningerne i en form, der gør det muligt at identificere enkeltpersoner.

De ovennævnte regler bidrager bl.a. til at sikre mod en unødvendig ophobning af data, der principielt altid indebærer en vis forøget risiko for krænkelse af den registrerede, idet oplysningerne kan komme uvedkommende i hænde.

3.1.3.2. Materielle behandlingsregler

Persondatalovens §§ 6-8 indeholder en række regler om, hvornår man f.eks. må indsamle, registrere og videregive personoplysninger. Hvilke regler, man skal følge i den enkelte situation, afhænger af oplysningernes karakter og formålet med databehandlingen.

I persondatalovens § 6, stk. 1, fastsættes betingelser for, hvornår behandling af almindelige personoplysninger må finde sted. Af bestemmelsen følger, at behandling af oplysninger kun må finde sted, hvis en af de i nr. 1-7 angivne betingelser er opfyldt.

Et fingeraftryk eller en matematisk værdi af et fingeraftryk – en såkaldt template – må efter Datatilsynets opfattelse anses for en almindelig ikke-følsom oplysning omfattet af persondatalovens § 6.

Videregivelse og behandling af oplysninger om enkeltpersoners rent private forhold er reguleret i persondatalovens §§ 7 og 8. De oplysninger, der omfattes af bestemmelsen i § 7, er oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold samt helbredsmæssige og seksuelle forhold.

Lovens § 8 omfatter oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end dem, der er nævnt i § 7.

Det fremgår af persondatalovens § 8, stk. 2, at de i stk. 1 nævnte oplysninger ikke må videregives. Videregivelse kan dog bl.a. finde sted efter § 8, stk. 2, nr. 1, hvorefter videregivelse kan ske, hvis den registrerede har givet sit udtrykkelige samtykke til videregivelsen, og efter § 8, stk. 2, nr. 2, hvorefter videregivelse kan ske, hvis videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den oplysningen angår.

Bestemmelsen forudsætter, at der i hvert enkelt tilfælde, hvor oplysninger ønskes videregivet, skal ske en konkret vurdering af, om videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til den, oplysningen angår.

Et samtykke skal indhentes i overensstemmelse med persondatalovens § 3, nr. 8, hvorefter et samtykke er enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Der gælder ingen formkrav til et samtykke, men der skal være tale om en viljestilkendegivelse. Heraf må antages at følge, at et såkaldt "negativt samtykke", hvor en person i en situation undlader at reagere og derved bliver forpligtet, eller en anden form for stiltiende eller indirekte samtykke som udgangspunkt ikke opfylder lovens krav, jf. herved også persondatalovens generelle krav om, at et samtykke skal være "udtrykkeligt".

At et samtykke skal være frivilligt betyder, at samtykket ikke må være undergivet tvang. Dette gælder uanset, om det er den dataansvarlige selv eller andre, der udøver pression overfor den registrerede. Det er derimod fast antaget i såvel teori som praksis, at den omstændighed, at den registrerede opnår en modydelse, herunder f.eks. adgang til en bestemt restaurationsvirksomhed, ikke bevirker, at et samtykke ikke kan anses for at være afgivet frivilligt.

I kravet om, at et samtykke skal være specifikt, ligger, at samtykket skal være konkretiseret, således at det klart og utvetydigt fremgår, hvad der meddeles samtykke til,

herunder hvilke oplysninger der må behandles på baggrund af samtykket, af hvem og til hvilke formål.

Herudover skal der i forbindelse med samtykke gives tilstrækkelig information om samtykkets rækkevidde, således at den, der afgiver samtykket, er klar over, hvad dette indebærer.

Af persondatalovens § 8, stk. 4, 2. pkt., følger det, at private må behandle, herunder opbevare, oplysninger om bl.a. strafbare forhold, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. Også denne undtagelsesbestemmelse forudsætter, at der i hvert enkelt tilfælde, hvor private skal behandle oplysninger, foretages en konkret vurdering af, om behandlingen sker til varetagelse af en berettiget interesse, og om denne interesse klart overstiger hensynet til den registrerede.

3.1.3.3. Særlig om databeskyttelsesdirektivets regler om behandling af oplysninger om strafbare forhold

Af databeskyttelsesdirektivets artikel 8, stk. 5, 1. afsnit, følger, at behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger som udgangspunkt kun må foretages under kontrol af en offentlig myndighed. Behandling af de nævnte oplysninger må således efter bestemmelsen som udgangspunkt kun ske for en offentlig myndighed.

Hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning, herunder administrative forskrifter fastsat i henhold til lov, kan behandling af sådanne oplysninger dog også udføres for private.

Der er ikke i artikel 8, stk. 5, (eller i bestemmelsens øvrige regler) fastsat materielle behandlingskriterier for, hvornår der kan ske behandling af oplysninger om strafbare forhold. Dette spørgsmål må derfor antages at skulle vurderes ud fra direktivets artikel 7, som bl.a. fastsætter, at behandling af personoplysninger kan finde sted, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt. Behandling

af personoplysninger kan efter artikel 7 endvidere finde sted, hvis behandlingen er nødvendig for, at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til direktivet, går forud herfor.

Det bemærkes, at direktivet giver mulighed for, at medlemsstaterne uafhængigt af de generelle regler kan fastsætte særlige betingelser for databehandling på specifikke områder, jf. direktivets artikel 5 og betragtning 22.

3.1.4. Registreredes rettigheder

I overensstemmelse med databeskyttelsesdirektivets artikel 10-15 fastsætter persondataloven i kapitel 8-10 en række rettigheder for den registrerede. Registreredes rettigheder omfatter:

- Ret til at få information fra den dataansvarlige om, at der indsamles oplysninger om en selv, jf. §§ 28-29. Den dataansvarlige skal på eget initiativ give meddelelse til de personer, om hvem oplysninger indsamles. Meddelelsen skal gives ved indsamlingen af oplysningerne og i almindelighed inden for 10 dage. Oplysningspligten gælder både ved indsamling af oplysninger hos den registrerede selv og hos andre, og der skal bl.a. oplyses om den dataansvarliges og dennes eventuelle repræsentants identitet, formålene med behandlingen samt alle yderligere oplysninger, der er nødvendige for, at personen kan varetage sine interesser. § 30 angiver visse undtagelser til oplysningspligten i §§ 28 og 29, som herefter kan begrænses, hvis det er nødvendigt af hensyn til bl.a. statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse og efterforskning af straffesager, beskyttelse af den registreredes interesser eller andres rettigheder og frihedsrettigheder. Oplysningspligten gælder ikke, hvis den registrerede allerede er bekendt med de i bestemmelserne nævnte oplysninger, jf. § 28, stk. 2, og § 29, stk. 2, 1. led. Oplysningspligten i § 29 gælder endvidere ikke, hvis registreringen eller videregivelsen af oplysninger udtrykkeligt er fastsat ved lov, eller hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssigt vanskelig, jf. § 29, stk. 2, 2. led, og stk. 3.

- Ret til at få indsigt i de oplysninger, der behandles om en selv, jf. §§ 31-34. Den registreredes indsigtsret følger af persondatalovens § 31, som fastslår den registreredes ret til at få oplyst, om der behandles oplysninger om vedkommende, og i givet fald ret til en række nærmere angivne oplysninger, herunder om behandlingens formål, og hvilke oplysninger der er omfattet af behandlingen.

- Ret til at gøre indsigelse mod, at behandling finder sted, jf. § 35. Efter § 35 kan den registrerede til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Det følger af direktivets artikel 14, stk. 1, litra a, at andet kan bestemmes i den nationale lovgivning. I tilfælde af berettiget indsigelse må den af den dataansvarlige iværksatte behandling ikke længere omfatte de pågældende oplysninger.

- Ret til at få korrigeret eller slettet oplysninger, der er urigtige eller vildledende, når anmodning herom fremsættes af den registrerede, jf. § 37. Den registrerede kan ligeledes som udgangspunkt stille krav om, at tredjemand, som har fået sådanne oplysninger udleveret, skal underrettes om korrektionen eller sletningen.

- Ret til at tilbagekalde et samtykke, jf. § 38. Samtykke kan tilbagekaldes på et hvilket som helst tidspunkt, dog ikke med "tilbagevirkende kraft" Efter tilbagekaldelse af et samtykke til behandling kan samtykket ikke længere være grundlag for behandling, og det må i den konkrete situation vurderes, om de registrerede oplysninger skal slettes eller blokeres.

- Ret til at gøre indsigelse mod at blive underkastet afgørelser, der har retsvirkninger for eller i øvrigt berører den registrerede i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, jf. § 39. Den registrerede har i dette tilfælde ret til hos den dataansvarlige snarest muligt og uden ugrundet ophold at få at vide, hvilke beslutningsregler der ligger bag afgørelsen.

- Ret til at klage til Datatilsynet, jf. § 40.

3.1.5. Behandlingssikkerhed

I overensstemmelse med direktivets artikel 16 og 17 stilles i persondatalovens §§ 41 og 42 krav til behandlingens fortrolighed og datasikkerhed.

Det følger heraf, at den dataansvarlige skal iværksætte de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, jf. § 41, stk. 3, f.eks. ved ubeføjet udbredelse eller ikke-autoriseret adgang. Om disse foranstaltninger fremgår det nærmere i direktivets artikel 17, stk. 1, at de – under hensyn til det aktuelle tekniske niveau og de omkostninger, der er forbundet med deres iværksættelse – skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

Endvidere fastslås det, at de personer eller virksomheder, der arbejder for den dataansvarlige, kun må behandle personoplysninger efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov, jf. § 41, stk. 1. Dette indebærer bl.a., at den pågældende person eller virksomhed ikke må behandle oplysninger til andre formål end dem, som den dataansvarlige har fastsat, samt at vedkommende ikke må behandle oplysninger efter instruks fra andre end den dataansvarlige.

Endelig fremgår det, at en dataansvarlig, som overlader en behandling af oplysninger til et edb-servicebureau, skal sikre sig, at bureauet kan sørge for den nødvendige datasikkerhed. Den dataansvarlige har også pligt til at kontrollere, at bureauets sikkerhedsforanstaltninger er i orden, og at de rent faktisk gennemføres, jf. således § 42, stk. 1.

3.1.6. Anmeldelse

Direktivet fastsætter i artikel 18-20 regler om anmeldelse. Det følger heraf, at den dataansvarlige som udgangspunkt forud for iværksættelsen skal anmelde behandling af oplysninger til den i artikel 28 omhandlede tilsynsmyndighed, og at der fastsættes regler om, hvilke oplysninger anmeldelsen skal indeholde. Medlemsstaterne kan i visse tilfælde og under nærmere angivne betingelser fritage for anmeldelse eller fastsætte

regler om forenklet anmeldelse. Behandlinger, der efter medlemsstaternes egne definitioner indeholder særlige risici for personers rettigheder og frihedsrettigheder, skal ifølge artikel 20 undergives forudgående kontrol, som foretages af tilsynsmyndigheden efter modtagelsen af anmeldelsen.

Persondataloven indeholder i kapitel 12-14 regler om anmeldelse af behandlinger til tilsynsmyndighederne, dvs. til Datatilsynet eller Domstolsstyrelsen. Der sondres mellem anmeldelse af behandlinger, der foretages for den offentlige forvaltning (kapitel 12), for en privat dataansvarlig (kapitel 13) og for domstolene (kapitel 14). Alle behandlinger skal som udgangspunkt anmeldes, for så vidt angår domstolene til Domstolsstyrelsen, og for så vidt angår andre til Datatilsynet. Endvidere fremgår det, hvilke oplysninger en anmeldelse skal indeholde, bl.a. den dataansvarliges navn og adresse, behandlingens betegnelse og formål, samt oplysninger om personkredsen og de oplysningstyper, der behandles.

Den offentlige forvaltning skal i henhold til lovens § 44, stk. 1, ikke anmelde behandlinger, som ikke omfatter oplysninger af fortrolig karakter. En oplysning anses for fortrolig, hvis der er tale om forhold som nævnt i lovens §§ 7, stk. 1, eller 8, stk. 1, hvis dette er foreskrevet i en særlig lov, eller hvis det i øvrigt er nødvendigt at hemmeligholde oplysningen for at varetage væsentlige hensyn til private eller offentlige interesser, jf. straffelovens § 152 og forvaltningslovens § 27, stk. 1. Endvidere undtages i bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning[3], flere behandlingstyper, herunder behandlinger, som foretages i forbindelse med tilsyn, kontrol og administration mv. i henhold til bl.a. miljø- og energilovgivningen samt landbrugs- og fødevarelovgivningen.

For behandlinger hos private findes en liste over undtagelser fra anmeldelse i lovens § 49. Listen suppleres af bestemmelser i bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig[4].

[3] Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000.
[4] Justitsministeriets bekendtgørelse nr. 534 af 15. juni 2000, som ændret ved bekendtgørelse nr. 202 af 22. marts 2001.

Nogle behandlinger anses for at have en så alvorlig risiko for den personlige databeskyttelse, at Datatilsynet skal foretage en vurdering af behandlingen, før den kan iværksættes. Når en behandling omfatter følsomme oplysninger, kan behandlinger først påbegyndes, når den dataansvarlige har modtaget en udtalelse/tilladelse fra Datatilsynet.

Den offentlige forvaltning skal ifølge § 45 indhente en udtalelse fra Datatilsynet, inden databehandlingen påbegyndes, hvis behandlingen omfatter følsomme oplysninger, jf. § 7, stk. 1, og § 8, stk. 1, hvis behandlingen udelukkende finder sted i videnskabeligt eller statistisk øjemed eller med henblik på at føre retsinformationssystemer, eller hvis behandlingen omfatter sammenstilling eller samkøring af oplysninger i kontroløjemed.

En privat dataansvarlig skal ifølge § 50 indhente tilladelse, hvis behandlingen omfatter følsomme personoplysninger, jf. § 7, stk. 1, og § 8, stk. 4, hvis behandlingen vedrører advarselsregistre, stillingsbesættende virksomhed (”headhunter”) eller erhvervsmæssig videregivelse af oplysninger om økonomiske forhold eller udelukkende finder sted med henblik på at føre retsinformationssystemer.

Datatilsynet offentliggør anmeldelserne i en særlig fortegnelse over anmeldte behandlinger, jf. lovens § 54, som i overensstemmelse med direktivets artikel 21 endvidere angiver, hvilke oplysninger fortegnelsen skal indeholde. Fortegnelsen er stillet til rådighed for offentligheden gennem Datatilsynets hjemmeside, www.datatilsynet.dk. For behandlinger, som ikke er omfattet af anmeldelsespligt, skal den dataansvarlige stille de i § 43, stk. 2, nr. 1, 2, og 4-6, nævnte oplysninger (dvs. bl.a. den dataansvarliges navn og adresse, behandlingens betegnelse og formål samt oplysninger om personkredsen og de oplysningstyper, der behandles) til rådighed for enhver, der anmoder herom.

Som i direktivets artikel 13 kan de krævede oplysninger samt offentlighedens adgang begrænses i medfør af lovens § 54, stk. 3, hvis det er nødvendigt til forebyggelse, opklaring og forfølgning af lovovertrædelser, eller hvis afgørende hensyn til private interesser gør det påkrævet.

3.1.7. Tilsyn mv.

I henhold til direktivets artikel 28 skal medlemsstaterne udpege en eller flere offentlige tilsynsmyndigheder, der skal påse overholdelsen af de bestemmelser, som medlemsstaten vedtager til gennemførelse af direktivet. Tilsynsmyndigheden skal udøve sine funktioner i fuld uafhængighed, jf. stk. 1. Tilsynsmyndigheden skal høres ved udarbejdelsen af administrative foranstaltninger eller retsforskrifter om beskyttelse af personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger. Endvidere skal tilsynsmyndigheden kunne iværksætte undersøgelser, gribe effektivt ind over for en behandling af oplysninger samt indbringe overtrædelser af de nationale bestemmelser, som vedtages til gennemførelse af direktivet, for retsinstanserne. Tilsynsmyndighedernes afgørelser kan af en involveret part indbringes for en retsinstans. Enhver kan indgive anmodning til tilsynsmyndigheden om beskyttelse af sine rettigheder i forbindelse med behandling af personoplysninger samt om at få kontrolleret en behandlings lovlighed, når de nationale bestemmelser om undtagelser og begrænsninger (artikel 13) finder anvendelse. Tilsynsmyndigheden skal med regelmæssige mellemrum udarbejde og offentliggøre en rapport om sit arbejde.

I overensstemmelse hermed er Datatilsynet i persondatalovens § 55, stk. 1, udpeget som tilsynsmyndighed, og i lovens kapitel 16 beskrives Datatilsynets organisation samt tilsyns- og inspektionskompetence. Tilsynet med behandling af oplysninger vedrørende domstolenes administrative forhold er henlagt til Domstolsstyrelsen, jf. lovens § 67, stk. 1, idet tilsyns- og inspektionskompetencen beskrives i kapitel 17.

Datatilsynet, som er en uafhængig myndighed, er fælles for den offentlige og den private sektor, jf. §§ 55 og 56. Datatilsynet har bl.a. til opgave at føre tilsyn med overholdelsen af loven, behandle klager fra registrerede personer samt afgive udtalelser og udstede tilladelser i forbindelse med anmeldelse af behandlinger til tilsynet, jf. §§ 57-64. Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget, og denne beretning offentliggøres, jf. § 65. Endvidere har tilsynet mulighed for at offentliggøre sine udtalelser.

Datatilsynets afgørelser efter persondataloven kan ikke indbringes for anden administrativ myndighed, jf. § 61, men afgørelserne kan indbringes for domstolene samt Folketingets Ombudsmand.

3.2. Forvaltningsloven og straffeloven

I forvaltningslovens § 27 er der fastsat nærmere regler om tavshedspligt for personer, der virker i den offentlige forvaltning. Det fremgår således af § 27, at en oplysning er fortrolig, når den ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller privates interesser. I forvaltningslovens § 27, stk. 1, er opregnet en række hensyn, der efter en konkret vurdering kan føre til, at en oplysning er fortrolig og dermed undergivet tavshedspligt.

Efter forvaltningslovens § 27, stk. 1, nr. 6, kan hensynet til enkeltpersoners eller private selskabers eller foreningers interesse i at beskytte oplysninger om deres personlige eller interne, herunder økonomiske, forhold begrunde tavshedspligt. Oplysninger om strafbare forhold vil være omfattet af tavshedspligten.

Det fremgår af straffelovens § 152, stk. 1, at den som virker eller har virket i offentlig tjeneste eller hverv, og som uberettiget videregiver eller udnytter fortrolige oplysninger, hvortil den pågældende i den forbindelse har fået kendskab, straffes med bøde eller fængsel indtil 6 måneder.

En oplysning er ifølge straffelovens § 152, stk. 3, fortrolig, når den ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser.

Det følger af straffelovens § 152 e, at bl.a. bestemmelsen i § 152 ikke omfatter tilfælde, hvor den pågældende er forpligtet til at videregive en fortrolig oplysning eller handler i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv.

3.3. Den Europæiske Menneskerettighedskonvention

Efter Den Europæiske Menneskerettighedskonvention artikel 8 har enhver ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. Det fremgår af bestemmelsens stk. 2, at ingen offentlig myndighed må gøre indgreb i udøvelsen af

denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder eller friheder.

Videregivelse af oplysninger om privatpersoner, hvoraf det direkte eller indirekte kan udledes, at de pågældende er sigtet for et strafbart forhold, må anses for et indgreb i de pågældende personers ret til respekt for privatliv efter konventionens artikel 8, stk. 1, og videregivelse af sådanne oplysninger kan derfor kun ske på de betingelser, der er nævnt i artikel 8, stk. 2.

KAPITEL 3. Fremmed ret

1. Norge

I Norge kan politiet i medfør af lov nr. 55 af 13. juni 1997 om serveringsvirksomhet (serveringsloven) træffe beslutning om, at en gæst, som har forstyrret ro og orden eller brudt ordensreglerne i en restauration, skal nægtes adgang til restaurationen for en begrænset periode (adgangsnektelse). Beslutningen herom vil i givet fald rette sig både mod gæsten og restaurationen, ligesom den vil blive bekendtgjort over for dem begge af politiet.

Herudover kan der efter lov nr. 25 af 22. maj 1981 om behandlingsmåten i straffesaker (strafprocesloven) nedlægges forbud mod, at en person opholder sig på bestemte lokaliteter (besøgsforbud).

Det følger af lovens § 222 a, stk. 1, at anklagemyndigheden kan nedlægge et såkaldt besøgsforbud, såfremt der er grund til at tro, at en person vil begå en strafbar handling eller i øvrigt krænke freden på det pågældende sted. Anklagemyndigheden skal snarest muligt og senest inden 5 dage indbringe forbuddet for retten.

Besøgsforbuddet skal være konkretiseret og individualiseret med hensyn til, hvilket sted og hvilke personer det omfatter. Ifølge retspraksis fortolkes disse krav dog ikke strengt. Typisk vil der være tale om et forbud mod at opholde sig i eller i nærheden af et privat hjem. Det følger dog af retspraksis, at der også vil kunne nedlægges forbud mod at opholde sig i bestemte restaurationer, jf. herved bl.a. højesteretsafgørelsen i Rt. 2002, s. 1243, som omhandlede besøgsforbud i et indkøbscenter, og Borgating lagmannsretts[5] dom af 21. marts 2006 (LB-2006-20909), som vedrørte et forbud mod at opsøge, forfølge eller på nogen måde kontakte personer i dagscentre, omsorgsboliger, boenheder og ældrecentre i Oslo.

Besøgsforbuddet skal meddeles skriftligt til såvel den, forbuddet retter sig mod, som til den, der tilsigtes beskyttet ved forbuddet. Forbuddet skal være tidsbegrænset og må højest gælde et år.

[5] Svarende til landsretten i Danmark.

Der føres ikke noget særskilt register over personer eller restaurationer, der har fået meddelt et forbud.

2. Sverige

Der findes ikke regler om restaurationsforbud i Sverige.

Det antages efter svensk ret, at restauratører kan bortvise gæster fra en restauration, så længe bortvisningen ikke er motiveret af personens race, religion, hudfarve, seksuelle orientering eller lignende. Politiet vil efter omstændighederne yde restauratøren assistance i den forbindelse.

3. Storbritannien

I Storbritannien følger det af Licensed Premises Act (Exclusion of Certain Persons) (lov om udelukkelse af restaurationsgæster), at retten, hvis en person bliver dømt for personfarlig kriminalitet i forbindelse med et restaurationsophold, kan forbyde den pågældende at indfinde sig på den pågældende restauration og eventuelt andre navngivne restaurationer uden restauratørens samtykke.

Såfremt retten træffer afgørelse om et sådant forbud, vil en kopi af afgørelsen blive sendt til den eller de relevante restaurationer. Der findes ikke noget nationalt register i Storbritannien over personer, som har fået meddelt forbud mod at indfinde sig på restaurationer i medfør af den omtalte lovgivning.

De britiske myndigheder har oplyst, at de ikke er i besiddelse af statistiske oplysninger om anvendelsen af de omtalte regler, men at indtrykket er, at regelsættet kun anvendes i meget begrænset omfang. En mulig forklaring på dette kan være, at domstolene ikke er bekendt med muligheden for at anvende sådanne forbud. En anden mulig forklaring er, at problemerne ofte i praksis løses ved, at restauratøren selv meddeler gæsten en karantæne.

Der findes ikke regler om administrative restaurationsforbud i Storbritannien.

En stor andel af de britiske restaurationer er medlem af lokale Pubwatch organisationer. Disse organisationer er frivillige, private foreninger.

Det er kutyme, at når en person får karantæne på en restauration, som er tilknyttet en Pubwatch organisation, omfatter karantænen alle Pubwatch restaurationer i det pågældende område. Karantæneramte personer registreres typisk på en liste, som opbevares bag baren på de pågældende restaurationer. Ofte er dørmændene på Pubwatch restaurationer, som ligger i samme geografiske område, endvidere i radiokontakt med hinanden, således at de kan advare hinanden om uroskabende gæster, som de skal være opmærksomme på.

KAPITEL 4. Udvalgets overvejelser

1. Udvalgets grundlæggende overvejelser

1.1. Ønsket om en udvidelse af restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud

Debatten om et tryggere natteliv har i de seneste år bl.a. drejet sig om, hvordan restauratører og dørmænd sikres de nødvendige redskaber til at undgå, at personer med restaurationsforbud alligevel får adgang til restaurationen.

Der er i den forbindelse bl.a. blevet peget på, at restauratører og dørmænd ikke i tilstrækkelig omfang har adgang til identitetsoplysninger på personer, som politiet har meddelt restaurationsforbud i medfør af restaurationslovens § 31, stk. 2, og derfor har vanskeligt ved at identificere de pågældende personer i forbindelse med adgangskontrol mv.

1.1.1. Beslutningsforslag B 112

Folketinget behandlede i folketingsåret 2006-07 et forslag til folketingsbeslutning om gennemførelse af initiativer, der kan sikre et tryggere natteliv (B 112, fremsat den 13. marts 2007). I beslutningsforslaget blev der bl.a. lagt op til, at der skulle etableres et centralt register over restaurationsforbud, som restaurationerne skulle have adgang til.

I Folketingets Retsudvalgs beretning af 1. oktober 2007 over beslutningsforslaget (Folketingstidende 2006-07, Tillæg B, side 1783) bemærkede et flertal i udvalget (V, S, DF, KF og RV) bl.a. følgende vedrørende forslaget om etablering af et centralt register over restaurationsforbud:

> ”Flertallet forstår det således, at der kan være usikkerhed med hensyn til, i hvilket omfang politiet efter den gældende lovgivning kan videregive oplysninger om restaurationsforbud til den eller de pågældende restauratører, og ligeledes med hensyn til restauratørernes adgang til at videregive sådanne oplysninger til dørmænd og andre ansatte i restaurationsvirksomhederne.
>
> Flertallet er samtidig opmærksomt på, at etablering af en ordning, der kan sikre restaurationsvirksomhederne bedre mulighed for at identificere personer,

der er meddelt et restaurationsforbud, rejser en række spørgsmål af praktisk og retlig karakter, herunder med hensyn til persondatabeskyttelse."

1.2. Problemets omfang i praksis

Det er umiddelbart vanskeligt at bedømme, hvor ofte det sker, at en person med restaurationsforbud – som følge af restaurationens manglende kendskab til den pågældendes identitet – alligevel får adgang til restaurationen.

Det bemærkes i den forbindelse, at det som oftest ikke er muligt at fastslå, om det skyldes restaurationers manglende adgang til identitetsoplysninger på personer med restaurationsforbud eller andre årsager, når personer med restaurationsforbud alligevel får adgang til de pågældende restaurationer. Som mulige andre årsager kan nævnes en ineffektiv adgangskontrol eller manglende vilje til at håndhæve restaurationsforbud.

De generelle tal for restaurationsforbud og sigtelser for overtrædelser af restaurationsforbud kan dog give en vis indikation af problemets omfang.

1.2.1. Antallet af restaurationsforbud

Rigspolitiet har oplyst, at antallet af sager vedrørende meddelelse af forbud i medfør af restaurationsloven, der er registreret i perioden 2002 – 2008 (1. halvår), er:

År	2002	2003	2004	2005	2006	2007	2008 (1.halvår)
Antal	1.189	1.300	1.302	1.951	2.516	1.927	976

Oversigten omfatter alle forbud, der er meddelt i medfør af restaurationsloven. Der er således ikke kun tale om forbud, der er meddelt i medfør af restaurationslovens § 31, stk. 2. Tallene angiver ikke antallet af personer, der er meddelt forbud, men antallet af sager. I nogle tilfælde gives der således forbud til flere personer inden for samme sag (f.eks. forbud til både gæst og restauratør eller til flere gæster). En gennemgang af de

umiddelbart tilgængelige oplysninger, der i 2007 er registreret af politikredsene, har endvidere vist, at praksis med hensyn til registrering har været noget forskellig fra kreds til kreds. Det er derfor ikke muligt præcist at angive, hvor mange personer der er meddelt forbud i den omhandlede periode.

For omkring 1/5 af de registrerede oplysninger vedrørende 2007 gælder det, at det ikke er muligt at se, hvad der ligger til grund for det meddelte forbud, herunder om forbuddet er meddelt til en gæst eller en restauratør, eller om forbuddet vedrører en af restaurationslovens andre bestemmelser. Det må dog antages, at der kun i et meget begrænset omfang er tale om forbud efter andre bestemmelser i restaurationsloven end § 31, stk. 2.

Blandt de resterende 4/5 af registreringerne, hvor der foreligger oplysninger om baggrunden for forbuddet, var alle forbud således givet i medfør af restaurationslovens § 31, stk. 2. Baggrunden for forbuddene var følgende:

45,6 %: Sigtelser for bl.a. værtshusuorden og slagsmål eller anden voldelig, støjende eller truende adfærd (dvs. typisk overtrædelse af restaurationsloven eller ordensbekendtgørelsen). Denne gruppe omfatter også sigtelser i medfør af straffeloven for vold eller hærværk, men ud fra de umiddelbart tilgængelige oplysninger er det ikke muligt at angive, hvor mange sager der vedrører straffelovsovertrædelser.

44,1 %: Sigtelser for overtrædelse af lovgivningen om euforiserende stoffer.

4,6 %: Sigtelser for overtrædelse af våbenlovgivningen.

2,4 %: Andre lovovertrædelser, hovedsagelig lovovertrædelser begået mod politiet (fornærmelig tiltale, trusler og voldelig optræden, hindringer for udførelsen af tjenesten) samt tyveri begået på restaurationen.

3,3 %: Forbud meddelt til restauratører mod at modtage en bestemt person som gæst. Antallet af forbud til restauratører må imidlertid antages at være noget højere, end det umiddelbart fremgår, da det ikke kan udelukkes, at der i nogle tilfælde – udover forbud til en gæst – også er givet forbud til restauratøren, uden at det fremgår af registrerede oplysninger.

1.2.2. Antallet af overtrædelser

Rigspolitiet har oplyst, at der for perioden 2002 – 2008 (1. halvår) er registret følgende antal sigtelser for overtrædelse af forbud efter restaurationsloven:

År	2002	2003	2004	2005	2006	2007	2008 (1.halvår)
Antal	168	204	275	416	609	450	216

Som anført ovenfor under afsnit 1.2.1. omfatter Rigspolitiets opgørelser vedrørende forbud meddelt efter restaurationsloven ikke alene forbud, der er meddelt personer i medfør af restaurationslovens § 31, stk. 2, men også forbud, der er rettet mod restauratører med flere i medfør af andre bestemmelser i restaurationsloven. Tilsvarende gør sig gældende vedrørende registreringen af overtrædelser af forbud, der er udstedt i medfør af restaurationsloven.

En gennemgang af de umiddelbart tilgængelige oplysninger vedrørende de registrerede sager i 2007 viser, at fire af sagerne vedrørte sigtelser mod restauratører, der havde overtrådt et forbud mod at modtage en bestemt gæst i restaurationen.

412 sager vedrørte sigtelser for overtrædelse af forbud mod at indfinde sig i en restauration som gæst.

For så vidt angår de resterende sager kunne det ikke ud fra de umiddelbart tilgængelige oplysninger fastslås, hvilken type forbud der var overtrådt.

1.2.3. Hvor opstår problemerne i praksis?

1.2.3.1. De større diskoteker

Det må antages, at problemet med at identificere personer med restaurationsforbud i nattelivet navnlig opstår på større diskoteker, hvor et betydeligt antal personer har forbud mod at opholde sig, jf. restaurationslovens § 31, stk. 2, og hvor dørmændene, som udfører adgangskontrollen, ikke i forvejen kender de pågældende gæster.

I praksis kendes der eksempler, hvor et betydeligt antal personer på samme tid har haft forbud mod at opholde sig på et bestemt diskotek. I denne situation er det i praksis umuligt for dørmændene at sikre, at personer med restaurationsforbud ikke får adgang til restaurationen, medmindre dørmændene har adgang til identitetsoplysninger på de pågældende personer.

Dansk Erhverv og Horesta har oplyst, at det ikke umiddelbart er muligt at fastslå, hvor mange større diskoteker og natklubber der findes i Danmark.

Et udtræk fra Danmarks Statistik vedrørende antallet af enheder i virksomhedsgruppen "Diskoteker og natklubber" i 2007 fordelt på omsætninger viser følgende:

Antal enheder i branchen 554020 i 2007		
	Total	Vægtet
Under 0,5 mio kr	94	74
0,5 mio. til 4 mio. kr	111	107
4 mio. til 10 mio. kr.	56	55
10 - 15 mio. kr	9	9
15 - 25 mio. kr	0	0
25 - 50 mio. kr.	3	3
50 mio. kr.	0	0
I alt	273	248

Totaltallet på 273 omfatter det samlede antal virksomheder indenfor kategorien, der har haft åbent i årets løb. Det vægtede tal på 248 tager højde for virksomheder, der ikke har haft åbent hele året. Således tæller en virksomhed, der kun har haft åbent i et halvt år, kun med som en halv virksomhed i forhold til det vægtede tal.

Dansk Erhverv har peget på, at tallene i tabellen er forbundet med nogen usikkerhed. F.eks. dækker de virksomheder, som ifølge statistikken har en årlig omsætning på over 25 millioner kr., reelt over diskotekskæder med et større antal enheder. Hertil kommer at en del større diskoteker og natklubber er registreret som restaurationer og dermed ikke optræder i ovennævnte tal. Reelt må det således antages, at antallet af større diskoteker og natklubber er noget højere.

1.2.3.2. Forbudszoner

Problemstillingen med identifikation af gæster med restaurationsforbud er endvidere aktuel i de tilfælde, hvor politiet udsteder bredere forbud, der omfatter flere restaurationsvirksomheder end den virksomhed, hvor det strafbare forhold er begået ("zoneforbud"), jf. kapitel 2, afsnit 1.6.1. Her vil personalet på de andre restaurationsvirksomheder typisk ikke have kendskab til den episode, som har givet anledning til forbuddet, og derfor ikke have nogen reel mulighed for at vide, at den pågældende person er omfattet af et restaurationsforbud, medmindre de modtager underretning herom fra politiet.

Zoneforbud anvendes i dag i flere politikredse.

1.2.3.3. De små værtshuse og udskænkningssteder mv.

Problemet med identifikation af personer med restaurationsforbud er i mindre grad relevant på de små værtshuse og udskænkningssteder. Her vil der typisk kun være tale om få personer, som har forbud mod at komme på stedet, og der vil ofte være tale om personer, som personalet i forvejen kender identiteten på.

Det kan dog på ingen måde udelukkes, at problemet også vil kunne opstå på mindre restaurationsvirksomheder, f.eks. i forbindelse med udskiftninger i personalet.

1.2.4. Politiets nuværende praksis vedrørende videregivelse af oplysninger

Rigspolitiet har oplyst, at der i samtlige politikredse gives underretning til restauratøren, når en gæst har fået forbud mod at komme i restaurationen. I mange tilfælde bliver forbuddet meddelt umiddelbart i tilknytning til, at den lovovertrædelse, som giver

anledning til forbuddet, er begået. I sådanne tilfælde vil der typisk samtidig ske mundtlig underretning af restauratøren. I andre tilfælde meddeles forbuddet på et senere tidspunkt, og underretning af restauratøren sker således også efterfølgende.

1.2.5. Restauratørers egen registrering af oplysninger

Dansk Erhverv og Horesta har oplyst, at nogle diskoteker og natklubber anvender egne gæsteregistreringssystemer, hvor det typisk vil være muligt at registrere oplysningen om, at en bestemt gæst har fået et forbud af politiet i medfør af restaurationslovens § 31, stk. 2.

Dansk Erhverv og Horesta har oplyst, de ikke er bekendt med, hvor stor en andel af de større diskoteker og natklubber der anvender egne registreringssystemer. Formentligt er der kun tale om en mindre del af virksomhederne. Det er dog indtrykket, at tallet er stigende.

1.2.5.1. Nox Network og registreringssystemet MasterClub

Danmarks største diskoteksnetværk NOX Network omfatter 55 diskoteker rundt omkring i landet, herunder diskotekskæderne Crazy Daisy og Buddy Holly.

NOX Network har – bl.a. som følge af et stigende behov for at kunne afvise gæster på et mere objektivt grundlag – udviklet et elektronisk gæsteregistreringssystem kaldet "MasterClub" i samarbejde med en privat virksomhed.

Systemet gør det bl.a. muligt for diskotekerne at udelukke personer, som har udvist en adfærd, der ikke lever op til de krav, der stilles på diskoteket. Endvidere vil systemet efter omstændighederne kunne identificere gæster, som har restaurationsforbud i medfør af restaurationslovens § 31, stk. 2.

Systemet fungerer ved, at gæsten – første gang vedkommende indfinder sig i restaurationen – lader sig registrere i en elektronisk database. Restaurationen bestemmer selv, hvilke identitetsoplysninger den vil registrere. Systemet understøtter således både brug af webkamera, fingeraftrykslæser og magnetkortlæser. Typisk registreres både gæstens navn, adresse, CPR-nummer og fingeraftryk. Endvidere optages der et foto-

grafi af den pågældende. Det hele foregår elektronisk, og registreringen kan derfor gennemføres på ganske kort tid.

Når gæsten besøger restaurationen efterfølgende, vil vedkommende i forbindelse med adgangskontrollen blive identificeret ved hjælp af sit fingeraftryk mv., og restaurationen vil – såfremt restaurationen har modtaget oplysninger herom fra politiet og lagt oplysningerne ind i systemet – bl.a. kunne se, om den pågældende har forbud mod at komme på stedet i medfør af restaurationslovens § 31, stk. 2.

Nox Network har over for udvalget bl.a. oplyst følgende om diskotekernes erfaring med anvendelsen af registreringssystemet:

> "Diskotekerne i NOX Network, som anvender MasterClub, har allerede gjort sig mange positive erfaringer med anvendelsen af registreringssystemet.
>
> Det forhold at gæsterne skal registreres første gang, de kommer som gæst, og igen ved efterfølgende besøg skal identificere sig, medfører ikke nogle ulemper for hverken gæster eller ansatte. Gæsterne betragter registreringen som naturlig, og føler sig trygge ved såvel formålet eller processen. Dette fornemmes tydeligt lokalt, at registreringen er et positivt samtaleemne i nattelivet.
>
> Det har med stor tilfredshed, for såvel politiet som diskotekerne kunne konstateres, at brugen af MasterClub registreringssystemet har medført, at de kriminelle forhold på diskotekerne er faldet betragteligt siden indførelsen.
>
> Der er særligt to forhold, der har medført at de kriminelle aktiviteter er nedbragt væsentligt på diskotekerne.
>
> For det første kan konstateres, at brugen af MasterClub- registreringssystemet virker forbyggende, idet enkelte gæster vælger at forlade køområdet, når de ser at der sker en registrering eller nægter at lade sig registrere, og dermed ikke får adgang.
>
> For det andet er der det faktum, at alle gæster som får adgang er registreret, og dermed kan identificeres. Udelukkelser/karantæner kan nu håndhæves sikkert og korrekt, da overvågningsvideoen sammenholdt med registreringen med billede, sikrer at de involverede personer genkendes.
>
> Herudover er det NOX Networks indtryk, at alene snakken om registreringen har lagt en dæmper på personer, som har kriminel adfærd i nattelivet."

1.2.5.2. Datatilsynets afgørelse i Crazy Daisy-sagen

Datatilsynet har i en principiel afgørelse fra sommeren 2008 taget stilling til, i hvilket omfang det under afsnit 1.2.5.1 omtalte gæsteregistreringssystem er foreneligt med persondataloven [6]

Datatilsynets afgørelse i Crazy Daisy-sagen er medtaget i betænkningen som bilag 2.

I den konkrete sag var der tale om, at diskoteket ønskede at registrere gæsternes fingeraftryk (template) samt billeder af gæsterne. Der var ikke tale om, at diskoteket ønskede at gemme gæsternes fingeraftryk, men som nævnt alene at opbevare en matematisk beregnet værdi af fingeraftrykket (template), som benyttes til at foretage en positiv identifikation. Det er ikke muligt at gendanne fingeraftryk på baggrund af en sådan template. Herudover ønskede diskoteket at registrere en række generelle kundeoplysninger og oplysninger om eventuelle karantæneforhold og restaurationsforbud, herunder oplysninger om karantæne/forbudsperiode og årsagen til karantænen.

Systemet indebar, at alle gæster ville skulle registreres, og det ville ikke være muligt at være gæst på diskoteket, hvis man ikke lod sig registrere.

Hovedformålet var ifølge diskoteket at sikre et trygt og sikkert natteliv, bl.a. ved bedre at kunne håndhæve forbud udstedt af politiet efter restaurationsloven.

Af sikkerhedsmæssige årsager ønskede diskoteket endvidere at undgå lange køer uden for diskoteket, da dette ofte fører til optrin og frustrationer. Diskoteket ønskede derfor at kunne foretage en ensartet og hurtig genkendelse af de gæster, som allerede er i systemet, og som derfor umiddelbart kan tildeles adgang.

Diskoteket anførte i forbindelse med ansøgningen bl.a., at man forventede, at antallet af såvel fysiske som verbale overfald på vagtpersonale og dørmænd ville blive reduceret, da dørmanden ikke længere over for gæsten ville fremstå som den, der administrerer forbud og karantæner.

[6] Jf. Datatilsynets journal nr. 2008-42-0742.

Datatilsynet tilkendegav i sin udtalelse til det pågældende diskotek, at diskoteket med gæsternes udtrykkelige samtykke kan registrere billede, fingeraftryk (templates) og andre oplysninger af ikke-følsom karakter.

Det var således Datatilsynets vurdering, at diskotekets ønske om at foretage en ensartet kontrol af gæsterne inden for en afgrænset periode og at undgå køer uden for diskoteket udgjorde et sagligt formål. Hvis behandlingen baserede sig på et udtrykkeligt samtykke, der lever op til persondatalovens krav, ville den påtænkte behandling af oplysninger om fingeraftryk (template) og billede derfor efter Datatilsynets opfattelse kunne ske inden for persondatalovens rammer. Datatilsynet påpegede dog, at persondatalovens regler indebærer, at diskoteket skal slette templaten og billedet, hvis den registrerede tilbagekalder sit samtykke.

Vedrørende spørgsmålet om restaurationsforbud bemærkede Datatilsynet:

> "Det er Datatilsynets vurdering, at Crazy Daisy uden samtykke kan indsamle, registrere og bruge oplysninger om forbud udstedt af politiet i medfør af restaurationsloven, jf. persondatalovens § 8, stk. 6, jf. 7, stk. 2, nr. 4, og § 8, stk. 4, 2. pkt., samt identifikationsoplysninger, herunder personnummer, på personer, som har fået sådant forbud, jf. persondatalovens § 6, stk. 1, nr. 3 og 7, og § 11, stk. 2, nr. 1. Oplysningerne skal slettes, når forbuddet udløber."

Datatilsynet gav herudover konkret tilladelse til, at diskoteket med gæsternes *skriftlige* samtykke kan registrere andre følsomme personoplysninger, f.eks. om strafbare forhold og narkotikamisbrug, i forbindelse med, at diskoteket tildeler en gæst karantæne.

Datatilsynet lagde i den forbindelse til grund, at diskoteket har behov for at registrere karantæneårsagen for senere at kunne forklare en gæst, hvorfor vedkommende ikke kan blive lukket ind på diskoteket i en nærmere afgrænset tidsperiode. Datatilsynet fandt, at dette må anses som et sagligt og legitimt formål og derfor inden for rammerne af persondatalovens § 5.

Datatilsynet oplyste, at det også med hensyn til de følsomme oplysninger gælder, at hvis gæsten tilbagekalder sit samtykke, skal oplysningen om årsagen til karantænen slettes. Diskoteket vil i en sådan situation efter en konkret vurdering alene kunne

gemme navn, adresse og en neutral oplysning om, hvor længe en person er uønsket som gæst i diskoteket.

Crazy Daisy havde oplyst, at alle oplysninger sendes krypteret til en ekstern database, og at adgang til databasen foregår via webservice, som er placeret bag firewall. Serverne er placeret i et hostingcenter, der er sikret mod fysiske trusler som brand, tyveri og hærværk. Centret er udstyret med alarm- og adgangskontrolsystemer. Det er endvidere kun administrator, som kan se oplysninger om karantæneårsag. Manuelle oplysninger opbevares i ringbind på et aflåst kontor.

Datatilsynet fastsatte herudover i sin tilladelse en række yderligere vilkår om sikkerhedsforanstaltninger i forbindelse med diskotekets behandling af følsomme personoplysninger.

Datatilsynet stillede bl.a. krav om, at diskoteket skulle give den fornødne instruktion til medarbejdere, som behandler personoplysningerne. Medarbejderne skulle bl.a. gøres bekendt med sikkerhedsforanstaltningerne og de tilhørende retningslinjer. Endvidere var det et vilkår, at medarbejderne blev informeret om, at de opslag, som de foretager i diskotekets elektroniske system, vil blive registreret (logget) og kan bruges til at kontrollere uberettigede opslag og til stikprøvekontrol.

1.2.5.3. Datatilsynets vilkår for sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger

I forlængelse af Crazy Daisy-afgørelsen har Datatilsynet udarbejdet en række standardvilkår for sikkerhed i forbindelse med restaurationsvirksomheders egen registrering af gæster, jf. herved Datatilsynets vilkår for sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger.

Datatilsynet har i alt fastsat følgende 13 sikkerhedsregler, som restaurationer skal iagttage i forbindelse med behandlingen af personoplysninger:

"[…]

Generelle sikkerhedsbestemmelser

1. Den dataansvarlige skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i virksomheden til uddybning af de regler, der fremgår af dette bilag. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangs-kontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for virksomheden. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i virksomheden.

2. Den dataansvarlige skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af punkt 1.

3. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

4. Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at persondatalovens § 41, stk. 3, overholdes.

Inddatamateriale som indeholder personoplysninger

6. Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddatering. Materialet skal opbevares aflåst, når det ikke anvendes, og slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, hvortil det er indsamlet, dog senest efter en af den dataansvarlige fastsat frist. Ved tilintetgørelse skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Uddatamateriale som indeholder personoplysninger

7. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Materialet skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri. Når materialet ikke længere skal anvendes til de formål, som behandlingen varetager, dog senest efter en af den dataansvarlige fastsat frist, skal det slettes eller tilintetgøres.

Autorisation og adgangskontrol

8. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles ved hjælp af edb. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

9. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, samt personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

10. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i punkt 8 og 9. Kontrol heraf skal foretages mindst en gang hvert halve år.

11. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som behandles ved hjælp af edb, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

12. Der skal foretages registrering af alle afviste forsøg på adgang til edb-systemet. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg.

Logning

13. I edb-registre skal der foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes."

Datatilsynets vilkår for sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger er medtaget som bilag 3 til betænkningen.

2. Løsningsmodeller

2.1. Grundlæggende kriterier

En løsningsmodel vedrørende restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud skal opfylde en række grundlæggende kriterier:

2.1.1. Praktisk anvendelighed

Det er væsentligt, at der findes en model, som vil virke i praksis, således at restaurationerne får et brugbart og effektivt redskab til at identificere gæster med restaurationsforbud. Det er i den forbindelse bl.a. vigtigt, at løsningen tager højde for, hvordan adgangs- og identitetskontrol foregår i praksis, herunder særligt på de større diskoteker og natklubber, hvor problemerne med at identificere gæster med restaurationsforbud navnlig opstår, jf. afsnit 1.2.3. ovenfor.

Løsningsmodellen bør endvidere så vidt muligt være kompatibel med de eksisterende gæsteregistrerings- og adgangskontrolsystemer, som allerede findes på mange diskoteker og natklubber, jf. afsnit 1.2.5. ovenfor, så det – i det omfang det er muligt – undgås, at restaurationsvirksomheder bliver nødt til at operere med flere adgangskontrolsystemer.

2.1.2. Retssikkerhed

Udvalget finder, at der skal være tale om en afbalanceret og retssikkerhedsmæssig forsvarlig løsningsmodel, som sikrer en fornuftig balance mellem hensynet til et trygt natteliv og til den enkeltes borgers retssikkerhed.

Udvalget lægger i den forbindelse vægt på, at der ikke bør foretages en unødvendig registrering og overvågning af restaurationsgæster i nattelivet. Det er desuden vigtigt, at der findes en løsningsmodel, som – så vidt muligt – er sikret mod fejl, herunder såkaldte "falske positive", der fører til uberettiget nægtelse af adgang i forbindelse med adgangskontrol i restaurationsvirksomheder.

Endelig finder udvalget det væsentligt, at ordningen ikke må være uproportionalt indgribende over for personer med restaurationsforbud.

2.1.3. Persondatasikkerhed

Udvalget finder det afgørende, at der findes en løsningsmodel, som er datasikkerhedsmæssigt forsvarlig, således at risikoen for misbrug af oplysninger er minimal. Udvalget lægger i den forbindelse bl.a. vægt på, at der ikke bør videregives flere personoplysninger end nødvendigt, ligesom personoplysninger kun bør videregives til en afgrænset personkreds.

2.1.4. Omkostnings- og ressourceeffektivitet

Udgifterne til ordningen skal stå mål med de resultater, som man kan påregne, at ordningen vil indebære i forhold til øget tryghed i nattelivet. Det bør endvidere generelt tilstræbes, at løsningen er så omkostnings- og ressourceeffektiv som mulig – både for restaurationsvirksomhederne og de involverede myndigheder.

2.2. En decentral eller en central løsning

Restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud kan sikres på flere måder.

En mulighed er en decentral løsning, hvor det overlades til den enkelte restauration, der måtte ønske det, på baggrund af oplysninger fra politiet at etablere et register over personer, der har forbud mod at komme på den pågældende restauration.

En anden mulighed er en central løsning, således at der oprettes et centralt register over personer med restaurationsforbud, som den enkelte restauration kan få on-line adgang til i forbindelse med sin adgangskontrol. Et sådant register vil kunne oprettes både i offentligt og i privat regi.

Den decentrale løsning vil i givet fald kunne kombineres med en central løsning, således at der både sker videregivelse af oplysninger om udstedte restaurationsforbud til den enkelte restauration og oprettes et centralt register, således at hver enkelt restaura-

tion afhængig af sit behov kan vælge, om den ønsker selv at føre et register over personer med restaurationsforbud, eller om den ønsker at benytte det centrale register.

Begge løsningsmodeller er som udgangspunkt baseret på frivillighed, således at det overlades til hver enkelt restauration at tage stilling til, i hvilket omfang virksomheden har behov for at føre kontrol med, om de gæster, der kommer ind på restaurationen, har fået et forbud mod at komme der, og om en sådan adgangskontrol i givet fald skal være baseret på registrerede oplysninger om personer med adgangsforbud.

Som omtalt ovenfor under kapitel 2, afsnit 1.7.2. vil det dog efter omstændighederne kunne medføre tilbagekaldelse af alkoholbevillingen, hvis bevillingshaveren undlader at føre tilstrækkelig adgangskontrol, jf. restaurationslovens § 19, stk. 1, nr. 2.

Er der tale om, at politiet ud over at give gæsten et forbud mod at komme i en restauration også har givet restauratøren et forbud mod at modtage gæsten, jf. restaurationslovens § 31, stk. 2, 2. pkt., skal restauratøren naturligvis så vidt muligt sikre, at vedkommende ikke får adgang til restaurationen, men bestemmelsen i restaurationslovens § 31, stk. 2, 2. pkt., indebærer ikke, som restaurationsloven er indrettet i dag, at restauratøren som led i håndhævelsen af dette forbud har pligt til at indføre en generel adgangskontrol eller at etablere eller være tilknyttet et register over personer med adgangsforbud. Det kunne overvejes at ændre restaurationsloven således, at restauratøren i højere grad får ansvar for at håndhæve restaurationsforbud over for gæsterne, men et sådant forslag, der som påpeget af Advokatrådets repræsentant også rejser mere principielle spørgsmål, falder uden for udvalgets kommissorium.

I det følgende beskrives den decentrale og den centrale løsningsmodel nærmere med angivelse af de fordele og ulemper, der er forbundet med de to modeller.

2.2.1. Den decentrale løsningsmodel

2.2.1.1. Grundlæggende idé

Én mulig løsning på problemet med at sikre restaurationer adgang til identitetsoplysninger på personer med restaurationsforbud vil være at etablere en formaliseret videregivelsesordning, hvorefter politiet, når der udstedes et restaurationsforbud, automa-

tisk orienterer den restauration eller de restaurationer, der er omfattet af forbuddet, om identiteten på den person, som har fået udstedt et forbud. Restaurationen, som modtager oplysningerne, vil herefter, såfremt den finder det hensigtsmæssigt, selv kunne registrere oplysningerne, herunder eventuelt i et gæsteregistreringssystem, jf. Datatilsynets afgørelse i Crazy Daisy-sagen omtalt under afsnit 1.2.5.2.

En sådan underretningsordning kræver ikke, at der oprettes et centralt register over personer, der har fået et restaurationsforbud. Hvis restauratøren ønsker at systematisere og registrere de oplysninger, der modtages fra politiet, når en person har fået forbud mod at komme i restaurationen, gør restauratøren det således selv. Der vil ikke være en pligt til at registrere oplysningerne. Den enkelte restauration må selv på baggrund af restaurationens størrelse og karakter mv. tage stilling til, om man har et behov for eller ønske om at registrere oplysningerne.

2.2.1.2. Hvilke oplysninger bør politiet videregive til restaurationerne ved den decentrale løsningsmodel?

De oplysninger, som politiet typisk vil være i besiddelse af om en person, som har fået et restaurationsforbud, vil være de oplysninger, der findes i de eksisterende registre mv. i politiets regi, herunder navnlig Kriminalregistret og politiets sagsstyringssystem, POLSAS.

De oplysninger, som vil skulle videregives til restaurationerne, vil som minimum skulle omfatte personens navn og oplysninger om forbuddets tidsmæssige udstrækning. Det vil også være hensigtsmæssigt – i forhold til adgangskontrol – at videregive CPR-nummer eller fødselsdato for de personer, som ikke har et dansk CPR-nummer. Oplysninger om, hvilket konkret strafbart forhold der ligger til grund for forbuddets udstedelse, bør derimod ikke videregives, da oplysningen ikke i sig selv har betydning for håndhævelsen af forbuddet.

2.2.1.2.1. Særlig om politiets videregivelse af personfotos

Spørgsmålet om, hvorvidt politiet skal videregive et personfotografi af den pågældende, kan også give anledning til overvejelse.

På den ene side vil det kunne være praktisk for en restauration at have et foto af de personer, der har fået forbud mod at komme der, idet det vil kunne lette identifikationen og modvirke fejltagelser og muligheden for at opgive falsk navn mv.

På den anden side bør politiet, fordi der er tale om fortrolige oplysninger om enkeltpersoners strafbare forhold, som udgangspunkt kun videregive de oplysninger, der er *nødvendige* for at sikre restaurationernes mulighed for at identificere personer med restaurationsforbud.

Det bemærkes i den forbindelse, at videregivelsen af personfotografier af sigtede personer til en større kreds må antages at indebære en ikke uvæsentlig risiko for misbrug, idet der bl.a. vil opstå risiko for, at billederne bliver fremvist for udenforstående, som måske genkender den pågældende og dermed bliver klar over, at personen er straffet.

Hertil kommer, at politiet i mange tilfælde ikke vil være i besiddelse af et foto af den person, der har fået et restaurationsforbud, idet sådanne fotos kun optages i nogle sager, jf. reglerne i retsplejelovens kapitel 72, som er beskrevet i kapitel 2, afsnit 2.1.

En person, der bliver sigtet for en mindre forbrydelse begået i en restauration, og som i den forbindelse får et restaurationsforbud, vil således almindeligvis ikke blive fotograferet af politiet. Medmindre den pågældende i forvejen er registreret med foto i politiets registre, fordi vedkommende tidligere har begået anden og mere alvorlig kriminalitet, vil politiet således ikke være i besiddelse af et foto af vedkommende.

Udvalget har ikke fundet anledning til at foreslå ændring i reglerne for politiets optagelse af personfotos af sigtede, jf. retsplejelovens kapitel 72, således at politiet skal optage fotos af alle personer, der sigtes for en – måske mindre – lovovertrædelse i en restauration og derfor får et restaurationsforbud. Et sådant forslag ville – ud over at forekomme uforholdsmæssigt – falde uden for udvalgets kommissorium.

På den anførte baggrund foreslår udvalget ikke en generel ordning, hvorefter politiet skal medsende et foto til restauratøren eller bestyreren, når politiet giver meddelelse om, at en person har fået forbud mod at komme i den pågældende restauration.

Udvalget har overvejet, om politiet i de tilfælde, hvor politiet allerede er i besiddelse af et foto af den pågældende person, bør sende fotoet til restauratøren, enten af egen drift eller efter anmodning. Udvalget er imidlertid uanset de fordele, der ville være forbundet med en sådan ordning, overvejende betænkelig herved. Det skyldes, at den oven for omtalte risiko for misbrug af fotos ikke effektivt vil kunne imødegås, hvis en kopi af fotoet er blevet sendt til den pågældende restauration. Politiets egen opbevaring af fotos af sigtede mv. er således som omtalt i kapitel 2, afsnit 2.2., underlagt strenge regler, der bl.a. indebærer, at fotos af personer, der bliver frifundet, eller mod hvem påtale bliver opgivet, skal destrueres, jf. herved retsplejelovens § 792 f, stk. 1. Hvis politiet videregiver fotos af en person, der har fået et restaurationsforbud, til vedkommende restauration, er der ikke sikkerhed for, at fotoet bliver destrueret, hvis den sigtelse mod personen, der har ført til restaurationsforbuddet, bliver opgivet, eller hvis personen bliver frifundet. I begge tilfælde skal restaurationsforbuddet som redegjort for i kapitel 2, afsnit 1, ophæves, men restaurationen vil fortsat være i besiddelse af fotoet af den pågældende. Restaurationen vil også fortsat være i besiddelse af fotoet af en person, der har fået et restaurationsforbud, når tidsfristen for forbuddet på typisk 2 år er udløbet.

En adgang for politiet til at videregive fotos af personer, der har fået et restaurationsforbud, til restauratører, vil under alle omstændigheder kræve særlig lovhjemmel, idet reglerne i retsplejelovens kap. 75 a (§§ 812 ff.), der er gennemgået i kapitel 2, afsnit 2.3., og som omhandler politiets efterforskningsskridt, ikke udgør tilstrækkelig hjemmel.

Det bemærkes, at der ikke vil være noget til hinder for, at vedkommende restauration selv – med fornødent samtykke – optager og registrerer fotos af de personer, der ønsker at komme ind på restaurationen, jf. herved afsnit 1.2.5.2. ovenfor om Datatilsynets afgørelse i sagen om Crazy Daisy. Når restaurationen senere modtager oplysninger fra politiet om, at en person har fået et restaurationsforbud, vil disse oplysninger kunne indføres i restaurationens eget register, hvor det tidligere optagne foto af den pågældende findes.

2.2.1.3. Hvordan skal videregivelse af oplysningerne ved den decentrale løsningsmodel ske

Politiets videregivelse af identitetsoplysninger bør foregå på skriftligt grundlag således, at restaurationerne har mulighed for at opbevare oplysningerne, herunder eventuelt indføre dem i deres eksisterende gæsteregistrerings- og adgangskontrolsystem.

For at mindske risikoen for at oplysningerne uretmæssigt videregives til andre, kan det overvejes, om fremsendelse skal ske med almindelig post, således at modtageren ikke – som det er tilfældet med elektronisk post – uden videre vil kunne videresende oplysningerne til en større persongruppe.

Det kan i den forbindelse overvejes, om fremsendelsen af oplysningerne i givet fald bør ske pr. anbefalet post, således at det sikres, at oplysningerne når frem til de personer, som skal have adgang til oplysningerne, jf. afsnit 2.2.1.4. nedenfor. Ved at fremsende oplysningerne med anbefalet post understreges det samtidig overfor modtageren, at der tale om oplysninger, som skal behandles på en særlig forsvarlig måde.

Såfremt oplysningerne videresendes med e-post, bør det sikres, at indholdet er krypteret i overensstemmelse med Datatilsynets retningslinjer.

Det bør desuden udtrykkeligt fremgå af brevet eller e-posten, at oplysningerne er fortrolige og alene må anvendes til at identificere gæster, som overtræder restaurationsforbud, og således ikke må videregives til uvedkommende.

2.2.1.4. Hvem skal have adgang til oplysningerne

Af datasikkerhedsmæssige årsager – og for at minimere risikoen for misbrug af personfølsomme oplysninger – bør videregivelsen af de ovenfor omtalte personoplysninger kun ske til en afgrænset kreds af personer:

2.2.1.4.1. Indehavere og bestyrere

Politiets videregivelse af identitetsoplysninger om personer med restaurationsforbud bør ske til en fysisk person i restaurationen, som herefter vil være ansvarlig for den

videre behandling af oplysningerne, herunder i fornødent omfang videregivelse til dørmænd og andre, jf. afsnit 2.2.1.4.2. og 2.2.1.4.3 nedenfor.

Videregivelsen bør efter udvalgets opfattelse enten ske til næringsbrevsindehaveren eller bestyreren, idet såvel næringsbrevsindehavere som bestyrere i virksomheder med alkoholbevilling skal opfylde en række nærmere angivne betingelser og være godkendt af bevillingsmyndigheden, jf. restaurationslovens § 13 og 15. Den risiko for misbrug og utilsigtet spredning, der er forbundet med, at politiet videregiver fortrolige oplysninger om personer med restaurationsforbud, må således antages at være mindre, når videregivelsen sker til en godkendt næringsbrevsindehaver eller bestyrer, end hvis videregivelsen (fremsendelsen) af oplysningerne sker til en ikke godkendt person eller til restaurationsvirksomheden som sådan uden angivelse af en fysisk person.

2.2.1.4.2. Dørmænd

På restaurationer med adgangskontrol vil det i praksis som oftest være dørmænd, der står for adgangskontrollen. Det gælder ikke mindst på de større diskoteker, hvor identifikationsproblemet særligt opstår, jf. afsnit 1.2.3. ovenfor.

Det må derfor anses for afgørende, at dørmændene får adgang til de identitetsoplysninger på personer med restaurationsforbud, som restaurationen (næringsbrevsindehaveren eller bestyreren) modtager fra politiet.

Betænkelighederne ved en ordning, hvorefter dørmændene får adgang til fortrolige oplysninger om, at enkeltpersoner har fået restaurationsforbud, begrænses af, at der ligesom for næringsbrevsindehavere og bestyrere gælder en særlig godkendelsesordning for dørmænd i virksomheder med alkoholbevilling. Efter restaurationslovens § 15 a skal sådanne dørmænd således være autoriserede af politiet.

Betingelserne for at opnå autorisation som dørmand fremgår af restaurationslovens § 15 a, stk. 2, hvorefter autorisation kan meddeles personer, som opfylder en række krav til alder og vandel og om gennemførelse af en særlig uddannelse.

For så vidt angår uddannelseskravet fremgår det af bekendtgørelse nr. 247 af 11. april 2008 om dørmænd, at kravet om uddannelse er opfyldt, hvis ansøgeren har fremlagt

bevis for gennemførelse af arbejdsmarkedsuddannelsen som dørmand efter de af Undervisningsministeriet fastsatte regler herom. Arbejdsmarkedsuddannelsen som dørmand varer 8 dage og omfatter bl.a. undervisning i service, kommunikation og samarbejde, forebyggelse og afværgelse af konflikter samt førstehjælp og brandbekæmpelse. I uddannelsen indgår undervisning i relevant lovgivning, herunder restaurationsloven, straffeloven og lov om diskrimination. Uddannelsen afsluttes med en individuel prøve af ca. 45 minutters varighed.

Hvervet som dørmand kan endvidere ifølge restaurationslovens § 15 a, stk. 3, varetages af personer, som i henhold til lov om vagtvirksomhed er autoriseret til at drive vagtvirksomhed og af en vagtvirksomheds godkendte personale. Kravene for at blive autoriseret til at drive vagtvirksomhed eller godkendt som vagtpersonale, herunder krav til uddannelse mv., er fastlagt i lovgivningen om vagtvirksomhed.

En afvejning af de modstående hensyn – på den ene side nødvendigheden af, at dørmænd i fornødent omfang kan få adgang til de pågældende oplysninger, og på den anden side de principielle betænkeligheder ved, at fortrolige oplysninger spredes yderligere – synes på baggrund af de krav, der gælder for dørmænd, at måtte føre til, at det er forsvarligt at indføre en ordning, hvorefter næringsbrevsindehaveren eller bestyreren kan videregive de identitetsoplysninger på personer med restaurationsforbud, der modtages fra politiet, til dørmændene ved adgangskontrollen.

2.2.1.4.3. Andre end næringsbrevsindehavere, bestyrere og dørmænd

Det må overvejes, om der er behov for, at andre end næringsbrevsindehavere, bestyrere og dørmænd får adgang til de identitetsoplysninger på personer med restaurationsforbud, som politiet efter den decentrale løsningsmodel skal videregive til restaurationerne.

Spørgsmålet er særlig aktuelt for restaurationer uden adgangskontrol og dermed normalt uden dørmænd, idet der i næringsbrevsindehaverens eller bestyrerens fravær ikke vil være nogen til at kontrollere, om en person har fået et forbud mod at komme i restaurationen. De personalegrupper, der kunne blive tale om i sådanne tilfælde at give adgang til de modtagne identitetsoplysninger fra politiet, er bartendere og serveringspersonale mv.

Restaurationsvirksomheder uden adgangskontrol vil bl.a. være mindre værtshuse og udskænkningssteder og virksomheder, hvor der efter stedets karakter ikke er behov for adgangskontrol som f.eks. spiserestauranter, bistroer, caféer mv. Som anført i afsnit 1.2.3. må det antages, at problemet med identifikation af personer med restaurationsforbud særligt er aktuelt på større diskoteker og natklubber, hvor et betydeligt antal personer har forbud mod at opholde sig. På disse steder vil der typisk være adgangskontrol med dørmænd. Det kan dog langtfra udelukkes, at tilsvarende problemer efter omstændighederne også vil kunne opstå i restaurationsvirksomheder, som ikke har adgangskontrol, og at det i disse situationer vil være relevant, at andre medarbejdere end næringsbrevsindehavere, bestyrere og dørmænd også kan få adgang til identitetsoplysninger på personer med restaurationsforbud.

Videregivelse af identitetsoplysninger til en sådan større ubestemt personkreds giver dog anledning til betænkeligheder, bl.a. fordi det må antages, at risikoen for misbrug og utilsigtet spredning er større, når videregivelsen sker til medarbejdere, som – i modsætning til dørmænd – ikke er underlagt særlige autorisations- og uddannelseskrav

Af samme grund finder udvalget ikke, at det vil være forsvarligt at indføre en generel ordning, hvorefter næringsbrevsindehaveren eller bestyreren uden videre kan videregive de identitetsoplysninger på personer med restaurationsforbud, der modtages fra politiet, til andre medarbejdere i restaurationen end dørmændene ved adgangskontrollen.

På den anden side finder udvalget, at det vil være forkert helt at udelukke muligheden for, at næringsbrevsindehaveren eller bestyreren i restaurationer uden adgangskontrol kan videregive identitetsoplysningerne til andre medarbejdere.

Udvalget foreslår, at problemet løses ved, at der fastsættes en række specifikke krav til, under hvilke betingelser næringsbrevsindehaveren og bestyreren må videregive identitetsoplysninger til andre medarbejdere end dørmænd. Vilkårene bør som udgangspunkt svare til de vilkår, som Datatilsynet har fastsat til medarbejderes adgang til registrerede oplysninger i Crazy Daisy-afgørelsen, og de vilkår om sikkerhed i for-

bindelse med diskotekers anmeldelse af registrering af karantæneoplysninger, der efterfølgende er blevet udarbejdet, jf. afsnit 1.2.5.2. og 1.2.5.3. ovenfor.

2.2.1.5. Indførelse af en særlig tavshedspligt

En ordning, der indebærer, at politiet skal videregive identitetsoplysninger på personer med restaurationsforbud til vedkommende restauration (næringsbrevsindehaver eller bestyrer), bør af hensyn til at mindske risikoen for misbrug og spredning af oplysningerne forudsætte, at der indføres regler om tavshedspligt for næringsbrevsindehavere, bestyrere, dørmænd og andre, som oplysningerne vil kunne videregives til, jf. afsnit 2.2.1.4.2. og 2.2.1.4.3.

En tilsvarende ordning kendes fra lov nr. 307 af 30. april 2008 om sikkerhed ved bestemte idrætsbegivenheder, hvor der i § 6, stk. 3, er fastsat regler om tavshedspligt for de autoriserede kontrollører, som politiet kan videregive karantæneoplysninger til. I bestemmelsen er det fastsat, at kontrollørerne har tavshedspligt med hensyn til disse oplysninger, og at straffelovens § 152 og § 152 c - 152 f finder tilsvarende anvendelse. Bestemmelsen indebærer således, at det vil være strafbart for kontrollørerne uberettiget at videregive oplysningerne til andre.

Det vil som efter lov om sikkerhed ved bestemte idrætsbegivenheder kun være den *uberettigede* videregivelse af oplysninger, der skal strafbelægges. Næringsbrevsindehaverens og bestyrerens videregivelse af oplysninger til dørmændene vil således være berettiget og dermed ikke strafbelagt. Det samme vil efter omstændighederne kunne være tilfældet for videregivelse til andre medarbejdere, jf. afsnit 2.2.1.4.3. Tilsvarende vil en dørmands videregivelse af oplysninger til en anden dørmand i en afløsningssituation eller lignende efter omstændighederne også være berettiget.

2.2.1.6. Indførelse af særlige uddannelseskrav

Under hensyn til, at det i praksis først og fremmest vil være dørmænd, der vil skulle behandle de identitetsoplysninger på personer med restaurationsforbud, der modtages fra politiet, kan det overvejes som et led i den obligatoriske dørmandsuddannelse og eventuelt også vagtmandsuddannelsen, jf. afsnit 2.2.1.4.2, at indføre krav om undervisning i behandling af personfølsomme oplysninger, således at det sikres, at dør-

mænd (og vagter) bedre bliver i stand til på forsvarlig måde at håndtere sådanne oplysninger.

2.2.1.7. Fordele ved den decentrale løsningsmodel

Fordelen ved den decentrale løsningsmodel, hvorefter politiet giver en individuel underretning til restaurationen om identiteten på personen, der har fået forbud mod at komme på restaurationen, er først og fremmest, at ordningen er enkel og billig at administrere og ikke forudsætter opbygning af et centralt register.

For mindre restaurationsvirksomheder har ordningen endvidere den betydelige fordel, at det ikke som ved den centrale løsningsmodel er nødvendigt at bruge ressourcer i form af edb-udstyr og oplæring på at få adgang til oplysningerne. Oplysningerne kommer med posten, eller evt. pr. mail, jf. afsnit 2.2.1.3., og det er herefter op til næringsbrevsindehaveren eller bestyreren at tage stilling til, hvilken brug der skal gøres af oplysningerne.

Oplysningerne vil desuden uden videre kunne indføres i de gæsteregistreringssystemer, som restaurationen måtte have i forvejen, jf. herved Datatilsynets afgørelse i Crazy Daisy-sagen omtalt i afsnit 1.2.5.2.

2.2.1.8. Ulemper ved den decentrale løsningsmodel

Den væsentligste ulempe ved den decentrale løsningsmodel er, at den gør det nødvendigt for restaurationerne selv at oprette et register, som de modtagne oplysninger om personer med restaurationsforbud kan indføres i.

Det vil ganske vist være frivilligt for restaurationerne, om de ønsker at oprette et sådant register, men hvis de vil kunne gøre systematisk brug af de oplysninger, de modtager fra politiet, vil oprettelsen af en eller anden form for eget register i mangel på et centralt register være en nødvendighed.

Restaurationernes registre vil skulle anmeldes til Datatilsynet og leve op til Datatilsynets vilkår mv.

For de – navnlig større – restaurationsvirksomheder, for hvilke det ikke vil være noget problem at sikre opkobling på et centralt register, vil det kunne være en ulempe ved den decentrale løsningsmodel, at virksomheden selv vil skulle behandle de oplysninger, der modtages fra politiet. For så vidt angår de restaurationer, der allerede har et gæsteregistreringssystem, jf. afsnit 1.2.5. ovenfor, vil der dog være tale om en forholdsvis begrænset opgave, idet de alene vil skulle indføre oplysningerne i det eksisterende system.

En anden ulempe ved den decentrale løsningsmodel er, at Datatilsynets mulighed for at føre kontrol med registrerede oplysninger om personer med restaurationsforbud vil være ringere, hvis oplysningerne findes i restaurationsvirksomhedernes egne registre, end hvis de findes i et centralt register hos politiet eller i et fælles centralt privat register.

Endelig kan det anføres, at risikoen for misbrug og spredning af oplysningerne vil være større ved den decentrale løsningsmodel, hvor de fortrolige oplysninger sendes til restaurationerne med henblik på indførelse i restaurationernes egne registre, frem for ved den centrale løsningsmodel, hvor de fortrolige oplysninger bliver indlagt i et centralt register. Betydningen af denne risiko bør dog ikke overbetones, idet den i væsentligt omfang imødegås ved at begrænse kredsen af modtagere af oplysningerne til næringsbrevsindehavere, bestyrere, dørmænd og evt. andre og ved at fastsætte regler om tavshedspligt og strafansvar mv., jf. afsnit 2.2.1.4.1 - 2.2.1.4.3 og 2.2.1.5. ovenfor.

2.2.2. Centrale løsningsmodeller

2.2.2.1. Adgang til et centralt offentligt register med oplysninger om restaurationsforbud

En anden mulig løsning på problemet med at sikre restaurationer adgang til identitetsoplysninger på personer med restaurationsforbud vil være at etablere et centralt offentligt register over sådanne personer, som restaurationerne vil kunne få on-line adgang til i forbindelse med deres adgangskontrol.

2.2.2.1.1. Dataansvar

Det vil efter udvalgets opfattelse være nærliggende at lade Rigspolitiet føre et sådant offentligt register, da registret vil bestå af oplysninger, politiet allerede er i besiddelse af. Som omtalt ovenfor findes identitetsoplysninger på personer med restaurationsforbud således navnlig i Det Centrale Kriminalregister. Desuden vil registret overordnet set kunne siges at have et politimæssigt sigte, idet formålet med registret vil være at sikre en bedre håndhævelse af restaurationsforbud udstedt af politiet i medfør af restaurationslovens § 31, stk. 2.

Politiet fører allerede i dag flere registre, som indeholder personoplysninger vedrørende strafbare forhold. Udover Kriminalregistret drejer det sig bl.a. om Fingeraftryksregistret og DNA-registret.[7] Bortset fra Kriminalregistret – som enkelte andre myndigheder har adgang til – er det alene politiet, som kan søge i disse registre. Der kendes ingen eksempler på, at privatpersoner og virksomheder har adgang til de omtalte registre.

Det vil ifølge Rigspolitiet både give anledning til alvorlige principielle betænkeligheder og væsentlige praktiske vanskeligheder at sikre restaurationsvirksomheder direkte elektronisk adgang til Kriminalregistrets oplysninger om restaurationsforbud.

Rigspolitiet har i den forbindelse påpeget, at Kriminalregistret indeholder særdeles personfølsomme oplysninger, som det er afgørende ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen. Såfremt det tillades, at private får direkte adgang til registret, vil det ifølge Rigspolitiet uundgåeligt indebære en generelt øget risiko for misbrug mv. Hertil kommer, at løsningen vil være meget omkostningskrævende for restaurationsvirksomhederne, idet restaurationerne vil skulle indføre omfattende sikkerhedsforanstaltninger så som bl.a. sikre dataforbindelser og særlige terminaler mv.

[7] Bekendtgørelse nr. 218 af 27. marts 2001 om behandling af personoplysninger i Det Centrale Register (Kriminalregistret), som ændret ved bekendtgørelse nr. 782 af 12. august 2005, bekendtgørelse nr. 1030 af 13. oktober 2006, bekendtgørelse nr. 137 af 12. december 2006 og bekendtgørelse nr. 679 af 20. juni 2007.

Endelig vil løsningen med direkte adgang til Kriminalregistret indebære, at der skal gennemføres grundlæggende ændringer i Kriminalregistrets opbygning mv. Rigspolitiet har i den forbindelse bemærket, at en "hit - no hit" løsning, som omtalt nedenfor i afsnit 2.2.2.1.2., umiddelbart vil kræve, at oplysningerne om restaurationsforbud i registret it-teknisk er linket til den eller de konkrete restaurationer, og at de relevante næringsbrevsindehavere, bestyrere, dørmænd og eventuelt andre ligeledes er linket til den bestemte restauration, hvilket ikke er tilfældet i Kriminalregistret i dag. Dette rejser en række – formentlig ganske komplicerede – spørgsmål dels i forhold til administrationen af brugeradgangen til registret, dels i forhold til opdateringen af registret med de relevante forbud.

En anden løsning vil være at overføre de relevante oplysninger fra Kriminalregistret – og eventuelt politiets sagsstyringssystem – til et nyt særskilt register, hvortil kun restaurationsvirksomheder vil have adgang. En sådan overførsel af oplysninger vil dog indebære en række af de samme tekniske udfordringer, som er omtalt ovenfor, og formentlig være behæftet med ikke ubetydelige udgifter.

2.2.2.1.2. Registrets indhold og funktion

Såfremt der oprettes et centralt offentligt register med oplysninger om personer med restaurationsforbud, vil restaurationerne som udgangspunkt alene have behov for at få et "ja" eller "nej" til, om den person, der søges på i det centrale register, har forbud mod at komme på netop denne restauration ("hit - no hit"). Det centrale register vil derfor kun skulle indeholde de oplysninger, der er nødvendige for, at en søgning på en bestemt person kan besvares med et "ja" eller "nej".

Det må antages, at registret – for at kunne levere et sådant svar – som minimum vil skulle indeholde oplysninger om CPR-numre på personer med restaurationsforbud samt oplysninger om, hvor og hvor længe de enkelte forbud gælder. Hvilke oplysninger, der vil skulle indgå i et centralt register, vil dog i sidste ende bl.a. afhænge af, hvilken teknisk løsning der vælges, jf. afsnit 2.2.2.5. nedenfor.

Et sådant elektronisk "hit – no hit" register vil eventuelt kunne være omfattet af persondatalovens § 39 om indsigelsesret overfor automatiserede afgørelser. Der ses ikke at foreligge afgørelser fra Datatilsynet herom. I givet fald vil det forudsætte, at en

gæst, som får et "nej", i hvert fald i et vist omfang har mulighed for at få afgørelsen vurderet af personalet på stedet, jf. kapitel 2, afsnit 3.1.4.

2.2.2.1.3. Hvem skal have adgang til registret

En oplysning om, at en person har fået et restaurationsforbud, er en fortrolig oplysning. Det gælder, selv om registret indrettes således, at der alene svares "ja" eller "nej" til et spørgsmål om, hvorvidt den person, der søges på, har forbud mod at komme i den pågældende restauration. Adgangen til at søge i et offentligt register bør derfor som udgangspunkt begrænses til næringsbrevsindehavere, bestyrere og dørmænd. I visse særlige situationer bør andre medarbejdere dog også kunne få adgang til oplysningerne. Om baggrunden herfor henvises til det, der er anført i afsnit 2.2.1.4.1 - 2.2.1.4.3. om videregivelse af oplysninger efter den decentrale løsningsmodel. Der henvises endvidere til afsnit 2.2.1.5 om indførelse af en særlig tavshedspligt for næringsbrevsindehavere, bestyrere, dørmænd og andre.

2.2.2.1.4. Tekniske løsningsmodeller

Et centralt offentligt register med oplysninger om restaurationsforbud vil kunne indrettes på flere måder.

Som omtalt ovenfor under afsnit 2.2.2.3. bør systemet af datasikkerhedsmæssige årsager under alle omstændigheder indrettes som et "hit - no hit"-system, hvorefter restaurationerne på baggrund af en forespørgsel kan få be- eller afkræftet, om en bestemt person aktuelt har forbud mod at komme i den pågældende restauration, jf. restaurationslovens § 31, stk. 2.

For at ordningen vil kunne fungere optimalt, vil det være nødvendigt, at restaurationerne får direkte elektronisk adgang til oplysningerne i registret.

En løsning som f.eks. indebærer, at restaurationerne i hvert enkelt tilfælde skal rette forespørgsel telefonisk til Rigspolitiet, vil således ikke kunne fungere i praksis, idet det både vil tage for lang tid og være for besværligt for restaurationen at få adgang til oplysningen om, hvorvidt en bestemt person er omfattet af restaurationsforbud.

Dansk Erhverv, Horesta og Sikkerhedsbranchen har i den forbindelse understreget, at det er en afgørende forudsætning for, at en central registerordning kan fungere i praksis, at den tager højde for, hvordan adgangs- og identitetskontrol foregår i praksis på de restaurationer, hvor problemerne med at identificere gæster med restaurationsforbud typisk opstår, dvs. på de større natklubber og diskoteker.

2.2.2.1.5. Biometribaseret register

Som omtalt ovenfor i afsnit 1.2.5. har en række diskoteker og natklubber allerede indført egne – typisk fingeraftryksbaserede – gæsteregistreringssystemer. Som det endvidere er omtalt i afsnit 1.2.5.2., fastslog Datatilsynet i den såkaldte "Crazy Daisy"-afgørelse, at denne type systemer – såfremt visse betingelser er opfyldt – kan etableres inden for rammerne af persondataloven.

I praksis fungerer denne type gæsteregistreringssystemer almindeligvis på den måde, at gæsten – første gang vedkommende indfinder sig på diskoteket – efter at have givet samtykke hertil lader sig registrere med navn, adresse og CPR-nummer. Samtidig optager restaurationen elektronisk et personfotografi og et elektronisk fingeraftryk i form af en template af personen. En template er, som der er redegjort for i afsnit 1.2.5.2., en matematisk beregnet værdi – men ikke en kopi – af et fingeraftryk. Et indscannet fingeraftryk kan således genkendes, når personen næste gang vil ind på restaurationen, men fingeraftrykket kan ikke gendannes og dermed kopieres.

Når gæsten efterfølgende besøger restaurationen, foregår adgangskontrollen alene ved, at personen lader sit fingeraftryk scanne, hvorefter systemet fremkalder de oplysninger, som restaurationen er i besiddelse af vedrørende den pågældende.

For en nærmere beskrivelse af det registreringssystem, som anvendes af diskotekskæden Nox Network, henvises til afsnit 1.2.5.1. ovenfor.

Fordelen ved kontrolsystemer baseret på biometri – som f.eks. genkendelse af fingeraftryk – er navnlig, at restaurationen kan gennemføre adgangskontrol af gæsterne på en ensartet og meget hurtig måde, idet det hverken er nødvendigt for dørmanden at kontrollere identitetspapirer eller foretage manuelle opslag mv. Dørmanden vil såle-

des straks få oplyst, om den pågældende gæst er i systemet, og om pågældende derfor umiddelbart kan tildeles adgang til restaurationen.

En anden fordel ved disse systemer er, at diskotekerne – ved at kunne gennemføre adgangskontrollen hurtigt og effektivt – ofte kan undgå, at der opstår lange køer uden for diskoteket, hvilket erfaringsmæssigt ofte fører til optrin og frustrationer.

Ifølge Horesta er diskoteksbranchens erfaring endvidere, at antallet af såvel fysiske som verbale overfald på vagtpersonale og dørmænd reduceres, når der indføres denne form for automatiseret adgangskontrol, idet det ikke på samme måde som tidligere er dørmanden, som over for gæsten fremstår som den, der administrerer forbud og karantæner mv.

Udvalget har i lyset heraf overvejet muligheden for at indføre et centralt register baseret på biometrisk adgangskontrol.

Udvalget har i den forbindelse taget udgangspunkt i en fingeraftryksbaseret løsning, idet andre former for biometrisk kontrol efter det oplyste endnu ikke er ligeså veludviklede. Fingeraftryksbaserede adgangskontrolsystemer anvendes som omtalt allerede i dag på en række diskoteker mv.

Efter at have overvejet spørgsmålet nærmere er det udvalgets opfattelse, at en sådan løsning vil give anledning til en række både principielle og praktiske betænkeligheder.

Som anført ovenfor i kapitel 2, afsnit 2.1., kan politiet efter de nugældende regler i retsplejeloven kun optage fingeraftryk af en sigtet, hvis det er nødvendigt for efterforskningen, eller hvis der er tale om en alvorlig forbrydelse. Dette indebærer, at en person, der bliver sigtet for en mindre lovovertrædelse begået på en restauration, og som i den forbindelse får et restaurationsforbud, i de fleste tilfælde ikke vil få optaget fingeraftryk af politiet.

Efter udvalgets opfattelse vil det – ud over at forekomme ganske vidtgående – også falde uden for udvalgets kommissorium at foreslå ændring af reglerne om politiets optagelse af fingeraftryk mv. i retsplejelovens kapitel 72, således at politiet fremover

vil skulle optage fingeraftryk af alle personer, der sigtes for en – måske mindre – lovovertrædelse på en restauration og derfor får et restaurationsforbud.

Hertil kommer, at en fingeraftryksbaseret løsning vil indebære en række praktiske vanskeligheder. Optagelse af fingeraftryk sker således i dag på politistationen med anvendelse af særligt udstyr og blanketter mv. Når politiet udsteder restaurationsforbud til en restaurationsgæst, sker det i dag ofte på stedet, det vil sige i restaurationen eller på gaden foran restaurationen. Kun i visse tilfælde – typisk når der er tale om mere alvorlige lovovertrædelser, eller når der er spørgsmål om detentionsanbringelse – vil personen blive indbragt på politistationen.

Hvis der vil skulle optages fingeraftryk af alle personer, som får restaurationsforbud i medfør af restaurationslovens § 31, stk. 2, vil det enten kræve, at personerne i alle tilfælde bliver indbragt til en politistation, hvor der kan optages fingeraftryk, eller at politiet anskaffer særligt udstyr, således at politipatruljer kan optage fingeraftryk på stedet. Uanset hvilken løsning der vælges, vil det være omkostningskrævende og upraktisk.

Det bemærkes i den forbindelse, at det ikke vil være en mulighed at lade politiet benytte restaurationens fingeraftrykksscanner til at optage fingeraftryk. Det skyldes bl.a., at denne scanner i sagens natur befinder sig ved indgangen, og det vil være et fundamentalt brud på almindelige diskretionshensyn, hvis en sigtet person vil skulle tvinges til at få taget sit fingeraftryk et sted, hvor der er uvedkommende personer til stede.

Endelig må det antages, at der vil være ganske betydelige udgifter forbundet med efterfølgende at behandle og opbevare de biometriske data (fingeraftrykkene) i et elektronisk register, hvortil restaurationerne skal have direkte adgang.

Sammenfattende er det herefter udvalgets opfattelse, at en central fingeraftryksbaseret løsning hverken vil være praktisk eller retssikkerhedsmæssigt forsvarlig.

2.2.2.1.6. CPR-baseret register

Den alternative løsning vil være at indføre et CPR-baseret system, hvor restaurationsvirksomheder ved søgning på CPR-nummer i et register kan få oplyst, om den pågældende person er omfattet af et aktuelt restaurationsforbud det pågældende sted.

Et sådant register vil alene skulle indeholde oplysninger om, hvilke personer der aktuelt er omfattet af restaurationsforbud, og hvilke restaurationer forbuddene vedrører.

Man kunne eksempelvis forestille sig en internetbaseret løsning, hvor Rigspolitiet overfører de relevante oplysninger fra Kriminalregistret – og eventuelt politiets sagsstyringssystem (POLSAS) – til et særskilt elektronisk register, hvortil der kan opnås adgang via internettet. Næringsbrevsindehaveren eller bestyreren får herefter fra politiet udleveret en individuel log-in og adgangskode (og eventuelt også tokenkode), hvorefter restaurationen via internettet kan sende forespørgsler til registret.

En fordel ved en sådan internetbaseret løsning vil være, at restauratørerne selv vil kunne beslutte, hvordan de etablerer adgang til registret.

Man kunne f.eks. forestille sig, at nogle – navnlig mindre – restaurationsvirksomheder alene vil have behov for at søge i registret lejlighedsvis og derfor blot vil benytte eksisterende internetfaciliteter i virksomheden. Omvendt vil eksempelvis større diskoteker – som ønsker at bruge oplysningerne fra registret på mere systematisk vis i forbindelse med adgangskontrol – kunne opsætte computerterminaler med internetadgang ved indgangen, således at dørmændene løbende kan foretage søgninger i registret.

Restaurationer som eksempelvis ønsker at kontrollere alle gæster – og som derfor har behov for at foretage hurtige søgninger i registret – vil kunne tilkoble sygesikringskortlæsere (eller andre ID-kortlæsere), således at der automatisk gennemføres en søgning i det centrale register, når personens sygesikringskort (eller eventuelt andet ID-kort) køres gennem en aflæsningsterminal. Dermed sikres det, at disse restaurationer vil kunne gennemføre en hurtig og ensartet kontrol af alle gæster.

Et CPR-baseret system har dog den betydelige ulempe, at det vil være vanskeligt for restaurationerne at sikre, at det CPR-nummer, som en gæst oplyser, rent faktisk er det

rigtige, eller at et sygesikringskort mv., der fremvises eller køres gennem en kortlæser ved adgangskontrollen, rent faktisk er vedkommendes eget kort og ikke et kort, som vedkommende har lånt eller stjålet.

Hertil kommer, at et CPR-baseret system ikke uden videre vil kunne anvendes på udlændinge, som ikke har noget dansk CPR-nummer.

2.2.2.2. Oprettelse af et fælles privat register med oplysning om restaurationsforbud

Udvalget har overvejet muligheden for, at restaurationsbranchen – som en alternativ løsning til et centralt offentligt register – opretter sit eget register over personer med restaurationsforbud, som enhver restaurationsvirksomhed, der ønsker det, kan få online adgang til.

Denne løsning skal ses i lyset af Datatilsynets afgørelse i Crazy Daisy-sagen, jf. afsnit 1.2.5.2. ovenfor, hvor Datatilsynet i en konkret sag gav tilladelse til, at en restaurationsvirksomhed med henblik på adgangskontrol – med gæsternes udtrykkelige samtykke – kunne registrere billeder, fingeraftryk (templates) og andre oplysninger af følsom karakter.

Afgørelsen indebærer efter udvalgets opfattelse, at det som udgangspunkt er muligt at lave et landsdækkende privat register, der i det store og hele virker som en reduceret udgave af de gæsteregistreringssystemer, som allerede anvendes flere steder i diskoteksbranchen, jf. afsnit 1.2.5. ovenfor, men som i modsætning til de eksisterende systemer er tilgængeligt for alle restaurationsvirksomheder, der ønsker det. I registret vil der skulle være oplysninger fra politiet om, hvilke personer der har fået forbud mod at komme i en bestemt restauration.

Dansk Erhverv og Horesta har oplyst, at man fra branchens side kan se en række fordele ved et fælles privat register med oplysninger om restaurationsforbud, jf. også nedenfor under afsnit 2.2.2.2.4. Man kan derfor fra branchens side generelt støtte ideen om oprettelsen af et sådant register, idet man dog ikke på nuværende tidspunkt kan udtale sig om, hvem der i givet fald skal stå for oprettelsen og driften af registret.

2.2.2.2.1. Dataansvar

Efter udvalgets opfattelse vil det være nærliggende at lade branchen selv stå for oprettelsen og driften af et fælles privat register med oplysninger om restaurationsforbud.

Udvalget finder imidlertid ikke, at det på nuværende tidspunkt er muligt at udtale sig nærmere om, hvem der skal oprette og stå for driften af et fælles privat register, idet løsningen ikke er færdigudviklet, og idet de økonomiske omkostninger forbundet med oprettelsen og driften ikke er tilstrækkelig oplyst. Udvalget opfordrer dog til, at branchen inddrages, når den registeransvarlige for et fælles privat register skal udpeges.

Det vil desuden skulle overvejes, om reglerne om udbud finder anvendelse.

Udvalget finder det afgørende, at en fælles privat registerløsning, uanset hvilken brancheorganisation mv., som står for oprettelsen og driften, ikke må begrænses til virksomheder, som er medlemmer af en bestemt brancheorganisation, men bør være tilgængelig for alle interesserede virksomheder, eventuelt mod et gebyr fastsat på grundlag af de udgifter, der er forbundet med administrationen og driften af registret.

Den dataansvarlige vil skulle anmelde registret til Datatilsynet og leve op til en række sikkerhedskrav, jf. bl.a. Datatilsynets vilkår om sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger

2.2.2.2.2. Registrets indhold

Som omtalt ovenfor under afsnit 2.2.2.1.2 vil restaurationerne som udgangspunkt alene have behov for at få et "ja" eller "nej" til, om den person, der søges på i det centrale register, har forbud mod at komme på netop denne restauration ("hit - no hit").

I modsætning til hvad der er tilfældet med et offentligt register, vil det i et privat register – med gæsternes udtrykkelige samtykke – være muligt at registrere identitetsoplysninger som f.eks. fotografi og fingeraftryk (templates), jf. herved afsnit 1.2.5.2.

Sådanne oplysninger vil kunne sikre, at der kan udføres en ensartet og meget hurtig adgangskontrol af gæsterne

2.2.2.2.3. Hvem skal have adgang til registret

Adgangen til at søge i et fælles privat register, som indeholder oplysninger om restaurationsforbud, bør begrænses på samme måde som adgangen til et centralt offentligt register, jf. afsnit 2.2.2.1.3.

Der henvises endvidere til afsnit 2.2.1.5. om indførelse af en særlig tavshedspligt for næringsbrevsindehavere, bestyrere, dørmænd og andre.

2.2.2.2.4. Registrets funktion

Såfremt restaurationsbranchen opretter et fælles register over personer med restaurationsforbud, vil det kunne fungere stort set på samme måde som de gæsteregistreringssystemer, der allerede anvendes på visse større diskoteker som f.eks. MasterClub omtalt under afsnit 1.2.5.1.

Første gang en gæst besøger en restauration – som er tilknyttet registret – vil vedkommende blive registreret med navn, CPR-nummer, fotografi og evt. fingeraftryk (template, jf. om dette begreb afsnit 2.2.2.1.5.). Registrering vil kunne foregå elektronisk og gennemføres på få minutter. Gæsten vil skulle give udtrykkeligt samtykke både til registreringen og den efterfølgende anvendelse af oplysningerne.

Ud fra de registrerede oplysninger vil der blive forespurgt i den centrale database, om gæsten har forbud mod at opholde sig på den pågældende restauration, jf. restaurationslovens § 31, stk. 2 (”hit - no hit”). Hvis dette ikke er tilfældet, vil gæsten kunne få adgang til restaurationen.

Når gæsten efterfølgende besøger restaurationer, som er tilknyttet registret, vil vedkommende automatisk blive identificeret i adgangskontrollen, f.eks. via fingeraftryk eller sygesikringskortlæser. Samtidig vil der blive forespurgt i registret, om vedkommende er meddelt et restaurationsforbud, som omfatter det pågældende sted.

Det vil være op til den enkelte restaurationsvirksomhed at afgøre, om gæster, som ikke ønsker at lade sig registrere, alligevel skal kunne få adgang til restaurationen.

2.2.2.2.4.1. Registrering af oplysninger om interne karantæner mv.

En anden fordel ved et fælles privat register vil være, at registret efter omstændighederne også vil kunne bruges til registrering af andre oplysninger end oplysninger om restaurationsforbud. Eksempelvis kunne man forestille sig, at nogle restaurationer vil have et ønske om at registrere gæster, som har fået meddelt intern karantæne på grund af dårlig opførsel på restaurationen.

Datatilsynet har i Crazy Daisy-afgørelsen omtalt i afsnit 1.2.5.2. ovenfor lagt til grund, at restaurationer i situationer, hvor en gæst meddeles karantæne på grund af sin adfærd, uden samtykke kan registrere navn og adresse på vedkommende samt oplysninger om, hvor længe personen er uønsket som gæst, jf. persondatalovens § 6, stk. 1, nr. 7.

Ønsker restaurationen derimod at registrere karantæneårsagen – f.eks. for at kunne forklare personen, hvorfor vedkommende ikke kan blive lukket ind på diskoteket – vil det kræve gæstens skriftlige samtykke, da der kan være tale om registrering af følsomme personoplysninger (oplysninger om strafbare forhold og narkotikamisbrug mv.), jf. persondatalovens § 8, stk. 3, jf. § 5, stk. 1. Samtykket skal være udtrykkeligt og skal opfylde persondatalovens krav, jf. herved kapitel 2, afsnit 3.1.2.3. Hvis den registrerede tilbagekalder samtykket, medfører persondatalovens § 38, at oplysningerne om årsagen til karantænen skal slettes.

2.2.2.2.4.2. Udveksling af oplysninger om restaurationsforbud og karantæner

Som tidligere anført bør restauratører kun have mulighed for at få adgang til oplysninger om restaurationsforbud vedrørende den pågældende restauration.

Såfremt et fælles privat register med oplysninger om restaurationsforbud indrettes på en sådan måde, at restauratørerne også har adgang til oplysninger om restaurationsforbud på andre restaurationer, vil registret få karakter af et advarselsregister, hvis formål er at videregive oplysninger om registrerede personer til de deltagende restauratører med henblik på, at de kan undlade at lukke dem ind på deres restauration.

Datatilsynet afviste i juli 2008 en ansøgning fra en konkret virksomhed, som netop ønskede at lave en fælles advarselsliste, hvor diskoteker gennem virksomhedens webside kunne se, hvilke gæster andre diskoteker afviste. Datatilsynets afgørelse er medtaget som bilag 4 til denne betænkning. Datatilsynet lagde i sin afgørelse vægt på, at der ikke inden for rammerne af persondatalovens § 8, stk. 4 og 5, og § 8, stk. 6, jf. § 7 kunne ske videregivelse og registrering af oplysninger om strafbare forhold eller andre følsomme oplysninger i et advarselsregister som det påtænkte.

I lyset heraf finder udvalget ikke, at der i et fælles privat register bør være adgang til, at restauratører kan få oplysninger om restaurationsforbud, som vedrører andre restaurationer. Det samme gælder, hvis et fælles privat register indeholder oplysning om personer, der af en restauration har fået karantæne mod at komme i restaurationen.

2.2.2.2.4.4. Oplysninger fra politiet

Det vil være nødvendigt, at et fælles privat register løbende modtager præcise oplysninger fra politiet om, hvilke personer der er omfattet af restaurationsforbud, og hvilke restaurationer forbuddene vedrører. Registret skal også modtage oplysning, når et forbud ophæves, jf. reglerne omtalt i kapitel 2, afsnit 1.

Det er derfor en forudsætning for, at den fælles private registerløsning kan fungere, at der findes en teknisk løsning, der sikrer, at der løbende overføres oplysninger om restaurationsforbud fra politiet til registret.

2.2.2.3. Fordele ved de centrale løsningsmodeller

2.2.2.3.1. Generelt

Den største fordel ved et centralt offentligt register eller et fælles privat register er, at de restaurationer, der ønsker en effektiv adgangskontrol, undgår selv at skulle registrere de personer, der har forbud mod at komme i den pågældende restauration.

Det vil endvidere være en fordel, at Datatilsynets mulighed for at føre tilsyn vil være bedre, og at risikoen for misbrug og spredning af identitetsoplysninger på personer med restaurationsforbud vil være mindre.

Endelig vil politiet – helt eller delvist – slippe for besværet og udgifterne ved at skulle sende oplysninger til restaurationer, som har adgang til registret, idet det forudsættes, at disse restaurationer vil kunne fravælge at modtage skriftlig orientering fra politiet, jf. afsnit 2.2.1.1. ovenfor.

2.2.2.3.2. Fordele ved et centralt offentligt register

Ved at oprette et centralt offentligt register frem for et fælles privat register er det ikke nødvendigt at overføre oplysninger om personer med restaurationsforbud fra politiets registre til en privat database. Datasikkerhedsmæssigt må det som udgangspunkt anses som en fordel, at oplysningerne forbliver hos politiet

2.2.2.3.3. Fordele ved et fælles privat register

Den væsentligste fordel ved et fælles privat register vil være, at der i registret, udover identitetsoplysninger på personer med restaurationsforbud, med gæsternes samtykke også vil kunne registreres billeder, fingeraftryk (templates) og andre oplysninger, som kan anvendes til at sikre en hurtig, effektiv og ensartet adgangskontrol.

Et fælles privat register vil således på mange måder kunne fungere på tilsvarende måde som de gæsteregistreringssystemer, der kendes fra diskoteksbranchen, jf. afsnit 1.2.5. ovenfor, og som branchen generelt har gode erfaringer med.

2.2.2.4. Ulemper ved de centrale løsningsmodeller

2.2.2.4.1. Generelt

Blandt ulemperne ved de centrale løsningsmodeller kan set fra restaurationernes synspunkt nævnes omkostningerne og besværet ved at skulle koble sig på et centralt register – hvad enten det er et offentligt eller et fælles privat register – for at få oplysninger om, hvilke personer der har forbud mod at komme i restaurationen.
Det bemærkes i den sammenhæng, at mange – navnlig mindre - restaurationer næppe vil have noget større ønske om eller behov for at kunne tilkoble sig et centralt elektro-

nisk register, men i stedet vil foretrække at modtage eventuelle oplysninger om personer med restaurationsforbud direkte fra politiet

Hertil kommer, at etableringen og driften af et centralt register med identitetsoplysninger på personer med restaurationsforbud – uanset hvilken løsningsmodel der vælges – uundgåeligt vil indebære økonomiske udgifter af en ikke ubetydelig karakter.

2.2.2.4.2. Ulemper ved et centralt offentligt register

En af de væsentligste ulemper ved et centralt offentligt register er, at det – i modsætning til et fælles privat register – hverken vil kunne indeholde personfotografier eller fingeraftryk, jf. afsnit 2.2.1.2.1. og 2.2.2.1.5. ovenfor.

Der vil således i givet fald kun kunne blive tale om et CPR-baseret system, hvilket har betydelige ulemper i forbindelse med adgangskontrol, bl.a. fordi det som anført i afsnit 2.2.2.1.6. vil være vanskeligt for restaurationerne at sikre, at det CPR-nummer, som en gæst oplyser, rent faktisk er det rigtige, eller at et sygesikringskort mv., der fremvises eller køres gennem en kortlæser ved adgangskontrollen, rent faktisk er vedkommendes eget kort og ikke et kort, som vedkommende har lånt eller stjålet.

Set fra et samfundsmæssigt synspunkt er der en risiko for, at man ved etableringen af et centralt offentligt register – som ifølge Rigspolitiet vil være behæftet med betydelige udgifter – vælger en dyr og ikke særlig effektiv løsning.

2.2.2.4.3. Ulemper ved et fælles privat register

Ulempen ved et fælles privat register vil navnlig være de datasikkerhedsmæssige betænkeligheder, som vil kunne være forbundet med, at en privat aktør fører et register, som indeholder personfølsomme oplysninger, herunder oplysninger om strafbare forhold.

Som omtalt i afsnit 1.2.5.2. ovenfor har Datatilsynet imidlertid i en principiel afgørelse fastslået, at persondataloven ikke er til hinder for, at private restauratører – såfremt en række grundlæggende vilkår vedrørende sikkerhed er opfyldt – indsamler, registre-

rer og bruger oplysninger om forbud udstedt af politiet i medfør af restaurationsloven, samt identifikationsoplysninger på personer, som har fået sådant forbud.

3. Udvalgets konklusioner

3.1. Alle restaurationer skal have adgang til oplysninger om restaurationsforbud

Det er udvalgets opfattelse, at alle restaurationer bør have adgang til oplysninger om, hvem der har fået et forbud efter restaurationsloven mod at komme det pågældende sted, og hvor længe forbuddet gælder. Hvis restaurationerne ikke får adgang til disse oplysninger, har de ingen mulighed for at medvirke til at sikre, at forbuddene bliver efterlevet.

Dette synspunkt indebærer dog ikke, at det primære ansvar for håndhævelsen af restaurationsforbud efter restaurationslovens § 31, stk. 2, ligger hos restauratøren. Som det fremgår af kapitel 2, afsnit 1.7.2., har dette ikke været hensigten med bestemmelsen. Det overordnede ansvar for håndhævelsen af restaurationsforbud ligger, som restaurationsloven er indrettet i dag, hos politiet, jf. også afsnit 3.5 nedenfor.

I praksis kan det dog ofte være vanskeligt for politiet effektivt at kontrollere, om der i en bestemt restauration opholder sig gæster i strid med et forbud, jf. restaurationslovens § 31, stk. 2. Det gælder ikke mindst i de større byer, hvor politipatruljerne typisk ikke på forhånd har kendskab til, hvilke personer som har forbud mod at komme på den pågældende restauration. Her vil politipatruljen typisk – for at kunne identificere eventuelle lovovertrædere – være nødt til at foretage en manuel identitetskontrol af samtlige gæster, hvilket både er meget tids- og ressourcekrævende og indgribende for restaurationen og dens gæster. Hertil kommer, at sådanne større kontrolaktioner ofte kan give anledning til uro og ballade.

Efter udvalgets opfattelse er der ingen tvivl om, at restauratørerne – såvel selvstændigt som i samarbejde med politiet – i praksis spiller en vigtig rolle i forbindelse med håndhævelsen af restaurationsforbud, herunder gennem adgangskontrollen på diskoteker og natklubber mv.

For at restauratørerne kan medvirke aktivt til at sikre overholdelsen af restaurationsforbud, er det dog en afgørende forudsætning, at restaurationerne har tilstrækkelige oplysninger til at kunne identificere de personer med restaurationsforbud, som forsøger at skaffe sig adgang til restaurationen.

Alle restaurationer – uanset størrelse – bør derfor have adgang til oplysninger om personer med restaurationsforbud.

3.2. Der bør tilvejebringes en klar hjemmel for politiet til at videregive identitetsoplysninger til de berørte restaurationer

Som nævnt i kapitel 2, afsnit 1.7.2., indeholder restaurationsloven ikke nogen klar regel om, at politiet kan videregive oplysninger til restauratører om, at en person er meddelt et forbud mod at opholde sig som gæst i restaurationen.

Udvalget finder det væsentligt, at der tilvejebringes en klar hjemmel i restaurationsloven til, at politiet kan videregive identitetsoplysninger på personer med restaurationsforbud til de berørte restaurationsvirksomheder og til et fælles privat register som omtalt i afsnit 3.6 nedenfor.

3.3. Individuel skriftlig underretning af berørte restaurationer

Udvalget finder, at der bør indføres en ordning, hvor politiet, når der meddeles et restaurationsforbud, som det almindelige udgangspunkt skriftligt underretter den eller de berørte restaurationer om det udstedte forbud, jf. den decentrale løsningsmodel beskrevet i afsnit 2.2.1.

Udvalget lægger vægt på, at mange restaurationer ikke vil have noget ønske om at tilkoble sig et centralt elektronisk register, og at der derfor – uanset om der indføres et sådant register – vil være behov for, at de modtager oplysninger om restaurationsforbud direkte fra politiet, jf. herved afsnit 2.2. og 2.2.2.4.1.

Udvalget finder samtidig, at der bør ske en systematisering og ensretning af den procedure, hvorved politiet underretter restaurationerne, således at alle restaurationsvirksomheder fremover modtager de samme oplysninger fra politiet, hvilket vil sige navn

og CPR-nummer på personen, som har modtaget forbud, samt oplysninger om forbuddets tidsmæssige udstrækning.

Oplysninger om, hvilket konkret strafbart forhold der ligger til grund for forbuddets udstedelse, bør derimod ikke videregives, da oplysningen ikke i sig selv har betydning for håndhævelsen af forbuddet, jf. afsnit 2.2.1.2.

På samme måde bør personfotografier af den pågældende, som politiet måtte være i besiddelse af, heller ikke videregives til restaurationen, jf. afsnit 2.2.1.2.1.

Udvalget foreslår, at oplysningerne tilsendes næringsbrevsindehaveren eller bestyreren med almindelig (eventuelt anbefalet) post eller med krypteret e-post, jf. herved afsnit 2.2.1.3.

3.4. Tavshedspligt mv.

I øjeblikket findes der ingen særlige regler for, hvordan restauratører og dørmænd mv. skal behandle de oplysninger, som de modtager fra politiet vedrørende personer, som har fået meddelt restaurationsforbud.

Udvalget finder, at der i restaurationsloven bør indføres regler om tavshedspligt for næringsbrevsindehavere og bestyrere samt for de dørmænd og andre medarbejdere, som næringsbrevsindehaveren og bestyreren skal kunne videregive oplysningerne til, jf. afsnit 2.2.1.5. ovenfor.

Reglerne bør understreges i den underretning, som politiet giver til restaurationen, når en person har fået et restaurationsforbud.

Udvalget finder herudover, at der under en eller anden form bør gives dørmænd uddannelse eller instruktion i behandling af personfølsomme oplysninger. Udvalget lægger i den forbindelse vægt på, at det i praksis først og fremmest vil være dørmænd, der vil skulle behandle de identitetsoplysninger på personer med restaurationsforbud, der modtages fra politiet.

3.5 Ensretning af politiets praksis vedrørende meddelelse af restaurationsforbud til restauratører

Det er udvalgets opfattelse, at det i nogle tilfælde vil være formålstjenligt, at politiet – i tilknytning til at en person er blevet meddelt et restaurationsforbud – tillige meddeler restauratøren forbud mod at modtage vedkommende som gæst, jf. restaurationslovens § 31, stk. 2, 2. pkt. Det gælder særligt i tilfælde, hvor politiet har mistanke om, at restauratøren ikke i tilstrækkelig omfang vil medvirke til at håndhæve forbuddet.

Som omtalt ovenfor i kapitel 2, afsnit 1.6.2. er der i dag i politikredsene forskellig praksis med hensyn til at meddele forbud til restauratører, jf. restaurationslovens § 31, stk. 2, 2. pkt. I nogle politikredse gives der stort set aldrig forbud til restauratøren, mens andre kredse som udgangspunkt både meddeler forbud til gæsten og restauratøren.

Udvalget finder, at politiets praksis vedrørende meddelelse af restaurationsforbud til restauratører bør ensrettes, således at der fastsættes nærmere retningslinjer for, hvornår politiet også bør meddele forbud til restauratøren, jf. restaurationslovens § 31, stk. 2, nr. 2.

Det kunne f.eks. ske gennem udarbejdelsen at et supplement til Justitsministeriets cirkulæreskrivelse af 21. december 2006 til politi- og anklagemyndighed om forbud efter restaurationslovens § 31, stk. 2, jf. herved betænkningens bilag 1.

Det kunne på længere sigt overvejes, om lovgivningen eventuelt bør ændres, således at restauratøren pålægges et øget selvstændigt ansvar i forbindelse med håndhævelsen af restaurationsforbud. Et forslag om en sådan eventuel lovændring, der som påpeget af Advokatrådets repræsentant kan rejse mere principielle spørgsmål, falder dog uden for udvalgets kommissorium.

3.6. Behovet for en central løsning

Udvalget finder, at den i afsnit 3.3. omtalte fremgangsmåde, hvorefter berørte restaurationer skriftligt underrettes af politiet om restaurationsforbud, med fordel kan suppleres med en central løsningsmodel som omtalt i afsnit 2.2.2.

Udvalget lægger herved vægt på, at der for en række restaurationers vedkommende – herunder navnlig større diskoteker og natklubber – vil være væsentlige fordele forbundet med en central løsning, som indebærer, at restaurationen, i stedet for at modtage oplysninger om restaurationsforbud pr. brev eller e-post direkte fra politiet, vil kunne tilkoble sig et centralt elektronisk register med oplysninger om personer med restaurationsforbud, jf. afsnit 2.2.2.3. ovenfor.

Det vil dog i givet fald være en forudsætning, at der udvikles et centralt registreringssystem, som er praktisk og effektivt, og som vil kunne opfylde branchens behov, herunder i forhold til at kunne gennemføre en hurtig, effektiv og ensartet adgangskontrol af gæster:

3.6.1. Et centralt offentligt register

Det er udvalgets vurdering, at et centralt offentligt register som nærmere beskrevet i afsnit 2.2.2.1. ovenfor ikke vil opfylde de behov, som diskoteksbranchen har for et praktisk og effektivt redskab til at identificere gæster med restaurationsforbud.

Det skyldes først og fremmest, at det ikke er praktisk muligt at oprette et offentligt register med identitetsoplysninger på personer med restaurationsforbud, som indeholder foto eller fingeraftryk af de pågældende, jf. afsnit 2.2.1.2.1. og 2.2.2.1.5.

Som beskrevet i afsnit 2.2.2.1.6. vil et centralt offentligt register formentlig kun kunne indrettes som et CPR-baseret system, hvor restaurationsvirksomheder ved søgning på CPR-nummer kan få oplyst, om den pågældende person er omfattet af et aktuelt restaurationsforbud det pågældende sted. Et sådant system har imidlertid betydelige ulemper i forbindelse med adgangskontrol, da det bl.a. vil være vanskeligt for restaurationerne at sikre, at det CPR-nummer, som en gæst oplyser, rent faktisk er det rigtige, eller at et sygesikringskort mv., der fremvises eller køres gennem en kortlæser ved adgangskontrollen, rent faktisk er vedkommendes eget kort og ikke et kort, som vedkommende har lånt eller stjålet.

Når hertil kommer, at etableringen af et centralt offentligt register ifølge Rigspolitiet vil være behæftet med betydelige udgifter, er det samlet set udvalgets opfattelse, at en offentlig registerløsning vil være en dyr, men ikke særlig effektiv løsning.

3.6.2. Et fælles privat register

Udvalget anbefaler derfor, at der inden for persondatalovgivningens rammer oprettes et fælles privat register, hvor de restaurationsvirksomheder, som ønsker det, kan få oplyst, om en bestemt person har restaurationsforbud det pågældende sted, jf. afsnit 2.2.2.2. Oplysningen skal gives som et "ja" eller "nej" (hit - no hit). Der skal ikke være adgang til at få oplysning om, hvorvidt en person har forbud mod at komme i andre restaurationer.

Som anført i afsnit 2.2.2.2.1. vil det efter udvalgets opfattelse være nærliggende at lade branchen selv stå for oprettelsen og driften af et sådant fælles privat register.

En væsentlig fordel ved et fælles privat register vil være, at der – i modsætning til i et centralt offentligt register – udover navn og CPR-nummer på personer med restaurationsforbud med gæsternes samtykke også vil kunne registreres billeder, fingeraftryk i form af templates, jf. om dette begreb afsnit 1.2.5.2. og 2.2.2.1.5., og andre identitetsoplysninger, som kan anvendes til at sikre en hurtig, effektiv og ensartet adgangskontrol.

En anden betydelig fordel ved et fælles privat register vil være, at det – efter omstændighederne – også vil være muligt for restauratøren at registrere andre oplysninger om gæsterne i systemet, herunder f.eks. oplysninger om interne karantæner på grund af dårlig opførsel, jf. afsnit 2.2.2.2.4.1. Ligesom det er tilfældet med restaurationsforbud, vil restauratøren dog kun kunne få adgang til oplysninger om interne karantæner, der vedrører den pågældende restauration, jf. afsnit 2.2.2.2.4.2

Overordnet set vil systemet fungere som en forenklet udgave af de gæsteregistreringssystemer, som allerede anvendes flere steder i diskoteksbranchen, jf. afsnit 1.2.5., og som branchen generelt har gode erfaringer med. I modsætning til de eksisterende systemer vil det foreslåede register dog være landsdækkende og tilgængeligt for alle restaurationsvirksomheder, der ønsker det.

Registret bør så vidt muligt indrettes, så det er kompatibelt med de eksisterende gæsteregistrerings- og adgangskontrolsystemer, som allerede findes på mange diskoteker og natklubber.

3.6.2.1. Politiets videregivelse af oplysninger til det fælles private register

Det vil være nødvendigt, at det fælles private register løbende modtager opdaterede oplysninger fra politiet om, hvilke personer der er omfattet af restaurationsforbud, og hvilke restaurationer forbuddene vedrører. Registret bør på tilsvarende måde løbende modtage oplysninger, når forbud ophæves.

Udvalget forudsætter i den forbindelse, at Rigspolitiet udarbejder en teknisk løsning, som sikrer, at der løbende – og i elektronisk form – kan overføres relevante oplysninger om restaurationsforbud fra politiet til det fælles private register.

En sådan teknisk løsning vil medvirke til at sikre, at oplysningerne i det fælles private register altid er opdaterede og vil desuden i betydelig grad begrænse driftsudgifterne for registret.

Som omtalt i afsnit 3.2. foreslår udvalget, at der skabes klar hjemmel i restaurationsloven til, at politiet kan videregive oplysninger om restaurationsforbud til et fælles privat register.

3.6.2.2. Sikkerhed og tavshedspligt mv.

Det er udvalgets opfattelse, at den foreslåede løsning med et fælles privat register kan gennemføres inden for rammerne af persondataloven, jf. bl.a. Datatilsynets afgørelse i Crazy Daisy-sagen beskrevet i afsnit 1.2.5.2. og afsnit 2.2.2.2.

Det er efter forslaget kun en begrænset personkreds, der vil kunne søge i det fælles private register. Der vil endvidere skulle gælde særlige regler om tavshedspligt mv., jf. herved afsnit 2.2.2.2.3. og afsnit 3.3.

Søgning vil ske på "hit – no hit" basis, og restaurationsvirksomheden vil alene kunne få oplyst, om en gæst har forbud mod at opholde sig i netop denne virksomhed.

Det vil ikke være muligt for restaurationerne at udveksle oplysninger om forbud mv., jf. afsnit 2.2.2.2.4.2.

Det fælles private register vil skulle anmeldes til Datatilsynet og overholde Datatilsynets generelle vilkår og eventuelle yderligere vilkår og krav, som Datatilsynet måtte stille. Fordi der er tale om et centralt register, vil Datatilsynet endvidere have bedre mulighed for at føre tilsyn og kontrol med dette register frem for med registre over personer med restaurationsforbud, der føres af de enkelte restaurationer, jf. herved afsnit 2.2.1.8. og 2.2.2.3.1. ovenfor.

KAPITEL 5. Udkast til forslag til lov om ændring af lov om restaurations- og hotelvirksomhed mv. (Videregivelse og behandling af oplysninger om restaurationsforbud)

1. Lovudkast

§ 1

I lov om restaurations- og hotelvirksomhed mv., jf. lovbekendtgørelse nr. 786 af 9. august 2005, som ændret ved lov nr. 408 af 8. maj 2006, lov nr. 538 af 8. juni 2006 og lov nr. 1549 af 20. december 2006, foretages følgende ændringer:

1. I § 31 indsættes som *stk. 3-6:*

"*Stk. 3*. Politiet kan videregive oplysninger til restauratører om, hvilke personer der efter stk. 2 har fået forbud mod at opholde sig som gæst i den pågældende restauration.

Stk. 4. De oplysninger, som politiet videregiver i medfør af stk. 3, må kun behandles af næringsbrevsindehavere, bestyrere, dørmænd og andre ansatte, og behandling må kun ske i det omfang, det er nødvendigt for at håndhæve forbud efter stk. 2.

Stk. 5. Næringsbrevsindehavere, bestyrere, dørmænd og andre ansatte har tavshedspligt med hensyn til de oplysninger, der er nævnt i stk. 3. Straffelovens §§ 152 og 152 c - 152 f finder tilsvarende anvendelse.

Stk. 6. Justitsministeren kan fastsætte regler om politiets videregivelse af oplysninger i medfør af stk. 3, herunder om at videregivelsen kan ske via et privat register. Justitsministeren kan endvidere fastsætte regler om den behandling af oplysninger, der er nævnt i stk. 4.

2. I § 37, stk. 1, nr. 1, indsættes efter "§ 30": ", § 31, stk. 4,".

§ 2

Loven træder i kraft den […]

§ 3

Loven gælder ikke for Færøerne og Grønland.

2. Bemærkninger til lovudkastets enkelte bestemmelser

Til § 31, stk. 3

Ved bestemmelsen tilvejebringes en klar hjemmel til, at politiet kan videregive identitetsoplysninger på personer med restaurationsforbud til de berørte restaurationsvirksomheder.

Politiet får ved bestemmelsen adgang til at videregive oplysninger til restauratører om, hvilke personer der efter restaurationslovens § 31, stk. 2, har fået forbud mod at opholde sig som gæst i den pågældende restauration. Ved begrebet "restauratør" skal forstås næringsbrevsindehaveren eller bestyreren, jf. restaurationslovens §§ 13 og 15.

Politiet vil kunne videregive oplysning om den pågældendes navn og CPR-nummer og om forbuddets tidsmæssige udstrækning. Oplysning om, hvilket konkret strafbart forhold der ligger til grund for forbuddets udstedelse, vil derimod som udgangspunkt ikke kunne videregives, da oplysningen ikke i sig selv har betydning for håndhævelsen af forbuddet. På samme måde bør personfotografier af den pågældende, som politiet måtte være i besiddelse af, almindeligvis heller ikke videregives til restaurationen.

Oplysningerne kan alene videregives til næringsbrevsindehaveren eller bestyreren, som herefter vil være ansvarlig for den videre behandling af oplysningerne.

Til § 31, stk. 4

Bestemmelsen fastlægger den personkreds, der må behandle de oplysninger om restaurationsforbud, som politiet i medfør af stk. 3 videregiver til næringsbrevsindehaveren eller bestyreren.

I restaurationer med adgangskontrol vil det normalt være dørmænd, der står for adgangskontrollen. Det vil derfor være nødvendigt, at dørmændene har adgang til de pågældende oplysninger. Ved "dørmænd" forstås autoriserede dørmænd, jf. restaurationslovens § 15 a, stk. 1, og personer, som i henhold til lov om vagtvirksomhed er autoriseret til at drive vagtvirksomhed, og en vagtvirksomheds godkendte personale, jf. restaurationslovens § 15 a, stk. 3. Der henvises til betænkningens kapitel 4, afsnit 2.2.1.4.2.

Efter omstændighederne vil det også være nødvendigt, at andre ansatte i restaurationen får adgang til oplysningerne. Det vil navnlig kunne være tilfældet i restaurationer uden adgangskontrol og dermed normalt uden dørmænd, idet der her – hvis adgangen til oplysningerne begrænses til næringsbrevsindehavere, bestyrere og dørmænd – i næringsbrevsindehaverens eller bestyrerens fravær ikke vil være nogen til at kontrollere, om en person har fået et forbud mod at komme i restaurationen. De personalegrupper, der kunne blive tale om i sådanne tilfælde at give adgang til de modtagne identitetsoplysninger fra politiet, vil være bartendere og serveringspersonale mv.

Behandling af de oplysninger, der modtages fra politiet, må efter bestemmelsen kun ske i det omfang, det er nødvendigt for at håndhæve restaurationsforbud. Der skal således være en saglig begrundelse for at få adgang til at beskæftige sig med de pågældende oplysninger.

Til § 31, stk. 5

Ved bestemmelsen fastsættes der tavshedspligt for næringsbrevsindehavere, bestyrere, dørmænd og andre ansatte med hensyn til de oplysninger om restaurationsforbud, som politiet har videregivet i medfør af stk. 3. Henvisningen til straffelovens § 152 og §§ 152 c-152 f, indebærer bl.a., at enhver *uberettiget* videregivelse eller udnyttelse af oplysningerne kan straffes med bøde eller fængsel indtil 6 måneder. Sker videregivelsen eller udnyttelsen med forsæt til at skaffe sig eller andre uberettiget vinding, eller foreligger der i øvrigt særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år.

Til § 31, stk. 6

Ved bestemmelsen bemyndiges justitsministeren til at fastsætte regler om politiets videregivelse af oplysninger i medfør af stk. 3, herunder om at videregivelsen kan ske via et privat register.

Det forudsættes, at der i medfør af bestemmelsen fastsættes regler om, at politiet skal give en restaurations næringsbrevsindehaver eller bestyrer individuel underretning, når en person har fået forbud efter stk. 2 mod at komme der. Den enkelte restauration skal dog have adgang til at fravælge en sådan individuel underretning, såfremt restaura-

tionen er tilsluttet et centralt register. Det forudsættes endvidere, at der fastsættes regler om, at underretningen skal gives skriftligt ved almindeligt eller eventuelt anbefalet brev eller krypteret e-post.

Bestemmelsen bemyndiger endvidere justitsministeren til at fastsætte de regler, der er nødvendige for, at en videregivelse af oplysninger om identitetsoplysninger på personer med restaurationsforbud kan gives via et privat register. Som omtalte ovenfor finder udvalget det naturligt, at et sådant register oprettes af eller på vegne af restaurationsbranchen. Om et sådant fælles privat register, der vil være underlagt reglerne i persondatalovgivningen, henvises til betænkningens kapitel 4, afsnit 3.6.2.

Endelig bemyndiger bestemmelsen justitsministeren til at fastsætte nærmere regler om den behandling af oplysninger, der er nævnt i stk. 4. Der vil i medfør af bestemmelsen bl.a. kunne fastsættes krav til den enkelte restaurations opbevaring og håndtering af de modtagne oplysninger.

Der vil til de regler, som justitsministeren fastsætter i medfør af bestemmelsen, kunne knyttes strafansvar for overtrædelse af reglerne, jf. restaurationslovens § 37, stk. 4.

Til § 37, stk. 1, nr. 1

Bestemmelsen indebærer, at der fastsættes strafansvar for at behandle oplysninger fra politiet om restaurationsforbud i strid med § 31, stk. 4. Straffen er bøde eller under skærpende omstændigheder eller i gentagelsestilfælde fængsel indtil 4 måneder. Bestemmelsen angår situationer, hvor en næringsbrevsindehaver, en bestyrer, en dørmand eller en anden ansat har behandlet oplysninger fra politiet om restaurationsforbud uden, at det har været nødvendigt for at håndhæve forbud efter § 31, stk. 2, f.eks. som et udslag af nysgerrighed. Strafansvar forudsætter dog, at den pågældende vidste eller burde vide, at behandlingen af oplysningerne var unødvendig, jf. herved straffelovens § 19.

Bestemmelsen er et nødvendigt supplement til reglen i § 31, stk. 5, om tavshedspligt, idet ikke enhver unødvendig behandling af oplysninger, jf. stk. 4, vil være en tilsidesættelse af tavshedspligten efter stk. 5.

BILAG

CIS nr 10092 af 21/12/2006 Gældende
Offentliggørelsesdato: 12-01-2007
Justitsministeriet

Den fulde tekst

Cirkulæreskrivelse om forbud efter restaurationslovens § 31, stk. 2

Til politi og anklagemyndighed

Det følger af restaurationslovens § 31, stk. 2, at politiet kan forbyde en person, der i forbindelse med restaurationsbesøg har begået en strafbar handling, at opholde sig som gæst i bestemte restaurationsvirksomheder.

Et sådant forbud kan meddeles af politimesteren/politidirektøren for så vidt det af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden må anses for nødvendigt. Afgørelsen træffes på grundlag af en konkret vurdering af de oplysninger, der indgår i sagen.

Folketingets Ombudsmand afgav den 16. april 2004 en udtalelse i anledning af en konkret sag om meddelelse af et forbud efter restaurationslovens § 31, stk. 2, hvori ombudsmanden på en række punkter udtalte kritik af behandlingen af sagen.

Justitsministeriet har endvidere i en række nyere sager taget stilling til spørgsmålet om karakteren af de strafbare forhold, som kan danne grundlag for et forbud, samt spørgsmålet om udstrækning af et forbud til flere restaurationer.

Med henblik på at opnå en ensartet behandling af sagerne i de enkelte politikredse har Justitsministeriet på den baggrund fundet anledning til at udarbejde en samlet gennemgang af reglerne om og praksis vedrørende politiets behandling af sager om meddelelse af forbud efter restaurationslovens § 31, stk. 2.

Cirkulæreskrivelsen indeholder en gennemgang af de generelle betingelser for at udstede et forbud efter restaurationslovens § 31, stk. 2 (afsnit 1). Endvidere behandler cirkulæreskrivelsen forbuddets udstrækning, herunder den geografiske og den tidsmæssige udstrækning af forbuddet (afsnit 2).

Endelig indeholder cirkulæreskrivelsen en gennemgang af forskellige forvaltningsretlige spørgsmål, som kan opstå i forbindelse med meddelelse af et forbud efter restaurationslovens § 31, stk. 2 (afsnit 3).

1. Betingelserne for at meddele forbud efter restaurationslovens § 31, stk. 2.

1.1 Det strafbare forhold

Det følger af restaurationslovens § 31, stk. 2, at politiet kan forbyde en person, der i forbindelse med restaurationsbesøg har begået en strafbar handling, at opholde sig som gæst i bestemte virksomheder. Forbuddet kan meddeles efter anmodning fra restauratøren, men også på politiets eget initiativ. Afgørelsen træffes på grundlag af en konkret vurdering af de oplysninger, der indgår i sagen.

Meddelelse af forbud forudsætter ikke, at der er begået flere strafbare handlinger i forbindelse med restaurationsbesøg. Ved lov nr. 1084 af 10. december 2002 blev restaurationslovens § 31, stk. 2, præciseret, således at det nu klart fremgår, at der er mulighed for at meddele et forbud allerede første gang, der konstateres en strafbar handling i forbindelse med restaurationsbesøg.

Det er efter restaurationslovens § 31, stk. 2, en betingelse for at meddele et forbud, at der i forbindelse med restaurationsbesøg er begået en strafbar handling. Det er ikke en forudsætning, at det strafbare forhold, som ligger til grund for forbuddet, er fastslået ved dom. Et forbud kan således meddeles, når den pågældende er sigtet for en strafbar handling i forbindelse med restaurationsbesøg.

Justitsministeriet har i en række sager efter en konkret vurdering ophævet forbud, hvor den pågældende ikke var blevet sigtet for den strafbare handling, som dannede grundlag for forbuddet, ligesom ministeriet har ophævet forbud, hvor den sigtelse, som lå til grund for forbuddet, af bevismæssige årsager blev frafaldet, idet ministeriet i disse tilfælde ikke fandt, at det med tilstrækkelig sikkerhed kunne fastslås, at der var begået et strafbart forhold.

Det fremgår af forarbejderne til restaurationslovens § 31, stk. 2, at det er en forudsætning for at meddele et forbud efter restaurationsloven, at det må anses for nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden.

Bemærkningerne må antages at forudsætte, at et forbud skal være nødvendiggjort af en forventning om, at den pågældende person i fremtiden vil forstyrre ro og orden på den konkrete restauration, såfremt vedkommende ikke meddeles forbud mod at tage ophold på restaurationen.

Bemærkningerne må endvidere antages at forudsætte, at ikke alle strafbare forhold begået på en restauration kan danne grundlag for et restaurationsforbud. Det er således ikke i sig selv tilstrækkeligt, at der er begået et strafbart forhold på en restauration. Det

strafbare forhold skal tillige have en sådan tilknytning til eller sammenhæng med restaurationsbesøget, at det er nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden på restaurationen at meddele et forbud på baggrund af overtrædelsen. Der skal være tale om strafbare handlinger, som typisk begås i restaurationsmiljøet, eller som det er vigtigt at modvirke særligt i restaurationsmiljøet.

Justitsministeriet har således i en konkret sag ophævet et restaurationsforbud, som var meddelt på baggrund af, at den pågældende var sigtet for overtrædelse af straffelovens § 279 ved på restaurationen at have forsøgt at benytte et stjålet dankort, idet ministeriet ikke fandt, at det strafbare forhold var af en sådan karakter, at det af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden på restaurationen var nødvendigt at meddele den pågældende et forbud efter restaurationsloven.

For så vidt angår besiddelse af euforiserende stoffer, er det ministeriets opfattelse, at en sådan besiddelse i en restaurationsvirksomhed efter en konkret vurdering af blandt andet karakteren af den pågældende restaurationsvirksomhed efter omstændighederne i sig selv kan danne grundlag for et restaurationsforbud af hensyn til lovlighed, ædruelighed og opretholdelse af ro og orden.

Dette indebærer, at der i situationer, hvor det strafbare forhold består i besiddelse af euforiserende stoffer, skal anlægges en vurdering af, om det i forhold til den konkrete restaurationsvirksomhed er nødvendigt at meddele et forbud. Besiddelse af euforiserende stoffer til eget forbrug, hvor de euforiserende stoffer ikke kan antages at være bestemt til at indtage i forbindelse med restaurationsbesøget, vil således ikke i alle tilfælde kunne danne grundlag for et forbud efter restaurationsloven. I vurderingen af, om et forbud er nødvendigt i relation til den konkrete restaurationsvirksomhed, skal indgå karakteren af den pågældende restauration, omstændighederne i forbindelse med besiddelsen, samt om der er tale om en restaurationsvirksomhed, hvor der ofte konstateres overtrædelser af lov om euforiserende stoffer.

En vurdering af baggrunden for og karakteren af det strafbare forhold vil kunne føre til, at kravet om, at forbuddet skal være nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden, ikke kan anses for at være opfyldt, idet der ikke foreligger det fornødne grundlag for at antage, at den pågældende i fremtiden generelt vil forstyrre ro og orden i forbindelse med restaurationsbesøg.

Også strafbare forhold begået uden for en restaurationsvirksomhed kan danne grundlag for meddelelsen af et forbud efter restaurationsloven, blot det strafbare forhold har tilknytning til restaurationsbesøget. Der kan for eksempel være tale om strafbare forhold begået i køen til restaurationen eller strafbare forhold, som udspringer af en episode inde på restaurationen.

Justitsministeriet har eksempelvis i en konkret sag vedrørende et forbud, som var meddelt på baggrund af en overtrædelse af politivedtægten begået på fortovet uden for en restauration, stadfæstet forbuddet under henvisning til, at handlingen fandt sted i tilknytning til restaurationsbesøget.

Det strafbare forhold skal dog have en vis nær og umiddelbar tilknytning til et restaurationsbesøg for at kunne danne grundlag for udstedelse af et forbud efter restaurationsloven.

Justitsministeriet har således i en konkret sag ophævet et forbud under henvisning til, at det strafbare forhold, som lå til grund for forbuddet, ikke havde en sådan tilknytning til den pågældendes forudgående besøg på restaurationsvirksomheden, at der var grundlag for at meddele et forbud. Ministeriet henviste i den forbindelse til, at den pågældende var dømt for forholdet, og at retten i den forbindelse havde lagt til grund, at der var tale om helt uprovokeret og meningsløs gadevold.

1.2 Den tidsmæssige sammenhæng mellem det strafbare forhold og forbuddet

Det skal være aktuelt nødvendigt at udstede et forbud, hvilket må antages at forudsætte, at et forbud skal udstedes i en vis tidsmæssig sammenhæng med det strafbare forhold, som ligger til grund for forbuddet.

Justitsministeriet har således i en konkret sag ophævet et forbud, der blev meddelt som led i en generel gennemgang af sager vedrørende værtshusrelateret vold i et forsøg på at nedbringe antallet af sådanne sager knap et år efter, at det seneste strafbare forhold, som dannede baggrund for forbuddet, var begået. Ministeriet fandt under hensyn til den medgåede tid ikke, at forbuddet på tidspunktet for meddelelsen var nødvendigt, ligesom der ikke i øvrigt sås at foreligge oplysninger, som gjorde et forbud aktuelt nødvendigt.

1.3 Forbuddets proportionalitet

En afgørelse om udstedelse af et forbud efter restaurationslovens § 31, stk. 2, skal endelig være i overensstemmelse med det forvaltningsretlige proportionalitetsprincip. Det må således antages, at en vurdering af grovheden af det begåede strafbare forhold vil kunne føre til, at et forbud ikke kan udstrækkes til at omfatte andre restaurationer end den, hvor det strafbare forhold er begået.

Justitsministeriet skal dog i den forbindelse bemærke, at Folketingets Ombudsmand i en udtalelse, som er optrykt i Folketingets Ombudsmands beretning, 1986, s. 82, i forbindelse med en konkret sag har bemærket, at et forbud må anses som et indgreb af ringe intensitet i forhold til adressaten.

Justitsministeriet har således som ovenfor nævnt i en række sager, hvor det strafbare forhold, som lå til grund for forbuddet, bestod i besiddelse af en lille mængde hash til eget forbrug, stadfæstet de pågældende forbud.

Justitsministeriet skal dog bemærke, at et forbud, der udstrækkes til at omfatte flere restaurationer må anses for forholdsvis

indgribende over for den pågældende, særligt hvor forbuddet omfatter størstedelen af restaurationerne i en by, således at forbuddet får karakter af en generel udelukkelse fra at deltage i byens restaurations- og natteliv.

Det må således antages, at en vurdering af grovheden af det begåede strafbare forhold vil kunne føre til, at et forbud ikke kan udstrækkes til at omfatte andre restaurationer end den, hvor det strafbare forhold er begået.

2. Forbuddets udstrækning

2.1 Forbuddets geografiske udstrækning

Der er efter praksis ikke grundlag for at antage, at det strafbare forhold, som ligger til grund for forbuddet, nødvendigvis skal være begået i den eller de restaurationer, som forbuddet vedrører. Der er således mulighed for at udstede forbud, som omfatter andre restaurationsvirksomheder end den virksomhed, hvor det strafbare forhold er begået. I tilfælde, hvor et forbud efter restaurationslovens § 31, stk. 2, udstrækkes til at omfatte flere restaurationer, skal der for hver enkelt restauration omfattet af forbuddet, anlægges en konkret vurdering af, om betingelserne i bestemmelsen er opfyldt i forhold til restaurationen, herunder om det af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden må anses for nødvendigt at udstede et forbud.

Justitsministeriet har i en række konkrete sager, hvor et restaurationsforbud er udstrakt til flere restaurationer, stadfæstet forbuddets udstrækning under henvisning til, at de pågældende restaurationer er beliggende på en sådan måde, at de udgør et samlet restaurationsområde.

I de konkrete sager har området været karakteriseret ved en flerhed af restaurationer, som er placeret inden for et snævert geografisk område, ofte side om side og med en tæt trafik af gæster mellem de forskellige restaurationer, således at de nærmest kan betragtes som én restauration. I disse situationer vil det oftest for at opnå den ønskede effekt af et forbud være nødvendigt, at dette udstrækkes til at omfatte samtlige restaurationer i området.

Justitsministeriet har endvidere i en række konkrete sager, hvor et forbud er udstrakt til flere restaurationer, stadfæstet forbuddets udstrækning under henvisning til, at de pågældende restaurationer er af samme karakter, og alle er beliggende inden for et begrænset geografisk område.

På grund af antallet og beliggenheden af restaurationerne kan der i disse tilfælde næppe siges at foreligge et samlet restaurationsområde, men i det omfang flere restaurationer af samme karakter er beliggende inden for et mindre geografisk område, kan forbuddet efter omstændighederne udstrækkes til at omfatte alle disse restaurationer.

Justitsministeriet har endelig i en række konkrete sager, hvor et forbud er udstrakt til flere restaurationer, stadfæstet forbuddets udstrækning på baggrund af en konkret viden om den person, som forbuddet er rettet imod, herunder at den pågældende typisk indfinder sig på alle restaurationerne i løbet af samme aften.

Det kan i disse situationer ikke anses for en forudsætning, at de restaurationer, som er omfattet af forbuddet, er beliggende tæt på hinanden, selvom dette ofte vil være tilfældet. Det er således ikke de pågældende restaurationer, men alene personens adfærd som begrunder forbuddets udstrækning. Der vil dog formentlig i sådanne tilfælde ofte være tale om restaurationer af samme karakter.

Et forbud kan ikke udstrækkes til at omfatte flere restaurationer alene på baggrund af en aftale med de pågældende restauratører herom. Der skal være omstændigheder ved den konkrete sag, som medfører, at det må anses for nødvendigt at udstrække forbuddet til også at omfatte andre restaurationer end den, hvor det strafbare forhold er begået.

Justitsministeriet har således i en konkret sag, hvor et forbud var udstrakt til at omfatte to restaurationer, har ophævet forbuddet for så vidt angår den ene restauration, idet forbuddet alene var udstrakt til denne restauration på baggrund af, at restauratøren på den pågældende restauration havde meddelt, at personer, som af politiet blev meddelt forbud mod at indfinde sig som gæster i andre restaurationsvirksomheder i byen, ligeledes var uønskede på hans restauration.

En vurdering af baggrunden for og karakteren af det strafbare forhold vil kunne føre til, at kravet om, at forbuddet skal være nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden på restaurationen, ikke kan anses for at være opfyldt i forhold til andre restaurationer end den, hvor forholdet er begået, idet der i disse tilfælde ikke foreligger det fornødne grundlag for at antage, at den pågældende i fremtiden generelt vil forstyrre ro og orden i forbindelse med restaurationsbesøg.

Justitsministeriet har således i en konkret sag ophævet et forbud, da ministeriet ikke fandt, at det strafbare forhold, som lå til grund for forbuddet var af en sådan karakter, at det kunne danne grundlag for at udstrække restaurationsforbuddet til andre restaurationer, end den hvor forholdet var begået. Justitsministeriet lagde i den forbindelse vægt på, at baggrunden for det strafbare forhold var en konkret konflikt mellem den pågældende og forurettede, samt at der ikke i øvrigt for Justitsministeriet var oplyst omstændigheder, som pegede på, at den pågældende i fremtiden ville forstyrre ro og orden på andre restaurationer end den, hvor det strafbare forhold var begået.

2.2 Forbuddets tidsmæssige udstrækning

Restaurationslovens § 31, stk. 2, tager ikke stilling til den tidsmæssige udstrækning af forbud, som meddeles efter bestemmelsen. I praksis udstedes et forbud efter restaurationsloven oftest for 2 år.

Justitsministeriet skal dog bemærke, at der i den enkelte sag skal anlægges en konkret vurdering af, om det er nødvendigt at

udstrække forbuddet til at gælde i 2 år. Justitsministeriet skal i den forbindelse bemærke, at ministeriet i en konkret sag, under henvisning til at der var tale om et enkeltstående forhold, fandt, at forbuddet i den konkrete sag ikke burde udstrækkes til mere end 1 år.

Det forudsættes således, at forbuddets tidsmæssige udstrækning begrænses til den periode, hvor forbuddet efter en konkret vurdering må anses for at være nødvendigt af hensyn til lovlighed, sædelighed, ædruelighed eller opretholdelse af ro og orden på restaurationen.

3. Forvaltningsretlige spørgsmål i forbindelse med udstedelse af restaurationsforbud

Meddelelse af et forbud efter restaurationsloven er en afgørelse, som træffes af en forvaltningsmyndighed, og sager om udstedelse af restaurationsforbud skal derfor behandles i overensstemmelse med reglerne i lov nr. 571 af 19. december 1985 (forvaltningsloven). Der henvises i den forbindelse til Justitsministeriets vejledning om forvaltningsloven.

3.1 Partshøring

Efter forvaltningslovens § 19, stk. 1, skal en part i en sag gøres bekendt med oplysninger vedrørende sagens faktiske omstændigheder og have lejlighed til at fremkomme med en udtalelse, når det må antages, at parten ikke er bekendt med, at myndigheden er i besiddelse af disse oplysninger. Det gælder dog kun, hvis oplysningerne er til ugunst for den pågældende part og er af væsentlig betydning for sagens afgørelse.

En partshøring efter forvaltningslovens § 19 kan foretages såvel mundtligt som skriftligt, afhængig af, hvilken fremgangsmåde der i den konkrete situation skønnes hensigtsmæssig. Mundtlig partshøring bør alene anvendes, hvor sagen er af forholdsvis enkel karakter.

En forbudssag efter restaurationslovens § 31, stk. 2, er ikke af en sådan karakter, at mundtlig partshøring er udelukket. Der vil som oftest være tale om enkle faktiske oplysninger, som den pågældende i forvejen er bekendt med.

Meddelelse af forbud efter restaurationsloven sker ofte på eller uden for restaurationen kort tid efter, at det strafbare forhold, som ligger til grund for forbuddet, er begået. Partshøringen foretages i disse situationer typisk mundtligt umiddelbart inden, at der meddeles et forbud.

Justitsministeriet skal i den forbindelse bemærke, at det som udgangspunkt ikke er udelukket at anvende denne fremgangsmåde, men ministeriet finder anledning til at bemærke, at den pågældende skal være i en tilstand, hvor partshøring med mening kan foretages. Partshøring på grund af den pågældendes tilstand kan være udelukket, hvis vedkommende er svært beruset, påvirket eller ophidset.

Et forbud kan som ovenfor nævnt udstrækkes til at omfatte andre restaurationer end den, hvor det strafbare forhold er begået. Justitsministeriet skal gøre opmærksom på, at den pågældende, i de tilfælde hvor et forbud udstrækkes til at omfatte flere restaurationer, ligeledes skal partshøres over de forhold, som ligger til grund for, at forbuddet udstrækkes til flere restaurationer.

Folketingets Ombudsmand har i anledning af en konkret sag den 28. marts 2000 udtalt, at det forhold, at et forbud omfattede 10 restaurationer, som ikke havde tilknytning til sigtelserne, talte for, at partshøringen burde være foretaget skriftligt eller i hvert fald med en vis frist, således at den pågældende havde haft lejlighed til nærmere at overveje sine eventuelle bemærkninger hertil.

Justitsministeriet skal på den baggrund gøre opmærksom på, at der i tilfælde, hvor et forbud udstrækkes til at omfatte flere restaurationer, og hvor de oplysninger, den pågældende skal partshøres over, derfor er mere komplicerede, kan være grund til at foretage partshøringen skriftligt eller med en vis frist, således at den pågældende får lejlighed til at overveje eventuelle bemærkninger.

Justitsministeriet har i flere sager konstateret, at det ikke fremgik af sagens akter, at der var foretaget partshøring, og hvilke oplysninger den pågældende i den forbindelse blev partshørt over. Justitsministeriet skal derfor bemærke, at det altid skal fremgå af sagens akter, om der er foretaget partshøring, samt hvilke forhold der er foretaget partshøring over.

3.2 Begrundelse

Det fremgår af forvaltningslovens § 22, at en afgørelse skal være ledsaget af en begrundelse, når den meddeles skriftligt, medmindre afgørelsen fuldt ud giver den pågældende part medhold.

Efter forvaltningslovens § 24 skal afgørelser dels indeholde en henvisning til de retsregler, i henhold til hvilke afgørelsen er truffet, dels angive de hovedhensyn der har været bestemmende for skønnet. Begrundelsen skal endvidere indeholde en kort redegørelse for de oplysninger vedrørende sagens faktiske omstændigheder, som er tillagt væsentlig betydning for afgørelsen.

En begrundelse for en forvaltningsafgørelse skal således efter forvaltningslovens § 24 fremtræde som en forklaring på, hvorfor afgørelsen har fået det pågældende indhold. Det skal i begrundelsen for forbuddet nærmere præciseres, hvilke handlinger der ligger til grund for forbuddets udstedelse, herunder hvor og hvornår de pågældende handlinger er begået.

I tilfælde, hvor et forbud udstrækkes til at omfatte flere restaurationer end den restaurationsvirksomhed, hvor forholdet er begået, skal det endvidere fremgå af begrundelsen, hvad der er baggrunden for at udstrække forbuddet til at omfatte flere restaurationsvirksomheder.

3.3 Klagevejledning

Efter forvaltningslovens § 25 skal afgørelser, som kan påklages til en anden forvaltningsmyndighed, når de meddeles skriftligt, være ledsaget af en vejledning om klageadgang med angivelse af klageinstans og oplysning om fremgangsmåden ved indgivelse af klage, herunder om eventuel tidsfrist. Det gælder dog ikke, hvis afgørelsen fuldt ud giver den pågældende part medhold.

Det skal således fremgå af det meddelte forbud, at afgørelsen om meddelelse af forbud (efter 1. januar 2007) kan påklages til Rigspolitichefen, jf. afsnit 4.

3.4 Gyldighed

Det skal endvidere fremgå af forbud meddelt efter restaurationslovens § 31, stk. 2, hvor længe forbuddet gælder.

Justitsministeriet skal i den forbindelse gøre opmærksom på, at forbuddet, der er fastsat for en periode på to år, begynder at løbe fra og med dagen efter den dag, hvor den begivenhed, som udløser fristen, finder sted, jf. restaurationslovens § 36 a, stk. 1. I forhold til lovens § 31, stk. 2, er det det strafbare forhold, som udløser fristen. Hvis der er tale om en fortsat forbrydelse, lægges periodens sidste dag til grund for fristberegningen.

Er det strafbare forhold f.eks. begået den 5. januar 2007, begynder fristen at løbe den 6. januar 2007, og fristen udløber således den 5. januar 2009 ved døgnets slutning.

Forbuddet kan håndhæves over for den pågældende, når forbuddet er forkyndt for vedkommende.

Hvis forbuddet forkyndes samme dag, som det strafbare forhold, der ligger til grund for forbuddet, er begået, kan forbuddet håndhæves over for den pågældende allerede fra dette tidspunkt. Fristen for forbuddet begynder imidlertid også i dette tilfælde først at løbe fra og med dagen efter.

Hvis forbuddet forkyndes på et senere tidspunkt, begynder fristen for forbuddet alligevel at løbe allerede fra og med dagen efter den dag, hvor det strafbare forhold er begået, jf. ovenfor.

4. Overgangsregler

I forbindelse med politi- og domstolsreformen er restaurationslovens § 34, stk. 1, blevet ændret således, at politiets afgørelser efter restaurationslovens § 31, stk. 2, fra 1. januar 2007 kan påklages til Rigspolitichefen og ikke som i dag til Justitsministeriet. Det følger af retsplejelovens § 109, stk. 2, at Rigspolitichefens afgørelser i klagesager over afgørelser truffet af politidirektørerne ikke kan påklages til Justitsministeriet.

Klager fremsat efter 1. januar 2007 behandles af Rigspolitichefen, mens klager, der er fremsat inden den 1. januar 2007, vil blive færdigbehandlet i Justitsministeriet.

Justitsministeriet, den 21. december 2006

Mette Lyster Knudsen

Adgangskontrol på diskoteker og førelse af intern karantæneliste

Brevdato: 20.06.08

Journalnummer: 2008-42-0742

Datatilsynet vender hermed tilbage til sagen om behandling af personoplysninger hos Diskotek Crazy Daisy i Viborg (herefter Crazy Daisy).

Sammenfattende er det Datatilsynets konklusion, at Crazy Daisy med gæstens udtrykkelige samtykke kan behandle oplysninger i form af fingeraftryk (template) og billede.

Hvis gæsten tilbagekalder sit samtykke skal Crazy Daisy slette fingeraftrykket (templaten) og billedet.

Datatilsynet kan endvidere - under forudsætning af, at Crazy Daisy iagttager persondatalovens regler - give tilladelse til behandlingen af følsomme personoplysninger i forbindelse med adgangskontrol på diskoteket og førelse af en intern karantæneliste.

Tilladelsen vil blive givet på følgende vilkår:

1. Behandling af følsomme personoplysninger i forbindelse med tildeling og administration af en karantæne må alene ske med den registreredes skriftlige samtykke. Samtykket skal være udtrykkeligt og skal opfylde persondatalovens krav. Dvs. det skal være en frivillig, specifik og informeret viljestilkendegivelse.
2. Tilbagekaldes samtykket, skal oplysninger om årsagen til karantæne slettes.
3. Behandlingen af følsomme personoplysninger skal ske under iagttagelse af de i bilag 1 beskrevne sikkerhedsregler.
4. Medarbejderne skal informeres om, at deres opslag logges, og at loggen kan bruges til at kontrollere uberettigede opslag samt til stikprøvekontrol.

En nærmere gennemgang af sagen følger nedenfor.

Sagsfremstilling

I juli 2007 indledte Datatilsynet en undersøgelse af Crazy Daisys behandlinger af personoplysninger, og diskoteket har i den forbindelse besvaret Datatilsynets spørgsmål i breve af 9. august og 22. oktober 2007 samt telefonisk den 3. og 4. december 2007.

Efterfølgende har Crazy Daisy den 21. februar 2008 anmeldt behandlingen "Adgangskontrol på diskotek - førelse af intern karantæneliste" til Datatilsynet samt ansøgt om tilladelse efter persondataloven § 50, stk. 1, nr. 1.

Datatilsynet har indhentet supplerende oplysninger, og der er efter aftale foretaget rettelser i anmeldelsen.

Crazy Daisys behandlinger af personoplysninger

Dataansvar

Det fremgår af anmeldelsen, at Crazy Daisy er dataansvarlig for de oplysninger, der behandles. Som databehandler - dvs. virksomhed, som foretager databehandling på vegne af Crazy Daisy - benyttes MCB A/S, Enghaven 49, 7500 Holstebro.

Behandlingens formål

Hovedformålet med behandlingen er at sikre et trygt og sikkert natteliv.

Crazy Daisy har om formålet nærmere oplyst, at det i praksis er umuligt at lave en ensartet kontrol af 800-1.000 gæster inden for en afgrænset tidsperiode. Af sikkerhedsmæssige årsager ønsker Crazy Daisy at undgå lange køer uden for diskoteket, da dette ofte fører til optrin og frustrationer. Det er derfor nødvendigt, at Crazy Daisy kan lave en ensartet og hurtig genkendelse af de gæster, som allerede er i systemet, og som derfor umiddelbart kan tildeles adgang.

Formålet er endvidere at give Crazy Daisy mulighed for mere systematisk at administrere en karantæne, som diskoteket eventuelt har tildelt en gæst eller håndhæve et forbud udstedt af politiet efter restaurationsloven, herunder at kunne forklare eventuelle gæster, hvorfor de ikke kan blive lukket ind på diskoteket.

Ved at flytte karantæneregistreringen over i et system er det Crazy Daisys overbevisning, at antallet af såvel fysiske som verbale overfald på vagtpersonale/dørmænd vil blive reduceret, da dørmanden ikke længere over for gæsten fremstår, som den der ene og alene administrerer forbud og karantæner.

Behandling af generelle kundeoplysninger om diskoteksgæster

Det fremgår af anmeldelsen, at der sker behandling af oplysninger om gæsterne i Crazy Daisys elektroniske adgangssystem, MasterClub. Det er nærmere oplyst, at alle gæster vil skulle registreres. Det vil ikke være muligt at være gæst på diskoteket, hvis man ikke lader sig registrere.

I MasterClub sker der indsamling, registrering, brug, opbevaring og sletning af generelle kundeoplysninger, herunder oplysninger om navn, adresse, telefonnummer, e-mail-adresse, fødselsdato, køn og ankomsttidspunkt. Der sker desuden behandling af oplysninger i form af billede og fingeraftryk.

Oplysningerne vil blive behandlet med gæstens frivillige og udtrykkelige samtykke, der indhentes i forbindelse med oprettelsen af gæsten i MasterClub, og den registrerede vil forud for registreringen i systemet generelt blive oplyst om systemets funktion og indretning samt de nærmere omstændigheder ved indsamlingen af oplysninger.

Crazy Daisy har oplyst, at diskoteket ikke gemmer gæstens fingeraftryk, men en matematisk beregnet værdi af fingeraftrykket - en såkaldt template, som benyttes til at lave en positiv identifikation. Det er ikke muligt at gendanne et fingeraftryk på baggrund af templaten.

Adgangskontrolsystemet er lavet til at sikre en lynhurtig registrering og genkendelse af gæsterne. Softwaren, der er opbygget omkring en database, som kører lokalt, installeres på en almindelig PC, og der tilkøbes en fingeraftryksscanner. Det er tillige muligt at tilkøbe en magnetkortlæser, der kan benyttes til diskotekets egne klubkort eller til sygesikringsbevis for hurtig registrering. Kortlæseren benyttes efter det oplyste ikke til at registrere oplysninger om personnummer.

Med fingeraftryksscanneren behøver Crazy Daisys kunder blot at registrere sig en enkelt gang - herefter kan de ankomme uden nogen form for ID og alligevel komme ind, blot ved at anvende

fingeraftrykksscanneren.

Af sikkerhedsmæssige årsager ønsker Crazy Daisy med registrering af gæ-sternes billede at have et parameter mere at måle på foruden fingeraftrykket, f.eks. for det tilfælde, at to fingeraftryk skulle ligge tæt op af hinanden.

Crazy Daisy mener ikke at kunne nøjes med oplysning i form af template, da det ikke direkte på denne oplysning alene (uden scanner) er muligt at genkende gæsterne.

Crazy Daisy anfører endvidere, at det er vigtigt at kunne sætte ansigt på gæsterne, således at dørmænd/entrépersonale allerede, når gæsten står i køen ude på gaden kan tage fat i person, der tidligere har fået tildelt en karantæne.

Behandling af eventuelle karantæneoplysninger om diskoteksgæster

Der behandles endvidere oplysninger om eventuelle karantæneforhold, herunder oplysninger om karantæneperiode og -årsag.

Oplysningerne om årsagen til karantænen kan f.eks. være, når en diskoteksgæst har begået strafbare forhold, herunder vold, hærværk, overtrædelse af våbenloven, fremsættelse af trusler, salg/besiddelse af euforiserende stoffer m.v. Der er desuden tale om oplysninger om helbredsmæssige forhold, herunder misbrug af narkotika, alkohol og lignende nydelsesmidler.

En diskoteksgæst vil imidlertid også kunne blive tildelt en karantæne uden at have begået noget strafbart.

Oplysninger om årsagen til karantæne behandles efter det oplyste med den registreredes samtykke.

Det er nærmere oplyst, at det er Crazy Daisys opfattelse, at diskoteket er i stand til at indhente et udtrykkeligt samtykke, der opfylder persondatalovens krav. Skulle dette imidlertid ikke være muligt, vil Crazy Daisy ikke foretage nogen registrering af karantæneårsag i MasterClub.

Indhentelse af samtykket til registrering af karantæneårsag foregår i forbindelse med, at den pågældende gæst dagen/nogle dage efter episoden indkaldes til et møde på diskoteket, hvor begrundelsen for karantænen forklares.

Behandling af oplysninger i form af billedoptagelser fra diskoteket

Der behandles desuden oplysninger i form af billedoptagelser, der optages på diskoteket i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed. Det er nærmere oplyst, at der sker tv-overvågning af diskotekets gange og lokaler.

Videregivelse af oplysninger til politiet

Vedrørende videregivelse er det oplyst, at identifikationsoplysninger og oplysninger om (formodede) begåede strafbare forhold videregives til politiet i forbindelse med indgivelse af en politianmeldelse.

Registrering af oplysninger i forbindelse med politiets udstedelse af forbud
Der sker behandling af oplysninger om et eventuelt forbud udstedt af politiet i medfør af restaurationslovens § 31, stk. 2. Informationen om et udstedt forbud sendes til diskoteket pr. anbefalet brev og indeholder oplysninger om navn, adresse, personnummer, årsagen til forbuddet og dets udløbsdato.

Brevene opbevares i ringbind på et aflåst kontor på diskoteket og behandles desuden i MasterClub.

Sikkerhedsforanstaltninger

Om sikkerhedsforanstaltningerne er det oplyst, at alle adgange til oplysningerne logges i systemet. Oplysningerne sendes krypteret til en ekstern database drevet af MCB A/S. Adgang til databasen foregår via webservice, som er placeret bag firewall. Serverne er placeret i et hostingcenter, der er sikret mod fysiske trusler som brand, tyveri og hærværk. F.eks. patruljerer hundevagt uden for åbningstiden. Centret er udstyret med alarm- og adgangskontrolsystemer. Det er endvidere kun administrator, som kan se oplysninger om karantæneårsag. Manuelle oplysninger opbevares i ringbind på et aflåst kontor.

Slettefrister

Oplysninger, der ikke er nødvendige for at opretholde det ønskede sikkerhedsniveau, slettes automatisk. Fingeraftryk slettes, hvis gæsten ikke har besøgt diskoteket inden for en periode på 90 dage. Billeder slettes, hvis gæsten ikke har besøgt diskoteket inden for en periode på 180 dage. Øvrige generelle kundeoplysninger slettes i systemet senest 24 måneder efter sidste besøg.

Oplysning om, at en gæst har fået karantæne på grund af dennes tidligere adfærd, vil forblive i systemet, så længe karantænen løber. Oplysning om karantæneårsagen forbliver i systemet, så længe karantænen løber, medmindre samtykke til opbevaring tilbagekaldes. Længden af en tildelt karantæne kan variere mellem 3 måneder og 2 år.

Oplysninger om forbud udstedt i medfør af restaurationsloven slettes, når forbudet udløber.

Oplysninger i form af billedoptagelser fra overvågningskameraer slettes efter 30 dage.

Opfyldelse af persondatalovens oplysningspligt

Om opfyldelse af persondatalovens oplysningspligt har Crazy Daisy oplyst, at diskoteket har opsat et skilt i entréen med information, og at entrépersonalet i forbindelse med indhentelse af samtykke gør meget ud at forklare gæsterne, hvad formålet med registreringen er.

Offentliggørelse af billeder på Crazy Daisys hjemmeside

Crazy Daisy har oplyst, at diskoteket gennem de seneste 5 år har taget billeder af gæster, som selv ønsker at få deres billede offentliggjort på diskotekets hjemmeside.

Crazy Daisy har endvidere oplyst, at diskoteket er meget opmærksom på kun at tage billeder af personer, som er bekendt med diskotekets fotograf og dermed samtykker til, at billedet bliver offentliggjort.

Det er Crazy Daisys opfattelse, at dette er normal praksis inden for diskoteksbranchen.

I den anledning skal Datatilsynet, som har drøftet sagen på et møde i Datarådet, udtale følgende:

For alle oplysningstyper giver persondataloven som udgangspunkt mulighed for, at behandling kan ske, hvis den registrerede har givet sit udtrykkelige samtykke hertil.

Behandlingen vil således kunne ske i medfør af persondatalovens § 6, stk. 1, nr. 1 (almindelige ikke-følsomme oplysninger), § 11, stk. 2, nr. 2 (oplysninger om personnummer), § 7, stk. 1, nr. 1 (oplysninger om helbredsforhold, herunder narkotikamisbrug m.v.) og § 8, stk. 4 og 5 (oplysninger om strafbare forhold).

De nærmere krav til et sådant samtykke findes i persondatalovens § 3, nr. 8, hvorefter et samtykke i

persondataloven er defineret som enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Datatilsynet skal henlede opmærksomheden på, at der ud over et udtrykkeligt samtykke også skal foreligge et sagligt formål, der lever op til persondatalovens § 5, stk. 2, og der må ikke behandles flere oplysninger end nødvendigt, jf. proportionalitetsprincippet i lovens § 5, stk. 3.

Oplysninger i form af fingeraftryk (template) og billede

Efter Datatilsynets opfattelse udgør ønsket om at lave en ensartet kontrol af gæsterne inden for en afgrænset periode og at undgå køer uden for diskoteket saglige formål.

Hvis behandlingen baserer sig på et udtrykkeligt samtykke, der lever op til persondatalovens krav, vil den påtænkte behandling af oplysninger om fingeraftryk (template) og billede efter Datatilsynets opfattelse kunne ske inden for persondatalovens rammer.

Hvis den registrerede tilbagekalder sit samtykke medfører persondatalovens § 38, at Crazy Daisy skal slette templaten og billedet.

Følsomme oplysninger om årsagen til en tildelt karantæne

Datatilsynet lægger til grund, at Crazy Daisy har behov for at registrere karantæneårsagen for senere at kunne forklare en gæst, hvorfor vedkommende ikke kan blive lukket ind på diskoteket i en nærmere afgrænset tidsperiode.

Det er derfor Datatilsynets vurdering, at Crazy Daisys behandling af oplysninger om diskoteksgæster tjener et sagligt og legitimt formål og kan ske inden for rammerne af persondatalovens § 5.

Hvis der foreligger et udtrykkeligt samtykke, der lever op til persondatalovens krav, vil årsagen til en karantæne således kunne registreres.

Henset til oplysningernes følsomme karakter (bl.a. strafbare forhold og narkotikamisbrug) vil det efter Datatilsynets opfattelse være god databehandlingsskik (jf. persondatalovens § 5, stk. 1), at diskoteksgæstens samtykke til behandling af følsomme oplysninger om karantæneårsager er skriftligt. Dette indgår derfor i de vilkår, som Datatilsynet stiller i medfør af persondatalovens § 50, stk. 5.

Hvis den registrerede tilbagekalder samtykket, medfører persondatalovens § 38, at oplysninger om årsagen til karantænen skal slettes.

Det er Datatilsynets umiddelbare vurdering, at Crazy Daisy i disse tilfælde efter persondatalovens § 6, stk. 1, nr. 7, alene vil kunne gemme oplysninger om navn, adresse, samt hvor længe personen er uønsket som gæst. Datatilsynet forudsætter således, at der ikke gemmes billeder, fingeraftryk (templates) og personnumre eller følsomme oplysninger om strafbare forhold og narkotikamisbrug, hvis samtykket tilbagekaldes.

Oplysninger om forbud udstedt af politiet efter restaurationsloven

Ifølge restaurationslovens § 31, stk. 2, kan politiet forbyde personer, som i forbindelse med restaurationsbesøg har begået en strafbar handling, at opholde sig som gæster i en bestemt virksomhed. Politiet kan tillige forbyde de pågældende restauratører at modtage disse personer som gæster.

Det er Datatilsynets vurdering, at Crazy Daisy uden samtykke kan indsamle, registrere og bruge oplysninger om forbud udstedt af politiet i medfør af restaurationsloven, jf. persondatalovens § 8, stk. 6, jf. 7, stk. 2, nr. 4, og § 8, stk. 4, 2. pkt., samt identifikationsoplysninger, herunder personnummer, på

personer, som har fået sådant forbud, jf. persondatalovens § 6, stk. 1, nr. 3 og 7, og § 11, stk. 2, nr. 1. Oplysningerne skal slettes, når forbuddet udløber.

Videregivelse af oplysninger til politiet

Behandling af følsomme oplysninger skal ske i overensstemmelse med persondatalovens §§ 7 og 8 og under iagttagelse af persondatalovens grundlæggende principper i § 5.

Det fremgår af persondatalovens forarbejder, at lovens § 8, stk. 4-5, tilsigter at videreføre den gældende retstilstand efter den nu ophævede lov om private registre m.v. Bestemmelsen opstiller derfor meget snævre rammer for, hvornår der kan ske registrering og videregivelse af følsomme personoplysninger uden samtykke. Det fremgår endvidere af forarbejderne, at bestemmelsen giver mulighed for, at en virksomhed kan registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse og eventuelt senere afgivelse af vidneforklaring i retten. Oplysningerne skal dog destrueres snarest muligt, jf. lovens § 5, stk. 5.

På baggrund af lovens forarbejder, jf. ovenfor, kan det efter Datatilsynets opfattelse ikke anses for at være i strid med persondatalovens § 8, stk. 4, at en virksomhed uden samtykke indsamler og registrerer oplysninger om strafbare forhold, når dette sker med henblik på politianmeldelse og/eller senere vidneforklaring i retten. Oplysningerne skal imidlertid destrueres snarest muligt, det vil sige senest, når sagen er afsluttet hos politiet eller domstolene.

De oplysninger, der er nødvendige for indgivelse af en politianmeldelse og eventuel senere forklaring for retten, vil således - specifikt til dette formål - kunne behandles uden samtykke, jf. persondatalovens § 8, stk. 6, jf. § 7, stk. 2, nr. 4, og § 8, stk. 4, 2. pkt. og stk. 5.

Det er en forudsætning, at oplysningerne alene anvendes til at indgive politianmeldelse, og at de slettes snarest muligt, det vil sige senest, når sagen er afsluttet hos politiet eller domstolene.

Videregivelse af oplysninger til andre end politiet

Crazy Daisy kan ikke videregive personoplysninger fra MasterClub til f.eks. andre diskoteker, medmindre der foreligger et udtrykkeligt samtykke hertil fra den enkelte diskoteksgæst.

Det er endvidere altid en betingelse, at videregivelsen tjener et sagligt formål og er proportional i forhold til det formål, der forfølges, jf. persondatalovens
§ 5, stk. 2 og 3.

Offentliggørelse af billeder på Crazy Daisys hjemmeside

Datatilsynet skal henlede opmærksomheden på, at persondataloven skal iagttages ved offentliggørelse af billeder af personer på Crazy Daisys hjemmeside.

Persondataloven medfører, at billeder af besøgende på et diskotek eller lignende kun kan offentliggøres med udtrykkeligt samtykke.

Læs mere om offentliggørelse af billeder på internettet på Datatilsynets hjemmeside.

Tv-overvågningsbilleder

Datatilsynet gør opmærksom på, at tv-overvågningsloven regulerer, i hvilke tilfælde og på hvilken måde tv-overvågning kan foretages af private. Endvidere indeholder straffeloven regler, som skal iagttages i forbindelse med tv-overvågning.

Den behandling af personoplysninger, som en tv-overvågning indebærer, er ligesom anden behandling

af personoplysninger reguleret i persondataloven og dermed undergivet Datatilsynets tilsyn.

Datatilsynet forudsætter, at Crazy Daisys tv-overvågning foretages med respekt af gældende lovgivning, herunder såvel persondataloven som tv-overvågningsloven og straffeloven.

Til orientering om reglerne om tv-overvågning kan henvises til Datatilsynets og Justitsministeriets pjece herom.

Slettefrister

Det følger persondatalovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Datatilsynet har noteret sig Crazy Daisys oplysninger om de slettefrister, der vil blive anvendt.

Information til de registrerede og disses øvrige rettigheder

Oplysningspligt

Datatilsynet har noteret sig, at Crazy Daisy forud for gæstens registrering i MasterClub informerer generelt om systemets funktion og indretning samt de nærmere omstændigheder ved indsamling af oplysninger.
I persondatalovens §§ 28 og 29 findes reglerne om oplysningspligt. Efter disse bestemmelser påhviler det den dataansvarlige ved registreringen af oplysningerne at informere den registrerede bl.a. om udstrækningen af registreringen, formålet hermed, samt yderligere oplysninger, der er nødvendige for, at den registrerede kan varetage sine interesser.

Crazy Daisy skal derfor overveje, om der påhviler diskoteket yderligere oplysningspligt over for den registrerede i medfør af ovennævnte bestemmelser.

Dette vil være særligt relevant, når Crazy Daisy modtager oplysninger fra andre end den registrerede selv og behandler disse oplysninger elektronisk eller i manuelle registre.

I de tilfælde, hvor Crazy Daisy modtager forbud fra politiet efter restaurationsloven og indtaster denne information i MasterClub, er det således persondatalovens udgangspunkt, at Crazy Daisy skal sende en meddelelse til den registrerede. Underretning vil eventuelt kunne undlades, hvis den registrerede allerede fra politiet har modtaget tilstrækkelige oplysninger om Crazy Daisys registrering til at kunne varetage sine interesser.

Læs mere om oplysningspligten på Datatilsynets hjemmeside og i rettighedsvejledningen.

Oplysningspligt i forbindelse med tv-overvågning

I forbindelse med tv-overvågning kan Crazy Daisy opfylde sin oplysningspligt i forhold til diskotekets gæster og ansatte ved at opsætte skilte eller på anden tydelig måde.

Princippet om god databehandlingsskik medfører, at ansatte, der overvåges, endvidere skal oplyses om bl.a. formålet med tv-overvågningen og om, i hvilke tilfælde optagelserne vil blive gennemgået og videregivet til politiet.

Informationen skal være forudgående, så f.eks. nyansatte skal have besked i forbindelse med deres ansættelse, eller når de begynder at arbejde i tv-overvågede lokaler. Informationen kan f.eks. gives i en personalehåndbog eller lignende, som den ansatte får udleveret.

Pligt til at give indsigt

Ifølge persondatalovens § 31, stk. 1, skal den dataansvarlige efter begæring fra en person give meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Ifølge § 31, stk. 2, skal den dataansvarlige snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.

Læs mere om indsigtsretten på Datatilsynets hjemmeside og i rettighedsvejledningen.

Datasikkerhed

Ifølge persondatalovens 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Af § 42, stk. 1, følger, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Efter § 42, stk. 2, skal gennemførelse af en behandling ved en databehandler ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren.

Datatilsynet har noteret sig, at det kun er administrator, som kan se oplysninger om karantæneårsag, at alle anvendelser af oplysningerne logges i systemet, at oplysningerne sendes krypteret til en ekstern database drevet af MCB A/S, at adgang til databasen foregår via webservice, som er placeret bag firewall, og at serverne er placeret i et hostingcenter, der er sikret mod fysiske trusler som brand, tyveri og hærværk.

Datatilsynet har endvidere noteret sig, at manuelle oplysninger opbevares i ringbind på et aflåst kontor på diskoteket.

Datatilsynet forudsætter, at Crazy Daisy har indgået en skriftlig databehandler aftale med MCB, jf. persondatalovens § 42.

Henset til oplysningernes følsomme karakter - oplysninger om strafbare forhold og narkomisbrug - har Datatilsynet fundet anledning til at fastsætte et vilkår - i henhold til persondatalovens § 50, stk. 5 - om, at behandlingen af personoplysninger skal ske under iagttagelse af de i vedlagte bilag beskrevne sikkerhedsregler. Se vilkår 4 og bilag 1.

I relation til pkt. 2 i bilag 1 forudsætter Datatilsynet, at Crazy Daisy instruerer sine medarbejdere i, hvilke krav der efter persondataloven stilles til behandling af personoplysninger, herunder indhentelse af samtykke, opfyldelse af oplysningspligten samt håndtering af den registreredes øvrige rettigheder.

Datatilsynets konklusion

Sammenfattende er det Datatilsynets konklusion, at Crazy Daisy med gæstens udtrykkelige samtykke kan behandle oplysninger i form af fingeraftryk (template) og billede.

Hvis gæsten tilbagekalder sit samtykke skal Crazy Daisy slette fingeraftrykket (templaten) og billedet.

Datatilsynet kan endvidere - under forudsætning af, at Crazy Daisy iagttager persondatalovens regler - give tilladelse til behandlingen af følsomme personoplysninger i forbindelse med adgangskontrol på diskoteket og førelse af en intern karantæneliste.

Tilladelsen vil blive givet på følgende vilkår:

1. Behandling af følsomme personoplysninger i forbindelse med tildeling og administration af en karantæne må alene ske med den registreredes skriftlige samtykke. Samtykket skal være udtrykkeligt og skal opfylde persondatalovens krav. Dvs. det skal være en frivillig, specifik og informeret viljestilkendegivelse.
2. Tilbagekaldes samtykket, skal oplysninger om årsagen til karantæne slettes.
3. Behandlingen af følsomme personoplysninger skal ske under iagttagelse af de i bilag 1 beskrevne sikkerhedsregler.
4. Medarbejderne skal informeres om, at deres opslag logges, og at loggen kan bruges til at kontrollere uberettigede opslag samt til stikprøvekontrol.

Ovenstående vilkår vil gælde indtil videre. Datatilsynet forbeholder sig ret til senere at tage vilkårene op til revision, hvis der skulle vise sig behov for det.

Eventuelle ændringer af forhold, der er omfattet af anmeldelsen

Eventuelle ændringer i de forhold, der er omfattet af anmeldelsen skal meddeles Datatilsynet i overensstemmelse med persondatalovens § 51.

Gebyr

Datatilsynets tilladelse er belagt med et gebyr på 1000 kr., jf. persondatalovens § 63, stk. 2, nr. 2. Beløbet skal indbetales til Danske Bank, Holmens Kanal 2-12, 1092 København K, reg.nr.: 0216, kontonr.: 4069058132. Der bedes i den forbindelse henvist til Datatilsynets journalnummer (se forsiden af dette brev), således at Datatilsynet kan identificere indbetalingen.

Endelig tilladelse vil blive udstedt, når Datatilsynet har modtaget betaling.

For en god ordens skyld vedlægges et eksemplar af den tilrettede anmeldelsesblanket som bilag 2.

For god ordens skyld skal det oplyses, at Datatilsynet vil offentliggøre dette brev på sin hjemmeside.

Efterskrift

Ved brev af 22. juli 2008 har Datatilsynet på ovenstående vilkår meddelt Crazy Daisy i Viborg endelig tilladelse til behandlingen "Adgangskontrol på diskotek - førelse af intern karantæneliste".

Tilbage til alle afgørelser

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk

Opdateret: 18.08.08

Datatilsynets vilkår om sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger

Efter persondatalovens § 50, stk. 5, fastsætter Datatilsynet i forbindelse med meddelelse af tilladelse til den anmeldte behandling nærmere vilkår for udførelsen af behandlingen til beskyttelse af de registreredes privatliv.

Den dataansvarliges behandlingssikkerhed skal leve op til kravene i persondatalovens kapitel 11. Til uddybning af disse krav har Datatilsynet stillet vilkår om, at behandlingen af personoplysninger skal ske under iagttagelse af de sikkerhedsregler, der er beskrevet i dette bilag.

Generelle sikkerhedsbestemmelser

1. Den dataansvarlige skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i virksomheden til uddybning af de regler, der fremgår af dette bilag. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for virksomheden. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i virksomheden.

2. Den dataansvarlige skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af punkt 1.

3. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

4. Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at persondatalovens § 41, stk. 3, overholdes.

Inddatamateriale som indeholder personoplysninger

6. Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddatering. Materialet skal opbevares aflåst, når det ikke anvendes, og slettes eller tilintetgøres, når det ikke længere

skal anvendes til de formål, hvortil det er indsamlet, dog senest efter en af den dataansvarlige fastsat frist. Ved tilintetgørelse skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Uddatamateriale som indeholder personoplysninger

7. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Materialet skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri. Når materialet ikke længere skal anvendes til de formål, som behandlingen varetager, dog senest efter en af den dataansvarlige fastsat frist, skal det slettes eller tilintetgøres.

Autorisation og adgangskontrol

8. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles ved hjælp af edb. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

9. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, samt personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

10. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i punkt 8 og 9. Kontrol heraf skal foretages mindst en gang hvert halve år.

11. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som behandles ved hjælp af edb, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

12. Der skal foretages registrering af alle afviste forsøg på adgang til edb-systemet. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg.

Logning

13. I edb-registre skal der foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes.

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk

Afslag på tilladelse til advarselsregister for diskoteker

Brevdato: 02.07.08

Journalnummer: 2008-43-0011

Glubbin ApS har den 6. februar 2008 som dataansvarlig virksomhed anmodet om Datatilsynets udtalelse vedrørende et nyt internetsite: Glubbin (Glubbin.com). Henvendelsen er den 6. maj 2008 fulgt op af en anmeldelse til Datatilsynet af et advarselsregister, benævnt "Et tidsbegrænset register over ekskluderede medlemmer af Glubbin". Ved brev af 9. maj 2008 har Glubbin ApS afgivet en supplerende udtalelse.

Der har den 8. april 2008 været afholdt et møde mellem Datatilsynet og en repræsentant fra Glubbin ApS m.fl. Der er endvidere indhentet telefoniske oplysninger.

Det fremgår herefter, at Glubbin ApS er en virksomhed, der beskæftiger sig med konceptudvikling og software til mobiltelefoner og sociale medieplatforme. Glubbin ApS støttes ifølge det oplyste økonomisk af Ministeriet for Videnskab, Teknologi og Udvikling via Østjysk Innovation A/S.

Glubbin (www.glubbin.com) er et nyt socialt internetsite, hvor unge over 18 år kan tilmelde sig og se, hvad der sker af events i nattelivet og modtage tilbud om disse arrangementer. Glubbin består af en landsdækkende klub (Glubbin Konceptet) for diskoteker og gæster over 18 år. Alle over 18 år kan tilmelde sig som medlem på Glubbins hjemmeside. Ved tilmeldingen accepterer medlemmet Glubbins betingelser, der bl.a. indebærer mulighed for udelukkelse/karantæne af medlemmet på grund af upassende adfærd.

Som eksempler på upassende adfærd er nævnt: hærværk, vold mv. på eventstedet, kopiering og uberettiget videregivelse mv. af det entrebevis, der sendes til medlemmet via medlemmets mobiltelefon.

Overtrædes medlemsbetingelserne ved de pågældende events på eventstedet, er det hensigten, at eventpersonalet indberetter til Glubbin om overtrædelse af medlemsbetingelserne med henblik på eksklusion af Glubbin.

Det fremgår endvidere, at formålet med det anmeldte register er at medvirke til opretholdelse af ro og orden i diskoteksmiljøet.

Hvis en person, der er medlem af Glubbin, meddeles karantæne fra Glubbin for upassende adfærd, nægtes den pågældende gæst adgang til de diskoteker, der er medlem af Glubbin. Dog afgør de diskoteker, der er tilsluttet Glubbin Konceptet, selv, om diskoteket vil lukke et karantæneramt Glubbin-medlem ind som gæst i karantæneperioden.

Optagelse i det påtænkte register skal ske, hvis Glubbin modtager indberetning fra et diskotek, der er tilmeldt Glubbin Konceptet, om at et medlem har overtrådt Glubbins medlemsbetingelser og samtidig er blevet meddelt karantæne af diskoteket. Glubbin har telefonisk supplerende oplyst, at en indberetning til det påtænkte register tillige skal kunne ske, selv om der ikke er meddelt en karantæne af vedkommende

diskotek, under forudsætning af, at medlemmet har udvist en upassende adfærd. Endvidere vil en upassende adfærd, udvist udelukkende på et diskotek, som udgangspunkt være tilstrækkeligt som indberetningsgrundlag.

Oplysninger om navn, adresse og karantæneperiode videregives af diskoteket til Glubbin. Oplysning om årsagen til karantænen, dvs. hvilken upassende adfærd der har været på tale, påtænkes ikke videregivet og heller ikke registreret hos Glubbin.

Når Glubbin har modtaget den omhandlede indberetning fra vedkommende diskotek, agter Glubbin at underrette det pågældende medlem om indberetningen. Medlemmet underrettes samtidig om, at medlemmet nu har karantæne fra Glubbin og de tilsluttede diskoteker i en tidsbegrænset periode, og at medlemmet kan kontakte Glubbin, hvis medlemmet mener, at vedkommende fortsat er berettiget til medlemskab, hvorefter Glubbin træffer afgørelse.

Glubbin behandler oplysninger om sine medlemmer. Oplysningerne, der behandles elektronisk og manuelt, omhandler oplysninger om navn, adresse, personnummer, evt. CVR-nummer og karantæneperiode. Oplysningerne påtænkes overført online til de diskoteker, der er tilsluttet Glubbin Konceptet. Glubbin påtænker at kræve en skriftlig indberetning fra vedkommende diskotek af den registrerede, vedlagt en vitterlighedserklæring. Vitterlighedserklæringens nærmere indhold er p.t. ikke fastlagt.

Glubbin overvejer p.t., hvorledes og i hvilket omfang det enkelte diskotek, der er tilsluttet Glubbin Konceptet, skal indformere gæsterne, der er Glubbin-medlem, om diskotekernes ordensreglement og de kriterier, der i givet fald kan begrunde indberetning til det påtænkte register.

De registrerede oplysninger slettes senest et år efter registreringen. Glubbin har telefonisk oplyst, at hvis karantæneperioden er kortere end et år, slettes de registrerede oplysninger samtidig med karantæneperiodens udløb.

Oplysning om medlemmets personnummer er krypteret, og der kræves en individuel log-in for at få adgang til medlemsoplysningerne. Baggrunden for at behandle oplysning om personnummer er ifølge det oplyste at sikre, at medlemmerne ved optagelse i Glubbin er over 18 år, hvorved personnummeret valideres via en algoritme eller køres op mod CPR.

Glubbin forventer, at ca. 50-100 diskoteker vil anvende det omhandlede register.

Glubbin har supplerende ved brev af 9. maj 2008 opregnet en række eksempler på **upassende adfærd** på eventstedet som betingelse for optagelse i det påtænkte register:

- forsøg på at forfalske sin billet,
- chikane og anden forulempelse, herunder vold, af andre diskoteksgæster,
- udøvelse af hærværk på vedkommende diskotek,
- undladelse af at efterkomme vedkommende diskoteks ordensregler og henstillinger.

Endvidere har Glubbin i samme brev supplerende redegjort for proceduren vedrørende **indhentelse af samtykke** i forbindelse med indmeldelse i Glubbin:

Det fremgår, at når en bruger tilmelder sig Glubbin på Glubbins hjemmeside (www.glubbin.com), så skal brugeren samtidig acceptere betingelserne for medlemskab. Brugeren kan endvidere ikke tilmelde sig uden at have haft åbnet linket til medlemsbetingelserne.

Glubbin fremhæver, at en optagelse af et medlem i Glubbins påtænkte register ikke udelukker, at vedkommende medlem kan besøge andre diskoteker, der ikke er tilsluttet Glubbin Konceptet, idet ikke alle diskoteker vil blive tilbudt at samarbejde med Glubbin.

Vedrørende **adgang til det påtænkte register** har Glubbin supplerende anført, at adgang hertil forudsætter personligt brugernavn og password på administratorniveau. Hos Glubbin vil 3-4 ansatte få adgang til de omhandlede oplysninger.

Endelig har Glubbin supplerende oplyst vedrørende Glubbins **behandling af klager**, at Glubbin ved modtagelse af en klage over optagelse i det påtænkte register vil oplyse de faktuelle forhold ved indhentelse af oplysninger fra de involverede parter. Der vil blive foretaget en individuel vurdering af, om den registrerede fortsat skal stå i registeret, og hvis Glubbin vurderer, at den registrerede skal slettes, vil dette ske straks, og den registrerede underrettes samtidig.

Glubbin har pointeret over for Datatilsynet, at Glubbin Konceptet endnu er i sin implementeringsfase, og at dette er baggrunden for, at udformningen af det påtænkte register p.t. ikke foreligger i sin endelige form. Glubbin afventer således Datatilsynets udtalelse til det påtænkte register med henblik på at få af-/bekræftet, om der er grundlag for at arbejde videre med konceptet.

Datatilsynet skal, efter at sagen har været behandlet på et møde i Datarådet, udtale følgende:

1. Er det anmeldte register et advarselsregister ?

Efter persondatalovens § 50, stk. 1, nr. 2, skal Datatilsynets tilladelse indhentes, forinden en behandling iværksættes, hvis behandlingen af oplysninger sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret (advarselsregister).

Datatilsynet må i det foreliggende tilfælde lægge til grund, at formålet med den anmeldte behandling er, at Glubbin skal videregive karantæneoplysninger mv. til diskoteker, der er tilsluttet Glubbin Konceptet, med det formål at advare de pågældende diskoteker mod at modtage de pågældende Glubbin-medlemmer som gæster.

På den baggrund er det Datatilsynets opfattelse, at det påtænkte register vil indebære en advarsel mod forretningsforbindelser med de registrerede. Databehandlingen er således omfattet af persondatalovens § 50, stk. 1, nr. 2, om advarselsregistre.

2. Kan der gives en tilladelse ?

Ved vurderingen af, om en ansøgning om tilladelse efter persondatalovens § 50, stk. 1, nr. 2, kan imødekommes, træffer Datatilsynet i hvert enkelt tilfælde afgørelse om, hvorvidt oprettelsen af det pågældende advarselsregister tjener anerkendelsesværdige interesser.

Glubbin har oplyst, at en betingelse for optagelse i det påtænkte register vil være, enten at medlemmet har overtrådt Glubbins medlemsbetingelser og er blevet meddelt karantæne fra et af de deltagende diskoteker, eller at medlemmet har udvist "upassende adfærd". Der vil ikke ske registrering af årsagen til den meddelte karantæne, f.eks. vold, hærværk mv.

Det er Datatilsynets vurdering, at Glubbin vil komme i besiddelse af følsomme oplysninger om f.eks. strafbare forhold, når Glubbin modtager indberetninger med angivelse af og eventuel dokumentation for de nærmere omstændigheder, der begrunder optagelse i det påtænkte register.

Diskotekernes videregivelse af oplysninger om strafbare forhold til Glubbin og Glubbins registrering af disse vil kun kunne ske, hvis betingelserne i persondatalovens § 8 er opfyldt.

Oplysninger om strafbare forhold må private dataansvarlige efter persondatalovens § 8, stk. 4, behandle, hvis den registrerede har givet et udtrykkeligt samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til

den registrerede.

Det fremgår endvidere af lovens § 8, stk. 5, at de i stk. 4 nævnte oplysninger ikke må videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

Efter persondatalovens § 8, stk. 6, må oplysninger om blandt andet strafbare forhold desuden behandles, hvis en af betingelserne i lovens § 7 er opfyldt. Følsomme oplysninger må efter lovens § 7, stk. 1, som udgangspunkt ikke behandles. Lovens § 7, stk. 2-7, indeholder en række bestemmelser, der muliggør en behandling af denne type oplysninger i specielle tilfælde.

På det foreliggende grundlag er det Datatilsynets opfattelse, at kriteriet for optagelse i det påtænkte register i høj grad lægger op til en subjektiv vurdering med risiko for registrering af vildledende/urigtige oplysninger.

Det er herefter Datatilsynets opfattelse, at der **ikke** inden for rammerne af persondatalovens § 8, stk. 4 og 5, og § 8, stk. 6, jf. § 7, vil kunne ske videregivelse til og registrering af oplysninger om strafbare forhold eller andre følsomme oplysninger i et advarselsregister som det påtænkte.

Det bemærkes i den forbindelse, at Datatilsynet i en række sager har udtalt, at § 8, stk. 4 og 5, indebærer, at advarselsregistre ikke vil kunne indeholde oplysninger om bl.a. strafbare forhold, medmindre den registrerede har givet sit udtrykkelige samtykke.

På denne baggrund kan Datatilsynet ikke give Glubbin ApS tilladelse til behandling af personoplysninger med henblik på at advare andre mod forretningsforbindelser med en registreret, jf. persondatalovens § 50, stk. 1, nr. 2.

Tilbage til alle afgørelser

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk