



Diskotek Crazy Daisy  
Gravene 20a  
8800 Viborg

Att.: Henrik Karlsen

Sendt til: [post@daisy-viborg.dk](mailto:post@daisy-viborg.dk)

27. juni 2008

### **Vedrørende adgangskontrol på Diskotek Crazy Daisy i Viborg**

Datatilsynet  
Borgergade 28, 5.  
1300 København K

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

CVR-nr. 11-88-37-29

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

Telefon 3319 3200  
Fax 3319 3218

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

E-post  
[dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)  
[www.datatilsynet.dk](http://www.datatilsynet.dk)

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.

J.nr. 2008-42-0742  
Sagsbehandler  
Inge Birgitte Møberg  
Direkte 3319 3233

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. Tilbagekalder 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<sup>1</sup> § 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 nattelev.

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 oprin 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 dørmændene 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.

<sup>1</sup> Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

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 templatens.

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 fingeraftryks-scanner. 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 fingeraftryksscanneren.

Af sikkerhedsmæssige årsager ønsker Crazy Daisy med registrering af gæsternes 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 øje-med. 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 entré-personalet i forbindelse med indhentelse af samtykke gør meget ud af 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 templatens 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 databehandlings-skik (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.<sup>2</sup>

#### 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.<sup>3</sup>

#### **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.

<sup>2</sup> [www.datatilsynet.dk](http://www.datatilsynet.dk), under punktet "Erhverv" → "Internettet" → "Billeder på internettet".

<sup>3</sup> Pjecen kan læses/hentes på Datatilsynets hjemmeside, under punktet "Publikationer".



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<sup>4</sup> og i rettighedsvejledningen<sup>5</sup>.

#### 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.

<sup>4</sup> [www.datatilsynet.dk](http://www.datatilsynet.dk), under punktet "Erhverv" → "Pligter i forhold til den registrerede" → "Oplysningspligt".

<sup>5</sup> Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

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<sup>6</sup> 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.

<sup>6</sup> [www.datatilsynet.dk](http://www.datatilsynet.dk), under punktet "Erhverv" → "Pligter i forhold til den registrerede" → "Indsigt".

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. Tilbagekalder 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.

Med venlig hilsen

Janni Christoffersen  
Direktør

- Bilag 1: Sikkerhedsregler for behandling af personoplysninger der er anmeldt til Datatilsynet af en privat dataansvarlig  
Bilag 2: Kopi af den tilrettede anmeldelse

## **Sikkerhedsregler for behandling af personoplysninger der er anmeldt til Datatilsynet af en privat dataansvarlig**

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.

|   |   |
|---|---|
| <b>1. Dataansvarlig</b>   | Navn*<br>Diskotek Crazy Daisy   |
|   | Adresse*<br>Gravene 20A, 8800 Viborg  |
|   | Tlf.nr.*<br>86615133  |
|   | E-post<br>Vil ikke blive offentliggjort i Fortegnelsen<br>post@daisy-viborg.dk              |
|   | Evt.J.nr./ID.nr.  |
|   | Kontaktperson*<br>Vil ikke blive offentliggjort i Fortegnelsen<br>Henrik Karlsen            |
|   | <input checked="" type="checkbox"/> Oplysningerne opbevares hos den dataansvarlige og/eller |
|   | <input checked="" type="checkbox"/> Oplysningerne opbevares hos databehandler               |
|   | Databehandlerens navn MCB A/S   |
|   | Databehandlerens adresse Enghaven 49, 7500 Holstebro  |
| <input type="checkbox"/> Den dataansvarlige er etableret i et tredjeland, og der er udpeget en repræsentant i Danmark |   |
| Repræsentantens navn  |   |
| Repræsentantens adresse   |   |
| <b>2. Betegnelse og</b>   | Behandlingens betegnelse:* Adgangskontrol på disko-   |



|                               |  |
|-------------------------------|--|
| <b>formål</b>                 | <p>tek - førelse af intern karantæneliste</p> <hr/> <p>Formål og evt. delformål:*</p> <p>At sikre et trygt og sikkert natteliv, at sikre en ensartet og hurtig genkendelse af de gæster, som allerede er i systemet, og som derfor umiddelbart kan tildeles adgang, at sikre dørmænd et bedre arbejdsmiljø, og at sikre, at følgende personer ikke får adgang til diskoteket: 1) Mindreårige 2) personer, som har karantæne og 3) personer som har forbud fra politiet.</p>  |
| <b>3. Generel beskrivelse</b> | <p>Følgende typer af behandling indgår: Der sker indsamling, registrering, brug, opbevaring og sletning af generelle kundeoplysninger og eventuelle karantæneforhold samt oplysninger i form af billede og fingeraftryk (template). Oplysningerne bliver kun registreret med samtykke fra gæsten. Oplysninger kan videregives til politiet i forbindelse med indgivelse af en politianmeldelse. Hvis der modtages et forbud fra politiet på en person, behandles oplysningerne indeholdt heri ligeledes.</p> <hr/> <p>Oplysningerne behandles:</p> <p><input checked="" type="checkbox"/> elektronisk og/eller</p> <p><input checked="" type="checkbox"/> manuelt</p> <p>Der behandles følgende følsomme oplysninger:</p> <p><input type="checkbox"/> Racemæssig eller etnisk baggrund</p> <p><input type="checkbox"/> Politisk overbevisning</p> <p><input type="checkbox"/> Religiøs overbevisning</p> <p><input type="checkbox"/> Filosofisk overbevisning</p> <p><input type="checkbox"/> Fagforeningsmæssige tilhørsforhold</p> <p><input checked="" type="checkbox"/> Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.</p> <p><input type="checkbox"/> Seksuelle forhold</p> <p>Der behandles følgende andre oplysninger om enkeltpersoners rent private forhold:</p> <p><input checked="" type="checkbox"/> Strafbare forhold</p> <p><input type="checkbox"/> Væsentlige sociale problemer</p> <p><input type="checkbox"/> Andet</p> |

|  |   |
|--|---|
| <p><b>4. Kategorier af registrerede og oplysningstyper</b></p> | <p>Der behandles oplysninger om følgende kategorier af personer:*</p> <p>A) Diskotekets gæster</p> <p>B) Diskotekets gæster, der har fået en karantæne</p> <p>C) Personer, der har fået et forbud fra politiet i medfør af restaurationsloven</p> <p>D)</p> <p>E)</p> <p>Der behandles følgende typer af oplysninger om de ovenfor angivne kategorier af personer:*</p> <p>ad A) Oplysninger om navn, adresse, telefonnummer, e-mail-adresse, fødselsdato, køn og ankomsttidspunkt. Desuden oplysninger i form af billede og fingeraftryk. Endvidere oplysninger i form af billedeoptagelser, der optages på diskoteket i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed.</p> <p>ad B) Oplysninger som under ad A) samt oplysninger om karantæneperiode og -årsag, herunder oplysninger om strafbare forhold og helbredsmæssige forhold i forbindelse med narkotikamisbrug m.v. Karantæneårsag opbevares kun på baggrund af gæstens samtykke.</p> <p>ad C) Oplysninger om navn, adresse, personnummer, årsagen til forbuddet og dets udløbsdato.</p> <p>ad D)</p> <p>ad E)</p> |
| <p><b>5. Modtagere</b></p>                                     | <p>Oplysningerne kan overføres til følgende modtagere eller kategorier af modtagere: Politiet i forbindelse med indgivelse af en politianmeldelse.</p>  |
| <p><b>6. Tredjelande</b></p>                                   | <p>Der påtænkes overført oplysninger til tredjelande:</p> <p><input type="checkbox"/> ja</p> <p><input checked="" type="checkbox"/> nej</p>   |
| <p><b>7. Sikkerhed</b></p>                                     | <p>Generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden: Alle ad-</p>   |

|  |   |
|--|---|
|  | <p>gange 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 kun administrator, som kan se oplysninger om karantæneårsag. alle anvendelser af oplysningerne logges i systemet. Manuelle oplysninger opbevares i ringbind på et aflåst kontor.</p>   |
| <b>8. Påbegyndelse</b>                   | <p>Tidspunkt for påbegyndelse af behandling:*<br/>Dato 1. juli 2008</p>   |
| <b>9. Sletning</b>                       | <p>Tidspunkt for sletning af oplysningerne:* 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 billedeoptagelser fra overvågningskameraer slettes efter 30 dage.</p> |
| <b>10. Underskrift</b>                   | <p>Offentliggøres ikke i fortegnelsen<br/>Dato* 22-01-2008<br/>Navn*<br/>Henrik Karlsen</p>   |
| Følgrebrev/bemærkninger til Datatilsynet |   |
| <b>Note fra Datatilsynet</b>             |   |

## **Diskotekers registrering af billede, fingeraftryk og karantæneoplysninger**

Datatilsynet har i forbindelse med en konkret sag taget stilling til diskotekers mulighed for at registrere gæsternes billede, fingeraftryk og eventuelle karantæneoplysninger.

### **Registrering af fingeraftryk og billede**

Diskoteker kan med gæstens udtrykkelige samtykke registrere dennes fingeraftryk (template) og billede.

Hvis gæsten tilbagekalder sit samtykke, skal diskoteket slette fingeraftrykket (templaten) og billedet.

### **Registrering af karantæneoplysninger**

Registrering af følsomme personoplysninger, f.eks. om strafbare forhold og narkotikamisbrug, i forbindelse med, at et diskotek tildeler en gæst en karantæne, må kun ske med gæstens skriftlige samtykke. Samtykket skal være udtrykkeligt og skal opfylde persondatalovens krav. Dvs. det skal være frivilligt, specifikt og informeret.

Der skal foretages anmeldelse til samt indhentes tilladelse fra Datatilsynet, hvis et diskotek registrerer følsomme personoplysninger, f.eks. om strafbare forhold og narkotikamisbrug.

Læs mere om anmeldelsespligten.

### **Hvis gæsten tilbagekalder sit samtykke**

Hvis gæsten tilbagekalder sit samtykke, skal oplysninger om årsagen til karantænen slettes.

Dvs. at diskoteket skal slette følsomme personoplysninger om strafbare forhold og narkotikamisbrug, hvis gæsten tilbagekalder samtykket.

Diskoteket vil efter en konkret vurdering kunne gemme oplysninger om navn, adresse, samt hvor længe personen er uønsket som gæst i diskoteket.

### **Forbud udstedt af politiet**

Diskoteker kan uden gæstens samtykke registrere og bruge oplysninger om forbud, som politiet har udstedt i medfør af restaurationsloven, i forbindelse med deres adgangskontrol.

Når et forbud fra politiet udløber, skal forbudet og alle oplysninger om det slettes eller makuleres hos diskoteket.

Der skal foretages anmeldelse til samt indhentes tilladelse fra Datatilsynet, hvis et diskotek registrerer og bruger følsomme personoplysninger, herunder oplysninger om strafbare forhold i form af forbud fra politiet.

Læs mere om anmeldelsespligten.

Læs mere: Brev til Crazy Daisy, Biometri, Anmeldelsesordningen