



Forside / Erhverv / Forskere og medicinalfirmaer / Standardvilkår for forskningsprojekter

Opdateret: 06.05.15

Standardvilkår for forskningsprojekter

(Projekter anmeldes på blanketten "Privat forskning")

Når Datatilsynet giver tilladelse til behandling af følsomme personoplysninger i et projekt til videnskabelige eller statistiske formål i henhold til persondatalovens § 10, jf. § 50, stk. 1, nr. 1, fastsættes en række vilkår for projektet. Vilkårene skal først og fremmest bevirke, at den dataansvarlige (projektlederen) overholder reglerne i persondataloven og at databehandlingen lever op til lovens krav om datasikkerhed.

Det fremgår af lovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

På denne baggrund har Datatilsynet udformet en række standardvilkår, som alle projekter skal efterleve. Hermed garanteres, at databehandlingen sker med den nødvendige sikkerhed, og at alle personer, der indgår i projekter til videnskabelige eller statistiske formål (de registrerede), omfattes af den samme beskyttelse.

Datatilsynets tilladelse til projektet er betinget af, at man følger Datatilsynets vilkår.

Standardvilkårene er gengivet nedenfor. Vilkår markeret "**Specialvilkår**" fastsættes efter behov, de øvrige vilkår fastsættes for alle projekter. I særlige tilfælde vil Datatilsynet også kunne fastsætte individuelle eller supplerende vilkår for et projekt.

DATATILSYNETS STANDARDVILKÅR:

TILLADELSE

Datatilsynet meddeler hermed tilladelse til projektets gennemførelse, jf. persondataloven, § 50, stk. 1, nr. 1. Datatilsynet fastsætter i den forbindelse nedenstående vilkår:

Generelle vilkår

Tilladelsen gælder indtil: (dato)

Ved tilladelsens udløb skal De særligt være opmærksom på følgende:

Hvis De ikke inden denne dato har fået tilladelsen forlænget, går Datatilsynet ud fra, at projektet er afsluttet, og at personoplysningerne er slettet, anonymiseret, tilintetgjort eller overført til arkiv, jf. nedenstående vilkår vedrørende projektets afslutning. Anmeldelsen af Deres projekt fjernes derfor fra fortegnelsen over anmeldte behandlinger på Datatilsynets hjemmeside.

Datatilsynet gør samtidig opmærksom på, at al behandling (herunder også opbevaring) af personoplysninger efter tilladelsens udløb er en overtrædelse af persondataloven, jf. § 70.

- (Den dataansvarliges navn) er ansvarlig for overholdelsen af de fastsatte vilkår.
- Oplysningerne må kun anvendes til brug for projektets gennemførelse.
- Behandling af personoplysninger må kun foretages af den dataansvarlige eller på foranledning af den dataansvarlige og på dennes ansvar.
- Enhver, der foretager behandling af projektets oplysninger, skal være bekendt med de fastsatte vilkår.
- De fastsatte vilkår skal tillige iagttages ved behandling, der foretages af databehandler.
- Lokaler, der benyttes til opbevaring og behandling af projektets oplysninger, skal være indrettet med henblik på at forhindre uvedkommende adgang.
- Behandling af oplysninger skal tilrettelægges således, at oplysningerne ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Urigtige eller vildledende oplysninger eller oplysninger, som er behandlet i strid med loven eller disse vilkår, skal berigtiges eller slettes.
- Oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til projektets gennemførelse.
- En eventuel offentliggørelse af undersøgelsens resultater må ikke ske på en sådan måde, at det er muligt at identificere enkeltpersoner.
- Eventuelle vilkår, der fastsættes efter anden lovgivning, forudsættes overholdt.

Elektroniske oplysninger

- Identifikationsoplysninger skal krypteres eller erstattes af et kodenummer el. lign. Alternativt kan alle oplysninger lagres krypteret. Krypteringsnøgle, kodenøgle m.v. skal opbevares forsvarligt og adskilt fra personoplysningerne.
- Adgangen til projektdata må kun finde sted ved benyttelse af et fortroligt password. Password skal udskiftes mindst én gang om året, og når forholdene tilsiger det.
- Ved overførsel af personhenførbare oplysninger via Internet eller andet eksternt netværk skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Oplysningerne skal som minimum være forsvarligt krypteret under hele transmissionen. Ved anvendelse af interne net skal det sikres, at uvedkommende ikke kan få adgang til oplysningerne.
- Udtagelige lagringsmedier, sikkerhedskopier af data m.v. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.

Manuelle oplysninger

- Manuelt projektmateriale, udskrifter, fejl- og kontrollister, m.v., der direkte eller indirekte kan henføres til bestemte personer, skal opbevares forsvarligt aflåst og på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med indholdet.

Biobank og biologisk materiale (Specialvilkår)

- Prøver med biologisk materiale og biologisk materiale i biobanker skal opbevares forsvarligt aflåst, således at uvedkommende ikke har adgang til det, og på en sådan måde, at det sikres, at materialet ikke fortabes, forringes eller hændeligt eller ulovligt tilintetgøres.
- Biologisk materiale, der er mærket med personnummer eller navn, skal opbevares under iagttagelse af særlige sikkerhedshensyn.
- Der skal fastsættes interne retningslinjer i projektet for opbevaring af biologisk materiale. Retningslinjerne skal ajourføres mindst én gang om året.

Oplysningspligt over for den registrerede

- Hvis der skal indsamles oplysninger hos den registrerede (ved interview, spørgeskema, klinisk eller paraklinisk undersøgelse, behandling, observation m.v.) skal der uddeles/fremsendes nærmere information om projektet. Den registrerede skal heri oplyses om den dataansvarliges navn, formålet med projektet, at det er frivilligt at deltage, og at et samtykke til deltagelse til enhver tid kan trækkes tilbage. Hvis oplysningerne skal videregives til brug i anden videnskabelig eller statistisk sammenhæng, skal der også oplyses om formålet med videregivelsen samt modtagerens identitet.
- Den registrerede skal endvidere oplyses om, at projektet er anmeldt til Datatilsynet efter persondataloven, samt at Datatilsynet har fastsat nærmere vilkår for projektet til beskyttelse af den registreredes privatliv.

Indsigtsret

- Den registrerede har ikke krav på indsigt i de oplysninger, der behandles om den pågældende.

Videregivelse

- Videregivelse af personhenførbare oplysninger til tredjepart må kun ske til brug i andet statistisk eller videnskabeligt øjemed.
- Videregivelse må kun ske efter forudgående tilladelse fra Datatilsynet. Datatilsynet kan stille nærmere vilkår for videregivelsen samt for modtagerens behandling af oplysningerne.
- **(Specialvilkår)** Oplysninger kan herudover videregives, hvis det fremgår af anden lovgivning, at oplysningerne skal videregives.

Behandling ved databehandler (Specialvilkår)

- Datatilsynets vilkår gælder også ved behandling hos databehandler.
- Ved behandling hos databehandler skal der indgås en skriftlig aftale herom mellem den dataansvarlige og databehandleren. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at oplysninger ikke må anvendes til databehandlerens egne formål. Databehandleren skal desuden give den dataansvarlige tilstrækkelige oplysninger til, at denne til enhver tid kan sikre sig, at Datatilsynets vilkår kan overholdes, og at de bliver overholdt.
- Hvis databehandleren er etableret i en anden medlemsstat, skal det desuden fremgå af aftalen, at de yderligere bestemmelser om sikkerhedsforanstaltninger for databehandlere, som eventuelt er fastsat i den medlemsstat, hvor databehandleren er etableret, også er gældende for databehandleren.

Ændringer i projektet

- Væsentlige ændringer i projektet skal anmeldes til Datatilsynet (som ændring af eksisterende anmeldelse). Ændringer af mindre væsentlig betydning kan meddeles Datatilsynet.
- Ændring af tidspunktet for projektets afslutning skal altid anmeldes.

Ved projektets afslutning

- Senest ved projektets afslutning skal oplysningerne slettes, anonymiseres eller tilintetgøres, således at det efterfølgende ikke er muligt at identificere enkeltpersoner, der indgår i undersøgelsen.
- Alternativt kan oplysningerne overføres til videre opbevaring i Statens Arkiver (herunder Dansk Dataarkiv) efter arkivlovens regler.
- Sletning af oplysninger fra elektroniske medier skal ske på en sådan måde, at oplysningerne ikke kan genetableres.

Overførsel af oplysninger til tredjelande (Specialvilkår)

- Overførsel af oplysninger til tredjelande, herunder til behandling hos databehandler samt til intern anvendelse i projektet, kræver forudgående tilladelse fra Datatilsynet.
- Overførsel kan dog ske uden tilladelse, hvis den registrerede har givet udtrykkeligt samtykke til dette. Den registrerede kan tilbagekalde samtykket.
- Overførsel af oplysninger skal ske med bud eller anbefalet post. Ved elektronisk overførsel skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Oplysningerne skal som minimum være forsvarligt krypteret under hele transmissionen.

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

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

JJ

Privathospitalet Mølholm A/S
Brummersvej 1
7100 Vejle
Att. Direktionen

7. august 2009

Vedrørende tilladelse til behandlingen "Patientbehandling hos Privathospitalet Mølholm A/S"

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2007-42-0333

Sagsbehandler
Karina Kok Jørgensen
Direkte 3319 3224

I henhold til lov om behandling af personoplysninger (persondataloven)¹ § 48 har Privathospitalet Mølholm A/S den 10. oktober 2005 anmeldt behandlingen "Biobank/knoglefryser" til Datatilsynet. Privathospitalet Mølholm A/S har endvidere den 13. september 2006 anmeldt behandlingen "Registrering af patientoplysninger i EPJ (Skalpell)" til Datatilsynet. Der er samtidig ansøgt om tilladelse i henhold til lovens § 50, stk. 1, nr. 1.

De oprindelige anmeldelser er ifølge aftale ændret således, at der er lavet én generel anmeldelse, der omfatter de oprindelige to anmeldelser, og som omfatter Privathospitalet Mølholm A/S' generelle behandling af personoplysninger "Patientbehandling hos Privathospitalet Mølholm A/S".

Privathospitalet Mølholm A/S har den 30. juli 2009 betalt 1.000 kr. til dækning af gebyr i henhold til persondatalovens § 63, stk. 2, nr. 2.

I den anledning meddeler Datatilsynet hermed

TILLADELSE

til behandlingen "Patientbehandling hos Privathospitalet Mølholm A/S".

Tilladelse gives på følgende vilkår:

- I. I det omfang behandling, herunder videregivelse, af personoplysninger ikke er reguleret af særregler, herunder navnlig i sundhedsloven og vævslovgivningen, skal behandling af personoplysninger, som foretages af Privathospitalet Mølholm A/S, ske i overensstemmelse med persondatalovens regler.

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer. Loven kan ses på Datatilsynets hjemmeside www.datatilsynet.dk under punktet "Lovgivning".

2. Behandling af personoplysninger forudsættes i øvrigt at ske under iagttagelse af gældende lovgivning, herunder navnlig sundhedsloven og vævslovgivningen.
3. Behandling af personoplysninger skal ske under iagttagelse af de i bilag 1 beskrevne sikkerhedsregler.
4. Den enkelte medarbejder skal informeres om, at deres opslag logges, og at loggen kan bruges til at kontrollere uberettigede opslag samt til stikprøvekontrol.

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

Der henvises i øvrigt til Datatilsynets brev af 23. april 2009.

Anmeldelsen vil snarest blive offentliggjort i fortegnelsen på Datatilsynets hjemmeside.²

Med venlig hilsen

Karina Kok Jørgensen

Bilag: Bilag 1 - Sikkerhedsregler for behandling af personoplysninger, der er anmeldt til Datatilsynet af en privat dataansvarlig.

² www.datatilsynet.dk.

Bilag 1

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

I medfør af § 50, stk. 5, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) 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 it-systemer. 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. Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at de fastsatte vilkår ligeledes gælder for behandlingen ved databehandleren.
4. Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarliges lokaliteter, skal den dataansvarlige fastsætte særlige retningslinier herfor, så det sikres, at de fastsatte vilkår iagttages.

5. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne. Udtagelige lagringsmedier, sikkerhedskopier af data m.v. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.
6. Såfremt der er etableret eller etableres en digital selvbetjeningsløsning – f.eks. adgang til at indsende og modtage oplysninger via login på en hjemmeside – skal login baseres på digital signatur.
7. 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. Al transmission af følsomme personoplysninger over internettet skal ske i krypteret form.
8. 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

9. 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

10. 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

11. 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, indda-

tere eller slette personoplysninger. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

12. 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.
13. Sundhedslovens regler om adgang til elektroniske patientjournaler skal iagttages ved autorisation. 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.
14. 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.
15. 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

16. 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.

Biologisk materiale

17. Prøver med biologisk materiale og biologisk materiale i biobanker skal opbevares forsvarligt aflåst, således at uvedkommende ikke har adgang til det, og på en sådan måde, at det sikres, at materialet ikke fortabes, forringes eller hændeligt eller ulovligt tilintetgøres.
18. Biologisk materiale, der er mærket med personnummer eller navn, skal opbevares under iagttagelse af særlige sikkerhedshensyn.
19. Der skal fastsættes interne retningslinier for opbevaring af biologisk materiale. Retningslinierne skal gennemgås mindst én gang om året og ajourføres i fornødent omfang.

JJ

Håndværksrådet
Islands Brygge 26
Postboks 1990
2300 København S

17. september 2007

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2007-43-0004
og 2007-221-0078

Tidligere j.nr.
2005-43-0205 og
2005-2221-0051

Sagsbehandler
Tina Fugl
Direkte 3319 3229

Vedrørende Håndværksrådets etablering af et advarselsregister over annoncehajer

Under henvisning til Datatilsynets brev af 22. januar 2007 og Håndværksrådets brev af 31. august 2007 samt indbetaling af gebyr den 5. september 2007 skal Datatilsynet hermed meddele Håndværksrådet

TILLADELSE

til behandling af personoplysninger med henblik på at advare andre mod forretningsforbindelse med eller ansættelsesforhold til en registreret. Tilladelsen meddeles på følgende vilkår:

Optagelse i advarselsregisteret:

1. Der må ikke ske registrering af en oplysning om et forhold, som er urigtigt eller vildledende.

Der må ikke registreres oplysninger om strafbare forhold.

2. Kun personer eller virksomheder, med hvem Håndværksrådet har indgået aftale om indberetning, må foretage indberetning til registeret. Håndværksrådet skal gøre indberetterne bekendt med, i hvilke tilfælde der må ske indberetning, herunder bl.a. at der ikke må indberettes oplysninger om strafbare forhold. Aftalen med indberetteren bør desuden omhandle forpligtigelsen efter vilkår 12 til at give meddelelse til Håndværksrådet, hvis de indberettede oplysninger viser sig urigtige eller vildledende.
3. Ved enhver indberetning skal Håndværksrådet kende indberetterens identitet. Hvis indberetningen sker via en hjemmeside på internettet, skal indberetteren være identificeret ved digital signatur, Net ID eller brugernavn og password. Hvis indberetningen undtagelsesvist modtages via almindelig e-post, må Håndværksrådet via almindelig post eller på anden vis indhente en underskrift eller anden sikkerhed for indberetterens identitet.

4. Der må kun indberettes oplysninger om annonceudbydere m.v., der har anvendt usædvanlige forretningsmetoder.
5. Der må kun ske videregivelse af oplysninger om personer eller virksomheder, hvis:
 - a) fem klager vedrørende samme annonceudbyder er indgivet
 - eller
 - b) en indgivet klage vedrører særligt grove omstændigheder.
6. Der må ikke ske telefonisk indberetning.
7. Der må alene videregives enkeltstående summariske oplysninger.
8. Der må kun registreres og videregives oplysninger om, hvorvidt en annonceudbyder er medlem/ikke er medlem af Foreningen af Danske Internetmedier (FDIM), hvis der foreligger dokumentation herfor.

Oplysningspligt

9. Der skal, senest 4 uger efter optagelse i advarselsregisteret, altid gives den registrerede meddelelse om navn og adresse på Håndværksrådet, formålet med behandlingen, hvem der har indberettet oplysningen, hvorvidt oplysningen vil blive videregivet og i givet fald kategorien af modtagere, om adgangen til indsigt, jf. vilkår 10, om adgangen til berigtigelse af de oplysninger, der vedrører den registrerede, jf. vilkår 13, samt om adgangen til at klage til Datatilsynet, jf. vilkår 15.

Indsigt

10. Håndværksrådet skal til enhver tid på begæring af den registrerede inden 4 uger på en let forståelig måde meddele denne indholdet af de oplysninger, som foreningen på tidspunktet for begæringens fremsættelse behandler om den pågældende. Håndværksrådet skal endvidere give oplysninger om formålet hermed, kategorier af modtagere af oplysningerne, samt tilgængelig information om, hvorfra oplysningerne stammer.

Godtgørelse af behandlingen

11. Det påhviler Håndværksrådet at godtgøre behandlingens berettigelse, når der af en registreret rejses tvivl om rigtigheden af en registrering eller videregivelse. I den forbindelse skal Håndværksrådet indhente udtalelser fra indberetterne, såfremt dette er nødvendigt til afklaring af sagen.

Urigtige/vildledende oplysninger

12. Indberetterne skal straks give meddelelse til Håndværksrådet om indberettede oplysninger, der viser sig urigtige eller vildledende, og oplysningerne skal snarest slettes eller berigtiges.
13. Videregivne oplysninger der viser sig urigtige eller vildledende, eller som er videregivet i strid med disse vilkår, skal af Håndværksrådet straks berigtiges skriftligt over for de medlemmer/deltagere i ordningen, der har modtaget oplysningen. Desuden skal der berigtiges over for den registrerede, som skal have oplyst, hvilke medlemmer/deltagere i ordningen der har modtaget berigtigelsen efter 1. pkt., og hvorfra oplysningen stammer.

Sletning af oplysninger

14. Oplysninger om en registreret skal slettes senest 2 år efter, at registreringen er sket.

Klageadgang

15. Henvendelser fra en registreret om sletning, berigtigelse eller blokering af oplysninger, der angives at være urigtige eller vildledende, eller sletning af oplysninger, der ikke må behandles jf. vilkår nr. 1-8, skal snarest og inden 4 uger efter modtagelsen besvares skriftligt af Håndværksrådet

Nægter Håndværksrådet at foretage den begærede sletning, berigtigelse eller blokering, kan den registrerede indbringe spørgsmålet for Datatilsynet, hvilket skal oplyses over for den registrerede.

Sikkerhed

16. Oplysningerne skal ajourføres løbende. Hvis der udsendes advarselstaster i papirform, skal disse udsendes mindst hver 3. måned. Straks efter modtagelsen, skal medlemmet/deltageren i ordningen destruere tidligere modtagne lister el. lign., hvilket skal angives af Håndværksrådet i forbindelse med udsendelsen. Kravet om destruktion af tidligere lister glæder også lister i elektronisk form, der er hentet fra hjemmeside, eller som medlemmet/deltageren i ordningen har modtaget via e-post, CD-rom eller diskette.
17. Der skal hos Håndværksrådet og medlemmerne /deltagerne i ordningen træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger i registeret ikke misbruges eller kommer til uvedkommendes kendskab.

18. Hvis der anvendes advarselslister i papirform, skal disse opbevares aflåst, når de ikke benyttes. Det samme gælder lister i elektronisk form, der er hentet fra en hjemmeside, eller som medlemmet/deltageren i ordningen har modtaget via e-post, CD-rom eller diskette.
19. Ved indberetning eller videregivelse via en hjemmeside på internettet eller ved fremsendelse af indberetninger eller advarselslister ved brug af e-post skal der anvendes en forsvarlig kryptering.
20. Hvis der gives brugerne af listen adgang til oplysningerne via en hjemmeside, må dette alene ske efter indtastning af bruger id og adgangskode (password). Håndværksrådet skal være i besiddelse af oplysninger om, hvem der har fået tildelt adgang, således at forpligtigelsen efter vilkår 13 til at foretage berigtigelse kan efterleves.
21. Der må ikke videregives oplysninger fra advarselslisten telefonisk.

Ændringer/ophør

22. Inden iværksættelse af ændringer i de oplysninger, der er meddelt Datatilsynet i forbindelse med udstedelse af tilladelse, skal Datatilsynet tilladelse indhentes. Ændringer af mindre væsentlig betydning skal dog kun anmeldes. Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen.

Ophør af førelsen af advarselsregisteret skal straks meddeles til Datatilsynet.

De ovenstående vilkår er glædende indtil videre. Datatilsynet forbeholder sig senere at tage vilkårene op til revision, hvis der skulle vise sig behov for det. Endvidere er vilkårene supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Det skal derfor understreges, at reglerne i persondataloven finder anvendelse i det omfang, der er tale om forhold, der er reguleret i de ovenstående vilkår

Anmeldelsen vil snarest blive offentliggjort i fortegnelsen på Datatilsynets hjemmeside www.datatilsynet.dk.

Med venlig hilsen

Lena Andersen
Kontorchef

Forenede Danske Motorejere
Firskovvej 32
2800 Lyngby

Sendt til: shp@fdm.dk

11. juni 2008

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2008-44-0012
Sagsbehandler
Jesper Husmer Pedersen
Direkte 3319 3216

Vedrørende anmeldelse af behandlingen "Spærreliste over spærrede MasterCard"

Under henvisning til Datatilsynets brev af 28. maj 2008 og Forenede Danske Motorejeres (herefter FDM) indbetaling af gebyr den 10. juni 2008 i henhold til persondatalovens § 63, stk. 2, nr. 2, skal Datatilsynet hermed meddele FDM

T I L L A D E L S E

til behandling af personoplysninger ved førelse af en spærreliste over spærrede MasterCard. Tilladelsen meddeles på følgende vilkår:

Optagelse på spærrelisten

1. FDM må optage et betalingskort på spærrelisten, når kortet meldes stjålet eller tabt, eller når kortindehaver ønsker kortet optaget på spærrelisten på grund af mistanke om, at kortnummer, udløbsdato og kontrolcifre er kommet til uvedkommendes kendskab. Der kan endvidere ske optagelse på spærrelisten ved mistanke om, at kortet er kopieret, samt når kontoforholdet er opsagt, og kortet er søgt inddraget. Der kan også ske spærring, såfremt kortindehaver ønsker fornyelse af sit kort, før kortet udløber, og kortet ikke er indleveret.

Endvidere kan der spærres for anvendelse af et kort, når kortindehaver har misbrugt sit kort med overtræk på den til kortet knyttede konto til følge, og FDM – forinden spærring finder sted – har udsendt mindst 2 skriftlige ryk-kere med angivelse af, at kortet skal afleveres til FDM og vil blive spærret, såfremt betaling ikke sker. Alle kort, der er tilknyttet den pågældende konto, kan spærres.

Herudover må der ske spærring straks, hvis der foreligger særlige omstændigheder, særligt hvis der er en begrundet formodning for misbrug af kortet, eksempelvis hvor der sker omfattende køb på kortet inden for et meget kort tidsrum, som ikke ligger inden for kortindehaverens normale forbrugsmønster.

Videregivelse og sletning af oplysninger

2. Der må kun videregives oplysninger om kortindehaverens konto- eller kortnummer. Der må ikke videregives oplysninger om årsagen til, at et betalingskort er spærret.
3. Oplysninger om kortnummeret på et spærret betalingskort skal slettes senest ved kortets udløbsdato. Oplysninger om kortnummeret skal dog slettes straks, når kortet er blevet inddraget eller på anden måde er kommet i kortudsteders besiddelse, bortset fra tilfælde, hvor kortet er spærret og inddraget på grundlag af misbrug eller mistanke om misbrug, og hvor der er risiko for, at kortet kan være kopieret. Endvidere skal oplysning om kortnummeret slettes straks, når tekniske muligheder for at benytte det pågældende kort uden spærring ikke længere er til stede, eksempelvis ved overgang til nye kort.

Udsteders oplysningspligt

4. Ved indledning af et kontraktforhold om udstedelse af et MasterCard skal det oplyses, at der i de i vilkår 1, 1. og 2. pkt., nævnte tilfælde vil kunne ske spærring af kort.
5. FDM skal give skriftlig meddelelse om spærring af kortet til kortindehaveren i forbindelse med, at spærring finder sted. Undtaget herfra er de tilfælde, hvor kortet af kortindehaver meldes tabt eller stjålet, samt i tilfælde, hvor kortindehaver melder kortet defekt eller ødelagt. Meddelelsen skal indeholde oplysning om kortudsteders navn og adresse, kategorier af modtagere af oplysningen om spærring, retten til indsigt (jf. vilkår 6) samt klageadgang til Datatilsynet (jf. vilkår 9).

Den registreredes indsigt

6. FDM skal til enhver tid på begæring af den registrerede give denne meddelelse om indholdet af de oplysninger, som FDM på tidspunktet for begæringens fremsættelse behandler om den pågældende, kategorier af modtagere af oplysningen om spærring samt tilgængelig information om, hvorfra oplysningerne stammer. Meddelelsen skal gives snarest – og inden 4 uger efter begæringen. Den registrerede kan forlange, at meddelelsen gives skriftligt.

Urigtige/vildledende oplysninger

7. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.
8. Videregivne oplysninger, der viser sig urigtige eller vildledende, eller som er videregivet i strid med vilkårene, skal af FDM berigtiges skriftligt over for den registrerede og de betalingsmodtagere, der har modtaget oplysningerne. Desuden skal den registrerede have meddelelse om, hvilke beta-

lingsmodtagere der har modtaget berigtigelsen efter 1. pkt., og hvorfra oplysningen stammer.

Berigtigelse skal ske på en af følgende måder:

- a) Den registrerede oplyser på forespørgsel fra FDM eller i forbindelse med en klagesag på foranledning af Datatilsynet, over for hvem berigtigelse ønskes, eller at berigtigelse ikke ønskes. FDM foretager herefter berigtigelse i overensstemmelse hermed. Hvis den registrerede angiver en betalingsmodtager, der kan udelukkes som modtager af oplysningerne, skal FDM oplyse den registrerede herom.
- b) Den registrerede oplyser på forespørgsel fra FDM eller i forbindelse med en klagesag på foranledning af Datatilsynet, at berigtigelse ønskes, men det oplyses ikke, over for hvem berigtigelse ønskes. FDM foretager herefter berigtigelse over for de betalingsmodtagere, som ifølge FDMs log over online-transaktioner har modtaget oplysningerne.

9. Indsigelser fra en registreret over for berettigelsen af en behandling af oplysninger skal snarest – og inden 4 uger – besvares skriftligt af FDM.

Nægter FDM at slette eller berigtige i overensstemmelse med indsigelsen, kan den registrerede indbringe spørgsmålet for Datatilsynet. Datatilsynet træffer herefter afgørelse om, hvorvidt der skal foretages sletning eller berigtigelse. FDM skal i svaret gøre den registrerede bekendt med adgangen til at indbringe spørgsmålet for Datatilsynet.

Sikkerhedsforanstaltninger

10. Oplysningerne på spærrelisten skal ajourføres løbende.

11. Der skal hos FDM og betalingsmodtagere træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger på spærrelisten ikke misbruges eller kommer til uvedkommendes kendskab.

Ændringer og ophør af førelsen af spærrelisten

12. Inden iværksættelse af ændringer i de oplysninger, som er meddelt Datatilsynet i forbindelse med udstedelse af tilladelse, skal Datatilsynets tilladelse indhentes. Ændringer af mindre væsentlig betydning skal dog kun anmeldes til Datatilsynet. Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen af ændringerne.
Ophør af førelsen af spærrelisten skal straks meddeles til Datatilsynet.

De ovenstående vilkår er gældende indtil videre. Datatilsynet forbeholder sig ret til senere at tage vilkårene op til revision, hvis der skulle vise sig behov herfor.

Endvidere er vilkårene supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Det skal derfor

understreges, at reglerne i persondataloven finder anvendelse, i det omfang der er tale om forhold, som ikke er reguleret i ovenstående vilkår.

Datatilsynet skal henlede opmærksomheden på, at vilkårene omhandler *spærring* af kort. Automatisk afvisning af køb, når kreditmaksimum overskrides, uden at kortet derved spærres, kan derfor ske, uafhængigt af om betingelserne for spærring er opfyldt.

Datatilsynet skal endvidere henlede opmærksomheden på persondatalovens § 42, stk. 2, hvoraf det følger, at gennemførelse af en behandling ved en databehandler skal 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 databehandler.

Af FDMs anmeldelse fremgår det, at der påtænkes overført oplysninger til tredjelande. Datatilsynet skal i den anledning henlede opmærksomheden på reglerne i persondatalovens § 27. Tilsynet skal endvidere henlede opmærksomheden på persondatalovens § 50, stk. 2, hvoraf fremgår, at sådanne overførsler i visse tilfælde kræver en tilladelse fra Datatilsynet. Det bemærkes afslutningsvist, at FDMs anmeldelse ikke kan tjene som ansøgning efter lovens § 50, stk. 2. En sådan tilladelse skal søges særskilt.

Med venlig hilsen

Jesper Husmer Pedersen

Intrum Justitia A/S
Lyngbyvej 20, 2.sal
2100 København Ø

Att.: Helle Petersen

25. juni 2008

Vedrørende anmeldelse/ansøgning om tilladelse til behandling af personoplysninger med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed

Datatilsynet
Borgergade 28, 5.
1300 København K

Under henvisning til Datatilsynets brev af 19. juni 2008 og Intrum Justitia A/S' indbetaling af gebyr den 23. juni 2008 skal Datatilsynet herved meddele Intrum Justitia A/S

CVR-nr. 11-88-37-29

TILLADELSE

Telefon 3319 3200
Fax 3319 3218

til behandling af personoplysninger med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed (kreditoplysningsbureau). Tilladelsen meddeles på følgende vilkår:

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

Særlige behandlingsregler

J.nr. 2008-45-0005

Sagsbehandler
Christine Boeskov
Direkte 3319 3246

1. Der må ikke ske registrering, videregivelse eller anden behandling, herunder trues med indberetning, af en fordring på en person eller virksomhed, hvis fordringen er bestridt.
2. Intrum Justitia A/S skal gennem abonnementsvilkår el. lign. sikre sig, at bureauets abonnenter ikke indhenter kreditoplysninger om en person til brug for ansættelse af den pågældende. Dette gælder, uanset om den person, der søges oplysninger om, har givet samtykke til, at oplysningerne indhentes. Oplysninger må dog indhentes, hvis der er tale om ansættelse i en særligt betroet stilling, hvor det af hensyn til stillingsbesættelsen er nødvendigt at indhente oplysninger om den pågældendes soliditet og kreditværdighed.
3. Intrum Justitia A/S skal sikre sig den nødvendige dokumentation for, at betingelserne for indberetning og videregivelse er opfyldt.

Oplysningspligt

4. Der skal, senest 4 uger efter indsamling af oplysningerne finder sted, altid gives den registrerede meddelelse om navn og adresse på Intrum Justitia A/S, formålet med behandlingen, hvem der har indberettet op-

lysningen, kategorierne af modtagere, om adgangen til indsigt, om adgangen til berigtigelse af de oplysninger, der vedrører den registrerede, samt om adgangen til at klage til Datatilsynet, jf. vilkår 8.

Hvis oplysningerne indsamles telefonisk hos den registrerede ved eksempelvis interviews skal bureauet endvidere oplyse, om det er obligatorisk eller frivilligt at besvare de stillede spørgsmål samt mulige følger af ikke at svare.

Hvis registreringen vedrører et skyldforhold, og der ikke foreligger en endelig retslig afgørelse, skal det som minimum fremgå af meddelelsen, at den registrerede vil blive slettet, hvis den registrerede ved henvendelse til bureauet bestrider fordringens størrelse eller rigtighed.

En sådan indsigelse kan afgives til bureauet såvel skriftligt som mundtligt af den registrerede.

Hvis registreringen vedrører et skyldforhold, hvor betingelserne for videregivelse i summarisk form i persondatalovens § 23, stk. 3, ikke er opfyldt, skal det fremgå af meddelelsen, at oplysninger om gælden ikke vil blive videregivet.

Hvis bureauet anvender oplysninger, der ikke må videregives i summarisk form, i bedømmelser af den registreredes kreditværdighed, skal dette fremgå af meddelelsen, som desuden skal indeholde en klar og udtrykkelig beskrivelse – i generel form – af de parametre, der vil komme til at indgå i beregningen.

Urigtige/vildledende oplysninger

5. Det påhviler Intrum Justitia A/S at godtgøre behandlingens berettigelse, når der af en registreret rejses tvivl om dens rigtighed.

Intrum Justitia A/S kan ikke stille krav om, at debitor skriftligt begærer sletning, berigtigelse eller blokering, ligesom Intrum Justitia A/S ikke som betingelse for at slette oplysningen kan kræve, at debitor fremsender dokumentation for bestridelsens berettigelse.

6. Ved en udokumenteret henvendelse fra en registreret om, at fordringen er afviklet ved betaling eller på anden måde ophørt, kan Intrum Justitia A/S dog foretage rimelige undersøgelser til afklaring af spørgsmålet, eksempelvis ved i umiddelbar forlængelse af den registreredes henvendelse at anmode den indberettende kreditor om at bekræfte den registreredes oplysning og afmelde registreringen.

Sletning af oplysninger

7. Oplysninger om forhold, der taler imod kreditværdighed, og som er mere end 5 år gamle, må ikke behandles, medmindre det i det enkelte til-

fælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed.

Intrum Justitia A/S er endvidere forpligtet til at iagttage eventuelle særlige sletningsfrister meddelt af Datatilsynet.

Klageadgang

8. Henvendelser fra en registreret om sletning, berigtigelse eller blokering af oplysninger, der angives at være urigtige eller vildledende, eller om sletning af oplysninger, der ikke må behandles, skal snarest og inden 4 uger efter modtagelsen besvares skriftligt af Intrum Justitia A/S.

Nægter Intrum Justitia A/S at foretage den begærede sletning, berigtigelse eller blokering, kan den registrerede indbringe spørgsmålet for Datatilsynet, hvilket den registrerede skal oplyses om.

Sikkerhed

9. Der skal hos Intrum Justitia A/S og bureauets abonnenter træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger i registeret ikke misbruges eller kommer til uvedkommendes kendskab.
10. Fremsendelse af oplysninger over det åbne internet må alene ske i forsvarlig krypteret form.
11. Hvis der gives bureauets abonnenter adgang til oplysningerne via en hjemmeside, skal der endvidere etableres en ordning, således at der kun gives adgang til oplysningerne efter indtastning af en adgangskode (password). Hvis oplysningerne gøres tilgængelige over det åbne internet, skal oplysningerne sendes i forsvarlig krypteret form.

Ændringer/ophør

12. Forinden iværksættelse af ændringer i de oplysninger, der er meddelt Datatilsynet i forbindelse med udstedelsen af tilladelse, skal Datatilsynets tilladelse indhentes. Ændringer af mindre væsentlig betydning skal dog kun anmeldes. Anmeldelse kan ske efterfølgende, dog senest 4 uger efter iværksættelsen.

Ophør af førelsen af kreditoplysningsbureauet skal straks meddeles til Datatilsynet.

De ovenstående vilkår er gældende indtil videre. Datatilsynet forbeholder sig senere at tage vilkårene op til revision, hvis der skulle vise sig behov for det.

Endvidere er vilkårene supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Det skal derfor

understreges, at reglerne i persondataloven finder anvendelse i det omfang, at der er tale om forhold, som ikke er reguleret i de ovenstående vilkår.

Datatilsynet skal om vilkår 3 bemærke, at tilsynet ikke vil stille krav om opbevaring af dokumentation i form af fotokopi af skylderkklæring, stævning m.v. ud over 3 måneder, under forudsætning af, at bureauet gennem kontakten med abonnenten sikrer, at skylderkklæringen, stævningen m.v. på et senere tidspunkt kan fremskaffes.

Datatilsynet kan ligeledes acceptere, at advokater ved indgåelse af en certificeringsaftale med bureauet generelt indestår for opfyldelse af betingelserne i persondatalovens § 23, stk. 3. Datatilsynet kan acceptere en sådan ordning under forudsætning af, at advokaten i forbindelse med konkrete indberetninger af fordringer oplyser, hvilken fordring der er tale om, samt hvilken type fundament der danner grundlag for registrering og videregivelse.

Anmeldelsen vil snarest blive offentliggjort i fortegnelsen på Datatilsynets hjemmeside www.datatilsynet.dk

Med venlig hilsen

Christine Boeskov



[Forside](#) / [Erhverv](#) / [Retsinformation](#) / [Standardvilkår for retsinformationssystemer](#)

Opdateret: 06.05.15

Standardvilkår for retsinformationssystemer

Det følger af persondatalovens § 9, stk. 3, at Datatilsynet kan fastsætte nærmere vilkår for behandlingen af personoplysninger i forbindelse med førelsen af retsinformationssystemer.

For så vidt angår private retsinformationssystemer følger det endvidere af persondataloven § 50, stk. 5, at Datatilsynet i forbindelse med meddelelse af tilladelse efter § 50, stk. 1, nr. 5, kan fastsætte nærmere vilkår at beskytte af de registreredes privatliv.

Datatilsynet har i 2001 fastsat standardvilkår for offentliggørelse af afgørelser og domme. De to sager, der har ført til fastsættelsen af standardvilkårene, er beskrevet i Datatilsynets årsberetning for 2001 s. 43ff. Årsberetningen kan ses under punktet "Publikationer".

Vilkår for offentliggørelse af afgørelser

Datatilsynet har fastsat følgende vilkår for offentliggørelse af myndigheders afgørelser i retsinformationssystemer:

1. I afgørelser, som indeholder fortrolige oplysninger eller oplysninger om enkeltpersoners rent private forhold, skal de pågældende oplysninger anonymiseres i overensstemmelse med vilkår nr. 2, jf. dog vilkår nr. 3, før videregivelse må finde sted.

I alle afgørelser skal det endvidere sikres, at der ikke videregives oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningen angår.

2. En eventuel anonymisering består i udeladelse af personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger vedrørende personer. I stedet for de udeladte oplysninger kan indsættes neutrale betegnelser. Personnumres løbenummer udelades.

Se yderligere om krav til anonymisering [her](#)

3. Afgørelserne kan forsynes med sagens journalnummer, sagslistennummer m.v.
4. Hvis en afgørelse har været behandlet af en højere instans, skal dette samt udfaldet heraf fremgå af gengivelsen af sagen.
5. Det skal kontrolleres, at der ikke er fejl i gengivelsen af afgørelserne. Fejl og lignende skal rettes eller slettes.
6. Der skal etableres sikkerhed for, at der i retsinformationssystemet ikke kan tilføjes data eller manipuleres med data.

7. Datatilsynets udtalelse skal indhentes inden iværksættelse af ændringer i førelsen af retsinformationssystemet.

Ændringer af mindre væsentlig betydning skal dog alene anmeldes til Datatilsynet.

Anmeldelsen kan ske efterfølgende, dog senest 4 uger efter ændringen er iværksat.

Datatilsynet har givet følgende uddybende bemærkninger til vilkårene.

Om begrebet "fortrolige" (ad vilkår nr. 1 og 2)

Fortrolige oplysninger som nævnt i vilkår nr. 1 er oplysninger, som ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller som det i øvrigt er nødvendigt at hemmeligholde for at varetage væsentlige hensyn til offentlige eller private interesser.

Følsomme oplysninger som nævnt i persondatalovens § 7, stk. 1, dvs. oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, vil være omfattet af begrebet "fortrolige oplysninger".

Endvidere vil oplysninger om strafbare forhold, og væsentlige sociale problemer og andre rent private forhold, som omtalt i persondatalovens § 8, stk. 1, være fortrolige.

Herudover vil oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold efter omstændighederne kunne være fortrolige.

Endvidere skal det bemærkes, at det blotte forhold, at en borger overhovedet har en sag hos en bestemt myndighed eller har en sag af en bestemt kategori, i sig selv kan være en fortrolig oplysning.

Oplysninger som i forvejen er offentligt tilgængelige, vil som hovedregel ikke være at betragte som fortrolige oplysninger.

Private foreningers eller selskabers interesse i at beskytte oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende vil også kunne føre til, at oplysningerne må anses for at være fortrolige, når væsentlige hensyn til de pågældendes økonomiske interesser tilsiger, at oplysningerne ikke videregives til uvedkommende.

Med hensyn til begrebet "fortrolig" henvises i øvrigt til punkt 2.1.3. "Behandlinger, der er undtaget fra anmeldelse" i Datatilsynets vejledning nr. 125 af 10. juli 2000 om anmeldelse i henhold til kapitel 12 i lov om behandling af personoplysninger.

Læs Datatilsynets vejledning på Retsinformation.dk.

Vilkår for offentliggørelse af domme

Datatilsynet har fastsat følgende vilkår for offentliggørelse af domme:

1. Der skal ske anonymisering i følgende sager:
 - a) I offentligt anlagte straffesager, bortset fra straffesager vedrørende overtrædelse af markedsføringsloven og lignende, skal der ske anonymisering. Der skal ske tilsvarende anonymisering i sager om erstatning i anledning af strafferetlig forfølgning omfattet af 1. punktum.

- b) I ægteskabssager, det vil sige sager om separation, skilsmisse, forældremyndighed og bidragspligt og i faderskabssager, skal der ske anonymisering.
- c) I sager om administrativ frihedsberøvelse, i sager om prøvelse af tvangsindlæggelse på en psykiatrisk hospitalsafdeling, i værgemålssager og i sager om anbringelse af børn uden for hjemmet i henhold til bistandsloven skal der ske anonymisering.
- d) I fogedsager og sager om konkurser mod enkeltpersoner, i gældssaneringsager og ved ægtefællers fællesbodelinger skal der ske anonymisering.
- e) I skattesager, hvor sagen indeholder oplysninger om den pågældendes samlede indtægts- eller formueforhold, skal der ske anonymisering.
- f) I ansættelsessager om bortvisning, hvor bortvisningen eksempelvis er begrundet i strafbare eller lignende forhold hos den ansatte, der er egnet til at nedsætte den ansattes almindelige omdømme, skal der ske anonymisering.
- g) I erstatningssager, hvor der findes beskrivelse af hændelsesforløb, der indeholder oplysninger om helbredsforhold eller andre personlige forhold, f.eks. diagnoser og sygdomsprogner, skal der ske anonymisering.
- h) I lejesager, der angår sager om ophævelse af lejemål på grund af lejerens adfærd eller lignende, skal der ske anonymisering.
- i) I alle sager, der indeholder i øvrigt fortrolige oplysninger, skal der ske anonymisering, hvis særlige forhold tilsiger dette. Dette gælder dog ikke i sager, hvor en fagforening er repræsentant (mandatar) for et medlem af fagforeningen.
- j) Anonymiseringskravet gælder for såvel sagsparter som vidner og andre bipersoner, jf. dog 2. og 3. punktum. I de sager, der er nævnt i litra a-c, gælder anonymiseringskravet ikke polititjenestemænd, der har optaget rapport, sagkyndige og lignende vidner. I de sager, der er nævnt i litra d-i, gælder anonymiseringskravet kun for vidner og andre bipersoner, såfremt særlige hensyn til en af sagens parter, vidnet selv eller andre bipersoner undtagelsesvis tilsiger dette.
2. En eventuel anonymisering består i udeladelse af personnavne, præcise adresseangivelser samt eventuelt andre identifikationsoplysninger vedrørende personer. I stedet for de udeladte oplysninger kan der indsættes neutrale betegnelser. Personnumres løbenummer udelades.
- Se yderligere om krav til anonymisering [her](#)
3. Domme kan forsynes med sagens journalnummer, sagslistennummer m.v.

4. Der skal etableres sikkerhed for, at der ikke kan tilføjes eller manipuleres med data, der befinder sig i retsinformationssystemerne.
5. Hvis en dom har været behandlet af en højere instans, skal dette samt udfaldet heraf fremgå af gengivelsen af sagen.
6. Det skal kontrolleres, at der ikke er fejl i gengivelsen af dommene. Fejl og lignende skal rettes eller slettes.
7. Datatilsynet skal have underretning om væsentlige ændringer i eller ophør af førelsen af retsinformationssystemerne.

Vilkårene er supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Reglerne i persondataloven finder derfor anvendelse i det omfang, at der er tale om forhold, som ikke er reguleret i de ovenstående vilkår.

Persondataloven finder endvidere anvendelse også på den behandling, som finder sted forud for offentliggørelsen. Persondataloven finder f.eks. anvendelse på elektronisk behandling, der sker ved redigering og anonymisering af dommene, og hvor persondatalovens sikkerhedsregler, herunder § 41, skal iagttages.

Persondataloven – med undtagelse af nogle få områder – omfatter kun behandling af personoplysninger. Vilkårene for retsinformationssystemer er derfor kun gældende for behandling af personoplysninger i et retsinformationssystem. Behandlinger af oplysninger om virksomheder m.v. i et retsinformationssystem vil dog skulle ske i overensstemmelse med de almindelige regler om tavshedspligt.

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