DATATILSYNET

JUSTITSMINISTERIET

# Vejledning om adfærdskodekser og certificeringsordninger

Januar 2018

Januar 2018

# Indhold

# 1.0 Forord

Når databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018 vil der være mange regler, som alle dataansvarlige og databehandlere (store som små) skal kunne overholde samt kunne dokumentere, at de overholder.

For nogle virksomheder kan det synes uoverskueligt at skulle sætte sig ind i og forstå databeskyttelsesforordningens mange forskelligartede regler. Det vil nok især være tilfældet for mikro, små og mellemstore virksomheder, hvor behandling af personoplysninger ikke er virksomhedens "kerneydelse". Ikke desto mindre vil de fleste små virksomheder, f.eks. tømrervirksomheder, frisører og købmænd, i et eller andet omfang behandle personoplysninger, herunder oplysninger om virksomhedens ansatte og virksomhedens kunder.

Herudover kan det skyldes, at mange små virksomheder, i modsætning til større virksomheder, ikke har en juridisk afdeling, der kan hjælpe med overholdelsen, ligesom de måske ikke har ressourcerne til at indhente ekstern juridisk rådgivning.

I databeskyttelsesforordningens kapitel 4, afdeling 5, har man, bl.a. i erkendelse af ovennævnte, indsat regler om adfærdskodekser og certificeringsordninger. Ønsket er, at disse ordninger skal kunne hjælpe dataansvarlige og databehandlere til at overholde databeskyttelsesforordningen, herunder f.eks. i forhold til behandlingsaktiviteter, der er særligt kendetegnende for en specifik branche eller lignende.

Udarbejdelse af bl.a. adfærdskodekser vil derfor kunne være et nyttigt redskab for især mikro, små og mellemstore virksomheder til at hjælpe med at sikre overholdelsen af forordningens regler.

Reglerne om adfærdskodekser og certificeringsordninger er dog ikke udelukkende tiltænkt at skulle hjælpe mikro, små og mellemstore virksomheder med deres overholdelse af forordningen. Store virksomheder og offentlige myndigheder mv., vil således også kunne benytte sig af ordningerne.
I denne vejledning får man bl.a. en introduktion til, 1) hvad adfærdskodekser og certificeringsordninger er, 2) hvem, der kan udarbejde en adfærdskodeks eller en certificeringsordning, 3) hvad man kan bruge ordningerne til, og 4) hvordan en adfærdskodeks eller en certificeringsordning kan blive godkendt.

Denne vejledning er baseret på reglerne i databeskyttelsesforordningens kapitel IV, afdeling 5 (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger), og som bl.a. er beskrevet i betænkning nr. 1565/2017 om databeskyttelsesforordningen i kapitel 5.22.-5.25.

# 2.0 Adfærdskodekser

## 2.1 Hvad er en adfærdskodeks?

I databeskyttelsesforordningens forstand er en adfærdskodeks et sæt retningslinjer, som skal bidrage til at sikre, at de virksomheder, der har tilsluttet sig kodeksen, anvender reglerne i databeskyttelsesforordningen korrekt.

Retningslinjerne i en kodeks skal bidrage til at sikre en korrekt anvendelse af forordningens regler ved at angive hvordan man i specifikke typetilfælde skal håndtere behandlingen af personoplysninger. Det kan f.eks. være ved at fastlægge nogle procedurer, som skal følges, for en specifik type behandling af personoplysninger.

En adfærdskodeks kan således benyttes inden for en specifik kategori af databehandlingsaktiviteter – som er sædvanlige for f.eks. en veldefineret gruppe af virksomheder.

Overholdelse af en kodeks kan således endvidere anvendes som et element til at påvise, at den dataansvarlige eller databehandleren lever op til sine forpligtelser efter forordningen.

Det er vigtigt at være opmærksom på, at tilslutning til og overholdelse af en godkendt adfærdskodeks, ikke i sig selv er et bevis på overholdelse af databeskyttelsesforordningen, heller ikke for så vidt angår de artikler i forordningen, som kodeksen måtte forholde sig til. Overholdelse af en adfærdskodeks kan dermed heller ikke fritage en dataansvarlig eller en databehandler for ansvar, men det må antages, at overholdelse af en godkendt adfærdskodeks har betydning for, om man kan ifalde et strafansvar for at overtræde reglerne i forordningen, eller er formildende for så vidt angår et eventuelt strafansvar, jf. mere herom i afsnit 2.3.

## 2.2 Hvem kan udarbejde en adfærdskodeks?

En adfærdskodeks kan ifølge databeskyttelsesforordningen udarbejdes af sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere.

De oplagte sammenslutninger er, der kan tænkes at tage initiativ til at udarbejde en adfærdskodeks, er bl.a. brancheorganisationer og –foreninger. Man kunne dog også forestille sig, at f.eks. KL eller Danske Regioner kunne have en interesse i – i forhold til specifikke behandlingsaktiviteter – at udarbejde adfærdskodeks, der retter sig mod kommunerne eller regionerne.

Når der peges på brancheorganisationer og -foreninger, så skyldes dette, at disse typisk har et indgående kendskab til, hvilke behandlinger af personoplysninger der er sædvanlige inden for de brancher, som organisationen eller foreningen repræsenterer.

Brancheorganisationer eller foreninger ved således også, på hvilke områder deres medlemmer er mest udfordrede i forhold til at overholde forordningen, og hvor de derfor kan have gavn af en adfærdskodeks, der specificerer anvendelsen af forordningen i forhold til disse områder.

**Eksempel 1 – behandling af HR-oplysninger**

Arbejdsgiverorganisationen A, der repræsenterer en lang række ejere af små servicevirksomheder i Danmark, bliver opmærksom på, at organisationens medlemmer har svært ved at forstå behandlingsreglerne i databeskyttelsesforordningens kapitel II.

Langt de fleste af A's medlemmer behandler kun personoplysninger om deres ansatte til HR-formål, og de har typisk under 5 ansatte.

A beslutter på baggrund af ovenstående at tage initiativ til at udarbejde en adfærdskodeks, der opstiller specifikke regler for behandling af HR-oplysninger i servicevirksomheder med under 5 ansatte, herunder regler om indsamling af oplysninger samt regler om sletning mv.

Efter at A's udkast til adfærdskodeks er blevet godkendt af Datatilsynet, vil A's medlemmer – på frivillig basis – kunne tilslutte sig adfærdskodeksen og dermed få hjælp til overholdelsen af de regler i databeskyttelsesforordningen, der især er relevante for medlemmerne.

Som det fremgår af eksempel 1, er det frivilligt, om man ønsker at tilslutte sig en adfærdskodeks. Man kan således sagtens overholde databeskyttelsesforordningen uden at tilslutte sig en adfærdskodeks.

## 2.3 Hvad kan en adfærdskodeks benyttes til?

Ifølge databeskyttelsesforordningens artikel 40, stk. 2, litra a-k, kunne en adfærdskodeks tænkes at specificere anvendelsen af følgende række eksempler på forordningens regler:

*a) rimelig og gennemsigtig behandling*
*b) de legitime interesser, som forfølges af den dataansvarlige i specifikke sammenhænge*
*c) indsamlingen af personoplysninger*
*d) pseudonymiseringen af personoplysninger*
*e) informationen, der gives til offentligheden og til registrerede*
*f) udøvelsen af registreredes rettigheder*
*g) informationen, der gives til børn, og beskyttelsen af børn og den måde, hvorpå samtykket fra indehavere af forældremyndighed over børn skal indhentes*
*h) foranstaltningerne og procedurerne omhandlet i artikel 24 og 25 og foranstaltningerne til at sikre behandlingssikkerhed som omhandlet i artikel 32*
*i) anmeldelse af brud på persondatasikkerheden til tilsynsmyndighederne og underretningen af de registrerede om sådanne brud på persondatasikkerheden*
*j) overførslen af personoplysninger til tredjelande eller internationale organisationer, eller*
*k) udenretslige procedurer og andre procedurer for bilæggelse af tvister mellem dataansvarlige og registrerede vedrørende behandling, uden at det berører registreredes rettigheder i henhold til artikel 77 og 79.*

Hvis man tager udgangspunkt i ovennævnte liste kunne en adfærdskodeks således f.eks. gå ud på at specificere databeskyttelsesforordningens regler i forhold til de registreredes rettigheder.

**Eksempel 2 – oplysningspligt**

Brancheorganisationen B repræsenterer bl.a. en række mindre virksomheder, der beskæftiger sig med rekruttering.

I forbindelse med udøvelsen af deres rekrutteringsvirksomhed indsamler B's medlemmer ofte oplysninger om de personer, som virksomheden forsøger at rekruttere (de registrerede) fra andre end de pågældende personer selv. Virksomhederne skal derfor – i overensstemmelse med databeskyttelsesforordningens regler om oplysningspligt (her artikel 14) – give de registrerede en række oplysninger, herunder oplysninger om, hvem virksomheden er, og med hvilke formål virksomheden behandler oplysninger.

Da det erfaringsmæssigt er svært for B's medlemmer at overholde databeskyttelsesforordningens regler om oplysningspligt, vælger B at udarbejde en adfærdskodeks, som kan lette B's medlemmers overholdelse af oplysningspligten. Kodeksen indeholder bl.a. en skabelon, som B's medlemmer kan benytte, når de opfylder deres oplysningspligt over for de registrerede, men kodeksen indeholder også en række regler, der kan hjælpe medlemmerne til at huske at opfylde deres oplysningspligt.

En adfærdskodeks kunne ligeledes gå ud på at specificere databeskyttelsesforordningens regler om behandlingssikkerhed.

**Eksempel 3 – pseudonymisering**

Brancheorganisationen C repræsenterer en række mindre forskningsvirksomheder, der – på samme måde – behandler store mængder følsomme oplysninger (helbredsoplysninger) om patienter til brug for udvikling af ny medicin mv.

For at hjælpe sine medlemmer til at overholde databeskyttelsesforordningens regler om behandlingssikkerhed (f.eks. sikre at oplysninger ikke kommer til uvedkommendes kendskab), tager C initiativ til at udarbejde en adfærdskodeks om pseudonymisering[1] af de patientoplysninger, som C's medlemmer benytter i deres forskning.

Adfærdskodeksen indeholder bl.a. en procedure, der skal sikre at pseudonymisering sker i overensstemmelse med anerkendte standarder og tilpasset til den pågældende databehandling, ligesom kodeksen indeholder regler for, hvordan pseudonymisering skal udføres i praksis, hvornår pseudonymisering skal finde sted samt regler for, hvordan virksomheden bør indrette arbejdsprocesserne, så færrest muligt kommer til at arbejde med ikke-pseudonymiserede oplysninger.

[1] Pseudonymisering defineres i databeskyttelsesforordningen som: "Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person."

Herudover nævnes det i en række bestemmelser i databeskyttelsesforordningen, at dataansvarlige og databehandlere bl.a. kan bruge overholdelse af en godkendt adfærdskodeks som et element til at påvise overholdelsen af krav i forordningen, ligesom overholdelse af godkendte adfærdskodekser kan inddrages ved vurderingen af, om der kan idømmes en straf for manglende overholdelse af forordningen, og i givet fald ved vurderingen af udmålingen af straffen, f.eks. størrelsen af en bøde.

Nedenfor gennemgås de bestemmelser i databeskyttelsesforordningen, hvor overholdelse af en godkendt adfærdskodeks kan tillægges betydning.

### 2.3.1 Den dataansvarliges ansvar (artikel 24)

Den dataansvarlige er ansvarlig for at overholde reglerne i databeskyttelsesforordningen og skal ifølge forordningens artikel 24 kunne påvise, at man overholder sine forpligtelser efter forordningen.

Overholdelse af en godkendt adfærdskodeks kan bruges som et element til at påvise, at den dataansvarlige lever op til sine forpligtelser efter forordningen.

**Eksempel 4 – en dataansvarlig har tilsluttet sig en godkendt adfærdskodeks vedrørende håndtering af brud på persondatasikkerheden**

En virksomhed V har tilsluttet sig en godkendt adfærdskodeks, der opstiller retningslinjer for virksomhedens håndtering af brud på persondatasikkerheden.

Adfærdskodeksen indeholder bl.a. klare retningslinjer for, hvordan virksomheden skal rydde op efter et eventuelt brud på persondatasikkerheden, og hvordan virksomheden skal søge at begrænse skadevirkningerne af bruddet. Herudover indeholder adfærdskodeksen klare retningslinjer for anmeldelse af brud på persondatasikkerheden til de relevante tilsynsmyndigheder samt retningslinjer for, hvornår og hvordan de berørte registrerede skal notificeres om bruddet.

Når virksomheden V har tilsluttet sig en adfærdskodeks, der opstiller klare retningslinjer for V's håndtering af eventuelle brud på persondatasikkerheden, vil V kunne benytte sin tilslutning til adfærdskodeksen som et element til at påvise, at V lever op til de forpligtelser, der – efter forordningen – påhviler V (som dataansvarlig), hvis denne konstaterer et brud på persondatasikkerheden.

### 2.3.2 Databehandlers påvisning af fornødne garantier (artikel 28)

Det fremgår af databeskyttelsesforordningens artikel 28, stk. 1, at en dataansvarlig kun må benytte databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i forordningen og sikrer beskyttelse af de registreredes rettigheder.

På samme måde fremgår det af artikel 28, stk. 4, at en databehandler kun må benytte en underdatabehandler, hvis denne kan stille de fornødne garantier.

Overholdelse af en godkendt adfærdskodeks kan bruges som et element til at påvise, at databehandleren stiller fornødne garantier. På samme måde kan overholdelse af en godkendt ad-

færdskodeks bruges som et element til at påvise, at en underdatabehandler stiller fornødne garantier.

**Eksempel 5 – en databehandler har tilsluttet sig en godkendt adfærdskodeks vedrørende behandlingssikkerhed i cloud-løsninger**

En virksomhed X har specialiseret sig i at udbyde skræddersyede cloud-løsninger til sine kunder inden for en given branche Y, hvor X (som databehandler) opbevarer sine kunders personoplysninger i "skyen".

Da virksomheden X går meget op i at sikre sine kunders oplysninger bedst muligt, har X valgt at tilslutte sig en godkendt adfærdskodeks vedrørende behandlingssikkerhed i cloud-løsninger i branchen Y. Adfærdskodeksen indeholder bl.a. klare retningslinjer for, hvordan cloud-udbydere skal beskytte sine oplysninger mod, at disse kan tilgås af uvedkommende, ligesom kodeksen indeholder retningslinjer for, hvordan cloud-udbydere løbende skal teste effektiviteten af deres tiltag, samt retningslinjer for løbende ekstern kontrol og cloud-udbyderens opfølgning derpå. Endelig indeholder kodeksen retningslinjer for, hvordan cloud-udbydere hurtigst muligt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

Når virksomheden X har tilsluttet ovennævnte adfærdskodeks, vil X kunne bruge denne tilslutning til at påvise over for potentielle kunder (dataansvarlige), at X – i sin løsning – kan stille de fornødne garantier i forhold til datasikkerheden i branchen Y.

### 2.3.3 Behandlingssikkerhed (artikel 32)

Ifølge databeskyttelsesforordningen skal den dataansvarlige og databehandleren gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til de risici, der er ved den pågældende behandling af personoplysninger.

Af databeskyttelsesforordningens artikel 32, stk. 3, fremgår det, at overholdelse af en godkendt adfærdskodeks, kan bruges som et element til at påvise den dataansvarliges eller databehandlerens overholdelse af kravene til behandlingssikkerhed.

For eksempler vedrørende behandlingssikkerhed kan der henvises til eksempel 3 og 5 ovenfor.

### 2.3.4 Konsekvensanalyse vedrørende databeskyttelse (artikel 35)

Efter databeskyttelsesforordningens artikel 35 skal en dataansvarlig foretage en konsekvensanalyse, hvis en type behandling – navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål – sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

En konsekvensanalyse er navnlig påkrævet, hvis 1) der sker en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, 2) der behandles følsomme oplysninger i stort omfang, eller 3) der sker systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Overholdelse af en godkendt adfærdskodeks skal inddrages behørigt ved vurderingen af konsekvenserne af de databehandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse.

**Eksempel 6 – et privathospital køber et nyt IT-system**

Privathospitalet H ønsker at købe et nyt IT-system, hvori H bl.a. vil registrere og behandle alle oplysninger om sine patienter.

I og med at H behandler følsomme personoplysninger (helbredsoplysninger) i stort omfang, vil H skulle lave en konsekvensanalyse, inden H tager det nye IT-system i brug.

Privathospitalet H har ved en tidligere lejlighed tilsluttet sig en godkendt adfærdskodeks vedrørende behandlingssikkerhed (for så vidt angår personoplysninger) på privathospitaler. Adfærdskodeksen indeholder bl.a. klare retningslinjer for pseudonymisering og kryptering af personoplysninger samt klare retningslinjer for privathospitalers beskyttelse af personoplysninger ud mod internettet (firewalls mv.).

Når H skal foretage sin konsekvensanalyse, vil H kunne inddrage sin efterlevelse af den godkendte adfærdskodeks vedrørende behandlingssikkerhed på privathospitaler, når H skal vurdere risikoen ved at overgå til det nye IT-system. Adfærdskodeksen kan således bidrage til at mindske risikoen ved at tage det nye IT-system i brug.

Det bemærkes, at der i artikel 35, stk. 8, alene henvises til godkendte adfærdskodekser. Dette er således et af blot to steder, hvor der ikke både henvises til godkendte adfærdskodekser og godkendte certificeringsordninger. Se mere herom i afsnit 3.4.2. (databeskyttelse gennem design og standardindstillinger).

### 2.3.5 Overførsler til tredjelande omfattet af fornødne garantier (artikel 46)

Hvis man som dataansvarlig eller databehandler ønsker at overføre personoplysninger til et tredjeland[2], skal man – ud over en videregivelseshjemmel – også have et såkaldt overførselsgrundlag i forordningens kapitel V. Et overførselsgrundlag kan f.eks. være fornødne garantier i form af Kommissionens standardkontrakter, eller at det pågældende tredjeland er godkendt af Kommissionen som et sikkert tredjeland.

Det fremgår af databeskyttelsesforordningens artikel 46, stk. 2, litra e, at de fornødne garantier i forbindelse med overførsel til et usikkert tredjeland kan sikres gennem en godkendt adfærdskodeks. Det er dog en betingelse for at anse en adfærdskodeks for at sikre fornødne garantier, at der er bindende tilsagn, som kan håndhæves, fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier, herunder vedrørende de registreredes rettigheder.

[2] Lande der ikke er medlem af EU eller EØS.

**Eksempel 7 – databehandleren i Indien**

En dansk virksomhed A ønsker at benytte en databehandler D i Indien til at drifte sine IT-systemer.

Da Indien er et usikkert tredjeland, skal A have et overførselsgrundlag i forordningens kapitel V, inden der kan overføres personoplysninger til D i Indien.

Et overførselsgrundlag kan i den forbindelse være, hvis D har tilsluttet sig en godkendt og bindende adfærdskodeks vedrørende overførsel af personoplysninger til databehandlere i tredjelande, der bl.a. indeholder klare retningslinjer om behandlingssikkerhed, håndtering af brud på persondatasikkerheden, brug af underdatabehandlere, uddannelse af medarbejdere og samarbejde med de relevante datatilsyn mv.

Det bemærkes, at D's tilslutning til et godkendt adfærdskodeks ikke fritager A for at indgå en databehandleraftale med D, jf. databeskyttelsesforordningens artikel 28.

#### 2.3.6 Administrative bøder (artikel 83)

Af databeskyttelsesforordningens artikel 83, stk. 2, litra j, fremgår det, at der skal tages behørigt hensyn til, om en godkendt adfærdskodeks er overholdt, når det skal afgøres, om der skal pålægges en administrativ bøde, og når det skal afgøres, hvor stor en eventuel administrativ bøde skal være.

Efterlevelse af en godkendt adfærdskodeks i forbindelse med en given behandling af personoplysninger vil således f.eks. kunne inddrages ved vurderingen af, om der er begået noget strafbart i forbindelse med manglende overholdelse af forordningen, og dermed om der skal pålægges en bøde.

På samme måde vil efterlevelse af en kodeks f.eks. kunne inddrages som en formildende omstændighed ved fastsættelsen af en administrativ bødes størrelse.

Som nævnt ovenfor i afsnit 2.1. er det vigtigt at være opmærksom på, at tilslutning til og overholdelse af en godkendt adfærdskodeks, ikke i sig selv er et bevis på overholdelse af databeskyttelsesforordningen, heller ikke for så vidt angår de regler i forordningen, som kodeksen måtte specificere anvendelsen af. Overholdelse af en adfærdskodeks kan dermed heller ikke i sig selv fritage en dataansvarlig eller databehandler for ansvar.

## 2.4 Hvordan udarbejder man en adfærdskodeks – indholdsmæssige minimumskrav?

Som nævnt ovenfor i afsnit 2.2 kan adfærdskodekser ifølge forordningen udarbejdes af sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere.

Som nævnt under samme pkt. lægges der med databeskyttelsesforordningen op til, at det typisk vil være brancheorganisationer eller lignende, der tager initiativ til at udarbejde en adfærdskodeks.

Inden en adfærdskodeks kan benyttes til at specificere anvendelsen af databeskyttelsesforordningen, skal den være godkendt af Datatilsynet.

For at en adfærdskodeks kan blive godkendt af Datatilsynet, vil den skulle leve op til nogle indholdsmæssige minimumskrav, der samlet set skal sikre, at kodeksen sikrer fornødne garantier. De indholdsmæssige minimumskrav vil kunne udvikle sig over tid, da det i et vist omfang vil være nødvendigt at koordinere disse med de øvrige datatilsyn i EU.

Datatilsynet kan dog allerede nu pege på, at følgende punkter – efter Datatilsynets opfattelse – som minimum skal berøres i en adfærdskodeks, hvis denne skal indeholde fornødne garantier:

- En adfærdskodeks skal have fokus på en veldefineret kategori af dataansvarlige eller databehandlere. Kodeksen skal således klart angive, hvilke typer organisationer eller sektorer, som kodeksen tilsigter at finde anvendelse på.

- En adfærdskodeks skal være rettet mod konkrete og veldefinerede behandlinger, som er typiske for ovennævnte kategorier af dataansvarlige og databehandlere.

- En adfærdskodeks skal forberedes omhyggeligt, og der bør i den forbindelse ske høring af relevante interessenter, herunder i muligt omfang de registrerede eller deres repræsentanter, f.eks. Forbrugerrådet eller lignende.

- En adfærdskodeks skal indeholde retningslinjer rettet mod konkrete behandlingssituationer, der er relevante for den branche eller lignende, som kodeksen er rettet mod. Retningslinjerne kan være relateret til det daglige arbejde og de eventuelle usædvanlige arbejdssituationer, som behandlingsaktiviteterne måtte indgå i samt fastsætte specifikke rammer for, hvordan man kan begrænse de risici, som er blevet identificeret i forhold til behandlingsaktiviteterne.

- En adfærdskodeks skal indeholde konkrete retningslinjer, som hjælper til at sikre, at de tilsluttede dataansvarlige eller databehandlere overholder forordningen, når de følger adfærdskodeksens retningslinjer. Kodeksen skal således i tilstrækkelig grad fokusere på specifikke databeskyttelsesspørgsmål og –problemer, der findes i den organisation eller sektor, som kodeksen finder anvendelse på, samt anvise tilstrækkelig klare løsninger på disse spørgsmål og problemer. I den forbindelse bør relevante kompetencer, såsom faglige, juridiske og it-sikkerhedsmæssige, inddrages i udarbejdelsen.

- En adfærdskodeks skal indeholde mekanismer, som gør et kontrolorgan i stand til at foretage en kontrol af, om den dataansvarlige eller databehandleren, der har tilsluttet sig et adfærdskodeks rent faktisk overholder reglerne i kodeksen. Disse kontrolmekanismer kan både være af teknisk og organisatorisk karakter.

- I forhold til enhver adfærdskodeks skal der være en central instans (f.eks. en brancheorganisation), der sørger for, at kodeksen løbende bliver opdateret og tilpasset, f.eks. i forhold til praksis fra Datatilsynet mv.

- En adfærdskodeks bør (i hvert fald hvis man ønsker at påberåbe sig kodeksen i forhold til efterlevelse af forordningen) indeholde en kontrolmekanisme, der sætter et kontrolorgan i stand til at kontrollere overholdelsen af kodeksen. Kontrolorganet skal være akkrediteret af Datatilsynet, jf. databeskyttelsesforordningens artikel 41. Et organ kan akkrediteres til at kontrollere overholdelsen af en adfærdskodeks, hvis dette organ har: **1)** påvist sin uafhængighed og ekspertise for så vidt angå kodeksens genstand, **2)** fastlagt procedurer, der gør det muligt at vurdere tilsluttede dataansvarlige eller databehandleres egnethed til at anvende kodeksen, kontrollere de tilsluttedes overholde af kodeksen, og regelmæssigt vurdere kodeksens virkemåde, **3)** fastlagt procedurer og ordninger for behandling af klager over overtrædelser af kodeksen mv. samt gøre disse procedurer og ordninger gennemsigtige for offentligheden, og **4)** påvist at organets opgaver og pligter ikke fører til en interessekonflikt.

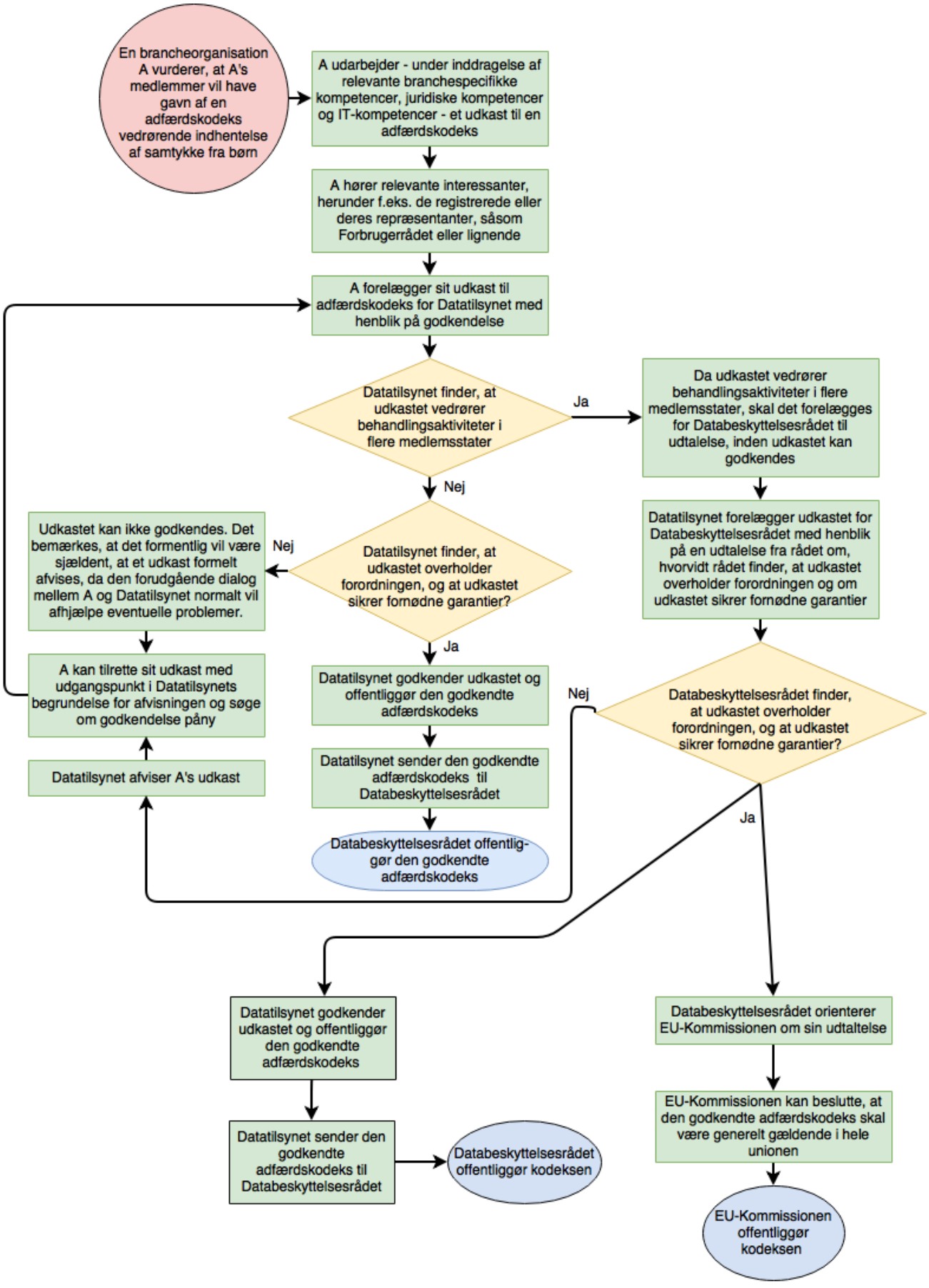
- En adfærdskodeks kan med fordel indeholde en bestemmelse med en ordlyd, der indholdsmæssigt minder om det følgende: "Overholdelse af denne adfærdskodeks fritager ikke de dataansvarlige eller databehandlere, der tilslutter sig kodeksen fra at overholde databeskyttelsesforordningen, ligesom overholdelse af denne kodeks på ingen måde berører Datatilsynets beføjelser eller opgaver, herunder i form af kontrol med overholdelsen af bestemmelser i denne kodeks."

Det bemærkes, at forordningens regler om kontrol af godkendte adfærdskodekser ikke gælder for offentlige myndigheder, hvorfor en adfærdskodeks udarbejdet af f.eks. KL med henblik på kommunernes behandlinger ikke vil skulle indeholde et kontrolorgan. Kodeksen skal dog indeholde en kontrolmekanisme, som vil gøre Datatilsynet i stand til at føre kontrol med, at kodeksen bliver overholdt.

Endvidere skal det bemærkes, at det ikke har nogen betydning for så vidt angår Datatilsynets kompetencer, at en adfærdskodeks har et indbygget kontrolorgan. Tilsynet vil således kunne føre tilsyn med behandlingsaktiviteter, der foregår i tilknytning til en adfærdskodeks, selvom overholdelsen af denne også kontrolleres af et akkrediteret kontrolorgan.

## 2.5 Hvordan er processen i forbindelse med udarbejdelse af og godkendelse af en adfærdskodeks?

I Figur 1 er det forsøgt illustreret, hvordan forløbet kan se ud i forbindelse med udarbejdelse af og godkendelse af en adfærdskodeks.


En brancheorganisation A vurderer, at A's medlemmer vil have gavn af en adfærdskodeks vedrørende indhentelse af samtykke fra børn
A udarbejder - under inddragelse af relevante branchespecifikke kompetencer, juridiske kompetencer og IT-kompetencer - et udkast til en adfærdskodeks
A hører relevante interessanter, herunder f.eks. de registrerede eller deres repræsentanter, såsom Forbrugerrådet eller lignende
A forelægger sit udkast til adfærdskodeks for Datatilsynet med henblik på godkendelse
Datatilsynet finder, at udkastet vedrører behandlingsaktiviteter i flere medlemsstater
Ja
Da udkastet vedrører behandlingsaktiviteter i flere medlemsstater, skal det forelægges for Databeskyttelsesrådet til udtalelse, inden udkastet kan godkendes
Nej
Datatilsynet forelægger udkastet for Databeskyttelsesrådet med henblik på en udtalelse fra rådet om, hvorvidt rådet finder, at udkastet overholder forordningen og om udkastet sikrer fornødne garantier
Udkastet kan ikke godkendes. Det bemærkes, at det formentlig vil være sjældent, at et udkast formelt afvises, da den forudgående dialog mellem A og Datatilsynet normalt vil afhjælpe eventuelle problemer.
Nej
Datatilsynet finder, at udkastet overholder forordningen, og at udkastet sikrer fornødne garantier?
Ja
A kan tilrette sit udkast med udgangspunkt i Datatilsynets begrundelse for afvisningen og søge om godkendelse påny
Datatilsynet godkender udkastet og offentliggør den godkendte adfærdskodeks
Nej
Databeskyttelsesrådet finder, at udkastet overholder forordningen, og at udkastet sikrer fornødne garantier?
Datatilsynet afviser A's udkast
Datatilsynet sender den godkendte adfærdskodeks til Databeskyttelsesrådet
Databeskyttelsesrådet offentlig-gør den godkendte adfærdskodeks
Ja
Datatilsynet godkender udkastet og offentliggør den godkendte adfærdskodeks
Databeskyttelsesrådet orienterer EU-Kommissionen om sin udtaltelse
Datatilsynet sender den godkendte adfærdskodeks til Databeskyttelsesrådet
Databeskyttelsesrådet offentliggør kodeksen
EU-Kommissionen kan beslutte, at den godkendte adfærdskodeks skal være generelt gældende i hele unionen
EU-Kommissionen offentliggør kodeksen

Figur 1

# 3.0 Certificeringsordninger

## 3.1 Hvad er en certificeringsordning i databeskyttelsesforordningens forstand (artikel 42)?

En certificeringsordning (certificeringsmekanisme) er en ordning, hvor en kvalificeret tredjepart (et certificeringsorgan) attesterer for, at en virksomhed eller en myndighed – der har anmodet om at blive certificeret – lever op til et foruddefineret sæt af kriterier eller krav.

Når der er tale om en certificeringsordning i databeskyttelsesforordningens forstand, er det vigtigt at være opmærksom på, at ovennævnte krav og kriterier relaterer sig til behandlingsaktiviteter. En certificering kan således f.eks. vedrøre en virksomheds eller en myndigheds indsamling, registrering, pseudonymisering eller sletning af personoplysninger. Derimod kan en certificering i forordningens forstand ikke vedrøre selve det it-system, hvori behandlingsaktiviteterne foregår.

På samme måde som med adfærdskodekser er tilslutning til en godkendt certificeringsordning tiltænkt at være en måde, hvorpå en dataansvarlig virksomhed eller myndighed eller en databehandler kan få hjælp til at sikre, at deres behandlingsaktiviteter overholder forordningen, ligesom en tilslutning kan hjælpe dem til at påvise, at de overholder forordningen. Som det er tilfældet med adfærdskodekser, kan man dog sagtens overholde databeskyttelsesforordningen uden at tilslutte sig en godkendt certificeringsordning. Tilslutning til og overholdelse af en godkendt certificeringsordning er således ikke i sig selv et bevis på overholdelse af forordningen, heller ikke for så vidt angår de artikler i forordningen, som certificeringsordningen måtte specificere anvendelsen af forordningen i forhold til.

Hvis en virksomhed eller en myndighed opnår en certificering, vil den pågældende virksomhed eller myndighed modtage et bevis, f.eks. et certifikat (eller mærke), der attesterer, at virksomheden eller myndigheden har tilsluttet sig en certificeringsordning og dermed bør udføre en behandlingsaktivitet på den specifikke måde, som det foreskrives i certificeringsordningen.

En virksomhed eller myndighed, der har opnået en certificering vil formentlig – alt efter certificeringsordningens bestemmelser – kunne fremvise et certifikat (eller mærke) på sin hjemmeside eller vedhæfte det som bilag til en aftale, og dermed oplyse andre parter om, at virksomheden eller myndigheden overholder de krav og kriterier, som er indeholdt i certificeringsordningen.

## 3.2 Hvem kan tage initiativ til en certificeringsordning?

I modsætning til databeskyttelsesforordningens bestemmelser om adfærdskodekser indeholder forordningens bestemmelser om certificering ingen anvisninger af, hvem der skal tage initiativ til at udarbejde en certificeringsordning. I praksis vil det formentlig typisk være en virksomhed, der kan se et forretningspotentiale i at lade sig akkreditere som certificeringsorgan i forhold til en specifik behandlingsaktivitet. Det kan f.eks. være en virksomhed, der har en stor viden inden for pseudonymisering af sundhedsoplysninger, og som har en forventning om, at f.eks. et stort

antal forskere kunne være interesseret i at lade sig certificere i pseudonymisering. Når en virksomhed skal kunne se et forretningspotentiale i at lade sig akkreditere, så skyldes dette bl.a., at der vil være omkostninger forbundet med at blive akkrediteret, ligesom der vil være omkostninger forbundet med at opretholde sin akkreditering. Se mere herom nedenfor.

**Eksempel 8 – pseudonymisering af sundhedsoplysninger**

En virksomhed A, der har et indgående kendskab til sundhedssektoren, har specialiseret sig i forskning med pseudonymiserede sundhedsoplysninger.

Da A har en forventning om, at mange forskningsvirksomheder kunne være interesserede at følge A's retningslinjer for forskning med pseudonymiserede sundhedsoplysninger, vælger A at lade sig akkreditere som certificeringsorgan, således at A's retningslinjer kan blive udbudt via en certificeringsordning.

Efter A er blevet godkendt som certificeringsorgan, kan A udbyde sin certificeringsordning vedrørende forskning med pseudonymiserede sundhedsoplysninger til andre forskningsvirksomheder i Danmark (eventuelt hele EU, hvis kriterierne er blevet godkendt af Databeskyttelsesrådet). Disse forskningsvirksomheder kan herefter vælge at lade sig certificere hos A.

## 3.3 Hvordan adskiller en certificeringsordning efter databeskyttelsesforordningen sig fra andre kendte typer af certificeringsordninger?

Certificering er udbredt i mange brancher og efter flere forskellige standarder. Under ISO[3] er det f.eks. muligt at opnå certificering inden for informationssikkerhed (ISO27001) og kvalitet (ISO9001). Herudover findes der andre standarder, der f.eks. relaterer sig til fødevaresikkerhed, bygningskonstruktion mv.

I Danmark skal alle statslige myndigheder følge – og alle andre offentlige myndigheder skal følge principperne i – informationssikkerhedsstandarden ISO 27001. Standarden opsætter de styrende rammer for bl.a. ledelsesforankring og risikostyring og indeholder et katalog af styringsmål og foranstaltninger (kontroller), der kan vælges til eller fra.

Hvor en certificering efter ISO 27001 drejer sig om en virksomheds eller en myndigheds generelle organisatoriske setup, risikostyring, overholdelse og egenkontrol – herunder også omkring generel beskyttelse af personoplysninger i forhold til organisationens fastsatte sikkerhedsmål – vil en certificering efter databeskyttelsesforordningen være målrettet påvisningen af, at en eller flere behandlingsaktiviteter overholder forordningen, herunder f.eks. artikel 32 om behandlingssikkerhed.

Selvom der således kan være et vist overlap mellem begreberne i de to typer certificeringsordninger, vil der konkret være stor forskel på indholdet og rækkevidden af certificeringen.

[3] International Organisation for Standardization.

Nedenfor i afsnit 3.4. beskrives det nærmere, hvad en certificering efter databeskyttelsesforordningen kan benyttes til.

## 3.4 Hvad kan en certificering bruges til?

Der fremgår ikke af databeskyttelsesforordningens artikel 42 (om certificering) noget nærmere om, hvilke behandlinger en certificering kan specificere anvendelsen af forordningen i forhold til. Det må dog antages, at det bl.a. kan være nogle af de samme behandlinger, som fremgår af forordningens artikel 40, stk. 2, litra a-k, for så vidt angår adfærdskodekser, jf. afsnit 2.3. ovenfor.

I lighed med adfærdskodekser er der dog en række bestemmelser i databeskyttelsesforordningen, hvori det nævnes, at overholdelse af en godkendt certificeringsordning kan bruges af dataansvarlige og databehandlere som et element til at påvise overholdelsen af krav, ligesom overholdelse af godkendte certificeringsordninger kan inddrages ved vurderingen af f.eks. fastsættelse af en sanktion.

Nedenfor gennemgås de bestemmelser i databeskyttelsesforordningen, hvor overholdelse af en godkendt certificeringsordning kan tillægges betydning. Det bemærkes i den forbindelse, at der i meget vidt omfang er sammenfald med de bestemmelser i forordningen, hvor overholdelse af en godkendt adfærdskodeks kan tillægges betydning. De eksempler, der fremgår af afsnit 2.3. vil derfor også i et vist omfang kunne benyttes som inspiration i forhold til certificeringsordninger, men de vil ikke blive gengivet på ny i det følgende.

### 3.4.1 Den dataansvarliges ansvar (artikel 24)

Overholdelse af en godkendt certificeringsordning kan bruges som et element til at påvise, at den dataansvarlige lever op til sine forpligtelser efter forordningen.

Hvilke dele af databeskyttelsesforordningen, som en certificeringsordning skal bruges til at påvise overholdelsen af, vil naturligvis afhænge af indholdet af certificeringsordningen.

### 3.4.2 Databeskyttelse gennem design og standardindstillinger (artikel 25)

En godkendt certificeringsordning kan bruges som et element til at påvise overholdelse af forordningens krav om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

**Eksempel 9 – databeskyttelse gennem design og standardindstillinger**

En virksomhed B har specialiseret sig i, hvordan man gennem standardindstillinger – IT-tekniske indstillinger og organisatoriske foranstaltninger – understøtter databeskyttelse i tjenester, såsom onlinetjenester og apps, der bruger lokationsdata.

De IT-tekniske standardindstillinger består bl.a. i funktioner, der sikrer, at lokationsdata alene indsamles til det pågældende formål, og sikrer, at der indhentes udtrykkeligt samtykke til brugen af lokationsdata til formålet.

Hvis B søger om og bliver akkrediteret som certificeringsorgan, vil B f.eks. kunne udbyde sine IT-tekniske standardindstillinger til udviklere af tjenester, der bruger lokationsdata.

Når en udbyder af en tjeneste, der bruger lokationsdata, herefter lader sig certificere, vil denne kunne benytte certificeringen til at påvise, at udbyderen efterlever forordningens artikel 25.

Det bemærkes, at der i artikel 25, stk. 3, ikke henvises til godkendte adfærdskodekser, hvorfor der her er en forskel på, hvad man benytte henholdsvis adfærdskodekser og certificeringsordninger til.

### 3.4.3 Databehandlers påvisning af fornødne garantier (artikel 28)

En databehandler eller en underdatabehandlers overholdelse af en godkendt certificeringsordning kan bruges som et element til at påvise, at databehandleren stiller fornødne garantier.

### 3.4.4 Behandlingssikkerhed (artikel 32)

Overholdelse af en godkendt certificeringsordning, kan bruges som et element til at påvise den dataansvarliges eller databehandlerens overholdelse af kravene til behandlingssikkerhed.

### 3.4.5 Overførsler til tredjelande omfattet af fornødne garantier (artikel 46)

Hvis man som dataansvarlig eller databehandler ønsker at overføre personoplysninger til et tredjeland, skal man – ud over en videregivelseshjemmel – også have et såkaldt overførselsgrundlag i forordningens kapitel V. Et overførselsgrundlag kan f.eks. være fornødne garantier i form af Kommissionens standardkontrakter, eller at det pågældende tredjeland er godkendt af Kommissionen som et sikkert tredjeland.

Det fremgår af databeskyttelsesforordningens artikel 46, stk. 2, litra f, at de fornødne garantier i forbindelse med overførsel til et usikkert tredjeland kan sikres gennem en godkendt certificeringsordning sammen med bindende tilsagn, som kan håndhæves, fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier, herunder vedrørende de registreredes rettigheder.

### 3.4.6 Administrative bøder (artikel 83)

Af databeskyttelsesforordningens artikel 83, stk. 2, litra j, fremgår det, at der skal tages behørigt hensyn til, om en godkendt certificeringsordning er overholdt, når det skal afgøres, om der skal pålægges en administrativ bøde, og når det skal afgøres, hvor stor en eventuel administrativ bøde skal være.

Overholdelse af en godkendt certificeringsordning i forbindelse med en given behandling vil således f.eks. kunne inddrages som en formildende omstændighed ved fastsættelsen af en administrativ bødes størrelse.

Som nævnt ovenfor i afsnit 3.1. er det vigtigt at være opmærksom på, at tilslutning til og overholdelse af en godkendt certificeringsordning, ikke i sig selv er et bevis på overholdelse af databeskyttelsesforordningen, heller ikke for så vidt angår de artikler i forordningen, som ordningen måtte specificere anvendelsen af forordningen i forhold til. Overholdelse af en godkendt certificeringsordning kan dermed heller ikke fritage en dataansvarlig eller databehandler for ansvar.

## 3.5 Hvordan kan man blive certificeret?

Af databeskyttelsesforordningens artikel 42, stk. 5, fremgår det, at certificering kan foretages af et akkrediteret certificeringsorgan eller af Datatilsynet på grundlag af kriterier, der er godkendt af Datatilsynet eller Databeskyttelsesrådet.

Det fremgår ikke nærmere, hvem der skal udarbejde de kriterier for certificering, der skal godkendes af Datatilsynet eller Databeskyttelsesrådet, ligesom det ikke fremgår, hvad der skal til, for at kriterierne kan blive godkendt.

Kriterierne kan blive udarbejdet af de certificeringsorganer, der ønsker at udbyde en given certificeringsordning[4]. Endvidere kan de nationale datatilsyn og Databeskyttelsesrådet i fællesskab udstede retningslinjer for, hvad der skal til for, at kriterier for certificering kan blive godkendt, idet der ellers er en stor risiko for, at praksis vil blive meget forskelligartet.

Hvis ovennævnte kriterier er godkendt af Databeskyttelsesrådet, kan det føre til en fælles certificering, Den Europæiske Databeskyttelsesmærkning. En fælles certificering vil således – modsat en ren national certificering – kunne benyttes i alle EU-lande. Det må formodes, at fælles certificeringer vil blive foretrukket af de virksomheder, der måtte ønske at lade sig certificere, især hvis de pågældende virksomheder opererer i flere medlemsstater. Dette er formentlig også baggrunden for, at medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen navnlig på EU-plan skal tilskynde til fastlæggelse af certificeringsordninger.

Alle godkendte certificeringsordninger – nationale og fælles – vil blive offentliggjort på Databeskyttelsesrådets hjemmeside. Herudover vil Datatilsynet offentliggøre alle nationale certificeringsordninger på sin hjemmeside.

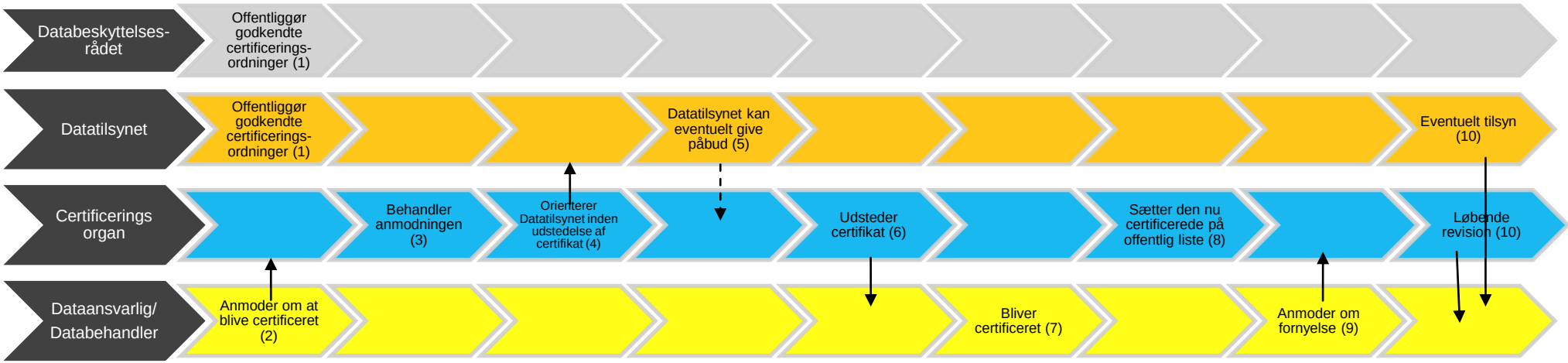
Ønsker en dataansvarlig at afsøge mulighederne for at lade sig certificere, kan de således besøge Databeskyttelsesrådets og Datatilsynets hjemmesider for at se, hvilke godkendte certificeringsordninger (og i øvrigt også certificeringsorganer), der måtte være på markedet.

[4] Se også side 24 ENISA's rapport fra november 2017 vedrørende anbefalinger til europæiske databeskyttelsescertifikater. Rapporten kan læses her: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification

Selvom det er muligt for både Datatilsynet og akkrediterede certificeringsorganer at foretage certificering, vil det i praksis – som udgangspunkt – være de akkrediterede certificeringsorganer, som vil stå for udstedelse af certifikater, forlængelse af certifikater (et certifikat gælder i højst tre år) og tilbagetrækning af certifikater (f.eks. hvis den certificerede virksomhed ikke længere lever op til kravene). Det er således det akkrediterede certificeringsorgan, som en dataansvarlig eller databehandler, der ønsker at blive certificeret, skal rette henvendelse til. Dette giver også bedst mening, da det må formodes, at det akkrediterede certificeringsorgan har størst viden om den certificeringsordning, som de har taget initiativ til og varetager administrationen af.

Det har ingen betydning for Datatilsynets opgaver og beføjelser i øvrigt, at det i det daglige er de akkrediterede certificeringsorganer, der står for udstedelse mv. af certifikater. Datatilsynet kan derfor bl.a. godt – som led i sin tilsynsvirksomhed – vælge at føre tilsyn med, om en certificeret virksomhed lever op til certificeringsordningens krav og kriterier. Det må i øvrigt også forventes, at Datatilsynet vil føre tilsyn med certificerede virksomheder, da det er en af tilsynets opgaver, jf. artikel 57.

I Figur 2 kan man få et overblik over et certificeringsforløb og de forskellige aktørers rolle.




Figur 2 Overordnet oversigt over certificeringsforløb

1. Datatilsynet og Databeskyttelsesrådet vil offentliggøre oversigter over godkendte certificeringsordninger (det vil af disse oversigter fremgå, hvilke certificeringsordninger der er rent nationale, og hvilke ordninger der er fælles).
2. En dataansvarlig eller en databehandler, der har fundet en relevant certificeringsordning på Datatilsynets eller Databeskyttelsesrådets hjemmeside, anmoder det kompetente certificeringsorgan om at blive certificeret.
3. Certificeringsorganet foretager en vurdering af, om den virksomhed, der søger om at blive certificeret, lever op til kravene og kriterierne for at blive certificeret.
4. Certificeringsorganet meddeler Datatilsynet om begrundelsen for udstedelse af et certifikat.
5. Datatilsynet kan eventuelt give et påbud til certificeringsorganet om at undlade at udstede et certifikat.
6. Certificeringsorganet udsteder et certifikat.
7. Nu kan en dataansvarlig/databehandler benytte sig af certifikatet, herunder f.eks. reklamere med det på sin hjemmeside.
8. Udstedte certifikater vil blive offentliggjort af certificeringsorganet, så eventuelle registrerede kan få bekræftet, om en given virksomhed er certificeret.
9. En certificering udstedes for en periode på højst 3 år, hvorefter det kan forlænges på samme betingelser, hvis de relevante krav og kriterier stadig er opfyldt.
10. Datatilsynet kan løbende føre tilsyn med, om kravene til certificering er overholdt og kan i den forbindelse f.eks. tilbagetrække et certifikat. Samtidig vil certificeringsorganet gennemføre løbende revision i overensstemmelse med bestemmelserne herom i certificeringsordningen.

## 3.6 Hvordan kan man blive akkrediteret som certificeringsorgan?

Hvis en virksomhed (eller en myndighed) ønsker at udbyde en given certificeringsordning, er det et krav, at virksomheden først bliver akkrediteret (godkendt) som certificeringsorgan.

I Danmark kan en virksomhed i princippet blive akkrediteret som certificeringsorgan af enten 1) Datatilsynet eller 2) det danske akkrediteringsorgan (DANAK[5]), der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008.

I praksis vil det dog være DANAK, der kommer til at stå for at akkreditere certificeringsorganer, idet DANAK har stor erfaring med at foretage akkreditering på andre områder. Det er således DANAK, som en virksomhed skal tage kontakt til, hvis den ønsker at blive akkrediteret som certificeringsorgan.

Når DANAK skal vurdere, om en virksomhed kan blive akkrediteret som certificeringsorgan, vil DANAK se på, om virksomheden lever op til disse kriterier:

a) Ansøgeren skal have påvist sin uafhængighed og ekspertise med hensyn til certificeringens genstand
b) ansøgeren skal have påtaget sig at opfylde kriterierne i artikel 42, stk. 5, som er blevet godkendt af Datatilsynet, der er kompetent i henhold til artikel 55 eller 56, eller af Databeskyttelsesrådet i henhold til artikel 63
c) ansøgeren skal have fastlagt procedurer for udstedelse, regelmæssig revision og tilbagetrækning af databeskyttelsescertificeringer, -mærkninger og –mærker
d) ansøgeren skal have fastlagt procedurer og ordninger for behandling af klager over overtrædelser af certificering eller den måde, hvorpå certificering er blevet eller bliver gennemført på af en dataansvarlig eller en databehandler, og for, hvordan disse procedurer og ordninger gøres gennemsigtige for registrerede og offentligheden, og
e) ansøgeren skal have vist til, at dens opgaver og pligter ikke fører til en interessekonflikt.

Herudover vil en virksomhed, der ønsker at blive akkrediteret som certificeringsorgan, skulle opfylde de krav, som følger af forordning (EF) nr. 765/2008 samt EN-ISO/IEC 17065/2012[6], som DANAK arbejder ud fra, samt eventuelle supplerende krav fastsat af Datatilsynet.

Det er endnu ikke besluttet, om Datatilsynet vil fastsætte supplerende krav, samt hvad disse krav i givet fald måtte gå ud på. De eventuelle supplerende krav vil blive meldt ud senest i foråret 2018.

Ved en gennemgang af ovennævnte krav kan det konkluderes, at der stilles ret høje krav til en virksomhed, der ønsker at blive godkendt som certificeringsorgan, herunder krav om, at virk-

[5] Den Danske Akkrediteringsfond. Se mere om DANAK her: http://portal.danak.dk/

[6] EN-ISO/IEC 17065/2012 opstiller krav til organer, der certificerer produkter, processer og serviceydelser.

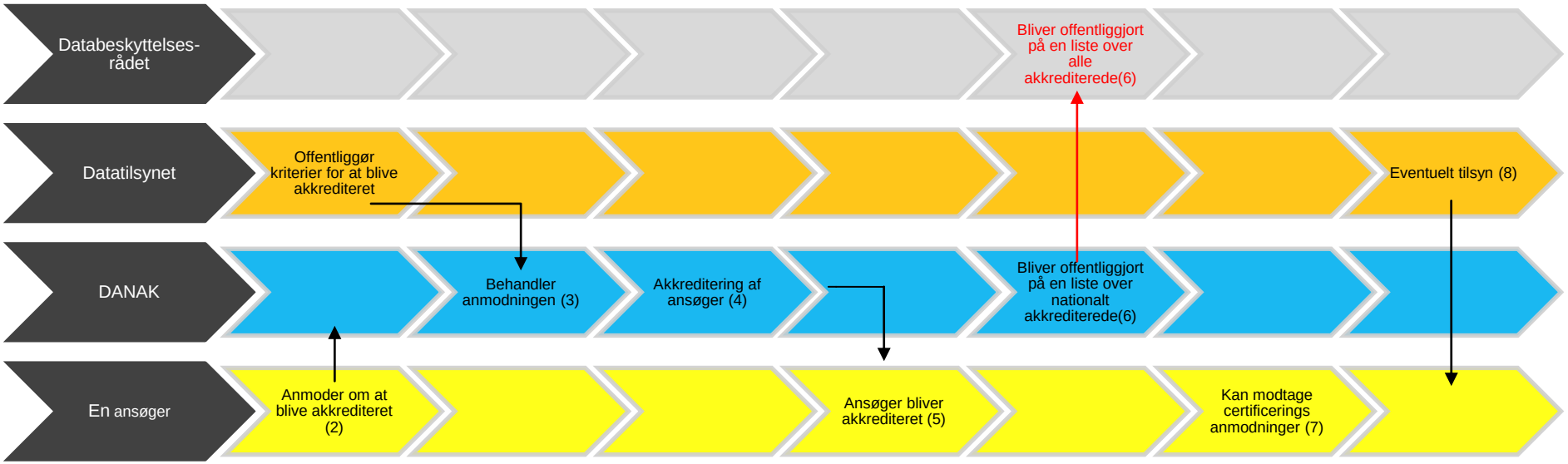
somheden både skal have ekspertise inden for databeskyttelse og certificering generelt, men også ekspertise i forhold til det område, som certificeringen specifikt retter sig imod.

En akkreditering kan udstedes for en periode på højst 5 år, og den vil kunne blive forlænget, hvis certificeringsorganet fortsat lever op til de fastsatte krav.

Datatilsynet sørger i øvrigt for løbende – i let tilgængelig form – at offentliggøre de til enhver tid gældende krav for at blive akkrediteret. Kravene vil fremgå af tilsynets hjemmeside.

Hvis et akkrediteret certificeringsorgan ikke længere lever op til kravene for at blive akkrediteret, kan både Datatilsynet og DANAK tilbagekalde akkrediteringen. Det samme gør sig gældende, hvis et certificeringsorgan foretager sig noget, som er i strid med databeskyttelsesforordningen.

I Figur 3 kan man få et overblik over et akkrediteringsforløb og de forskellige parters roller.




Figur 3 Overordnet oversigt over et akkrediteringsforløb

1. Datatilsynet offentliggør de kriterier for at blive akkrediteret, der er godkendt af tilsynet selv og Databeskyttelsesrådet.
2. En ansøger (virksomhed) anmoder DANAK om at blive akkrediteret som certificeringsorgan.
3. DANAK foretager en vurdering af, om ansøger lever op til kravene og kriterierne for at blive akkrediteret, herunder de af Datatilsynet opstillede kriterier og kravene i forordning (EF) nr. 765/2008.
4. DANAK akkrediterer ansøger.
5. Ansøger er nu godkendt som certificeringsorgan.
6. DANAK fører – på sin hjemmeside – en liste over de virksomheder (certificeringsorganer), der er blevet akkrediteret af DANAK. Samtidig fører Databskyttelsesrådet et offentligt tilgængeligt register over alle certificeringsordninger (og dermed også alle akkrediterede virksomheder).
7. Ansøger kan nu fungere som certificeringsorgan og kan dermed behandle anmodninger om certificering fra dataansvarlige/databehandlere.
8. Datatilsynet kan løbende føre tilsyn med, om et akkrediteret certificeringsorgan lever op til kravene og kriterierne for akkreditering og kan i den forbindelse f.eks. tilbagetrække en akkreditering.