# Vejledning

## Certificeringsordninger

April 2021

DATATILSYNET

# Indhold

# Forord

Denne vejledning erstatter Datatilsynets og Justitsministeriets vejledning om adfærdskodekser og certificeringsordninger fra januar 2018 (opdateret december 2018) i forhold til den del af vejledningen, som omhandler certificeringsordninger.

Når Datatilsynet har fundet anledning til at opdatere vejledningen i forhold til certificeringsordninger, skyldes det primært, at Det Europæiske Databeskyttelsesråd (EDPB) i 2018 har vedtaget to vejledninger om henholdsvis certificering og udarbejdelse af certificeringskriterier og akkreditering af certificeringsorganer, som begge er blevet opdateret i løbet af 2019, og at tilsynet har udarbejdet supplerende akkrediteringskrav til certificeringsorganer, som er blevet godkendt af EDPB i marts 2021.

Denne vejledning omhandler certificeringsordninger efter databeskyttelsesforordningen og henvender sig primært til virksomheder og myndigheder, som overvejer at udarbejde eller tilmelde sig en sådan certificeringsordning.

Databeskyttelsesforordningen indeholder et grundlæggende princip om ansvarlighed. Ansvarlighedsprincippet indebærer for det *første*, at den dataansvarlige – og i visse tilfælde databehandleren – har ansvaret for, at forordningens regler efterleves. For det *andet* skal den dataansvarlige også kunne påvise, at de behandlinger denne har ansvaret for, lever op til forordningens regler.[1]

For nogle virksomheder og myndigheder kan det synes uoverskueligt at skulle sætte sig ind i og forstå databeskyttelsesforordningens mange forskelligartede regler. Forordningen indeholder derfor en række tiltag, der skal hjælpe til at lette overholdelsen af databeskyttelsesreglerne både for dataansvarlige og databehandlere. Disse tiltag inkluderer både obligatoriske krav (såsom udpegelse af databeskyttelsesrådgivere og udarbejdelse af fortegnelser m.v.), og en række frivillige værktøjer.

Med ønsket om at kunne hjælpe dataansvarlige og databehandlere til at overholde databeskyttelsesreglerne er der i forordningen bl.a. indsat en mulighed for at udarbejde såkaldte certificeringsordninger.

Certificering er et frivilligt værktøj, som myndigheder og virksomheder som dataansvarlige og databehandlere kan bruge til at kunne demonstrere, at de efterlever reglerne i databeskyttelsesforordningen. Herudover kan certificering bidrage til at øge gennemsigtigheden omkring myndighedens eller virksomhedens behandling af personoplysninger over for bl.a. borgere, kunder, forretningsforbindelser m.v., idet en certificering kan bruges som et middel til hurtigt

1 Se databeskyttelsesforordningens artikel 5, stk. 2.

at kunne vurdere niveauet af databeskyttelse for myndighedens eller virksomhedens produkter, processer eller tjenester.

I denne vejledning får du bl.a. en introduktion til, hvad en databeskyttelsesretlig certificeringsordning er, hvem der kan udarbejde en certificeringsordning, hvad man kan bruge certificeringsordninger til, og hvordan en certificeringsordning godkendes. Du kan også læse om, hvordan man som myndighed eller virksomhed tilslutter sig en certificeringsordning.

Det bemærkes, at denne vejledning ikke berører brugen af certificeringsordninger som overførselsgrundlag, jf. databeskyttelsesforordningens artikel 46, stk. 2, litra f. Det skyldes, at EDPB er ved at udarbejde en vejledning herom, som Datatilsynet afventer.

Vejledningen er et supplement til EDPB's vejledninger om certificering og udarbejdelse af certificeringskriterier og akkreditering af certificeringsorganer.

# 1. Hvad er en certificeringsordning?

I dette indledende afsnit finder du en overordnet beskrivelse af certificeringsordninger, og hvad formålet med ordningerne er.

## 1.1 Hvad er en certificeringsordning?

En certificeringsordning er en ordning, der bygger på tredjeparts certificering. Et akkrediteret (godkendt) certificeringsorgan attesterer, at en virksomhed eller en myndighed (dvs. en dataansvarlig eller en databehandler) – der har anmodet om at blive certificeret – lever op til et foruddefineret sæt af kriterier (certificeringskriterier).

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

Hvor en certificering efter ISO 27001 drejer sig om en virksomheds eller en myndigheds ledelsessystem eksempelvis organisatoriske set up, 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, herunder tilknyttede processer og procedurer, overholder specifikke krav i databeskyttelsesforordningen.

Certificering efter databeskyttelsesforordningen kan anvendes til en bestemt behandling eller flere behandlinger af personoplysninger (dvs. behandlingsaktiviteter) indeholdt i et produkt, en proces eller en tjeneste, der tilbydes af en dataansvarlig eller databehandler[2].

### Eksempler på behandlingsaktiviteter

Certificering efter databeskyttelsesforordningen relaterer sig til behandlingsaktiviteter, dvs. bestemte former for behandling af personoplysninger. En certificering kan eksempelvis vedrøre indsamling, registrering, organisering, opbevaring, ændring, videregivelse, offentliggørelse, pseudonymisering eller sletning af personoplysninger m.v..

Når en virksomhed eller myndighed opnår en certificering under en certificeringsordning, kan det være med til at demonstrere, at virksomhedens eller myndighedens behandlingsaktiviteter finder sted i overensstemmelse med reglerne i databeskyttelsesforordningen.

Certificeringskriterierne – som certificeringsordningen bygger på – skal godkendes af Datatilsynet, eller af EDPB, hvis der er tale om en fællescertificering, som kan benyttes i alle EØS-

2 Certificering kan kun udstedes til virksomheder eller myndigheder, der er dataansvarlige og databehandlere, og kan derfor ikke udstedes til enkeltpersoner, eksempelvis databeskyttelsesrådgivere.

lande[3]. Herudover skal certificeringsordningen godkendes af den danske akkrediteringsfond, DANAK[4], inden der kan ske akkreditering af certificeringsorganet. Du kan læse mere om akkreditering af certificeringsorganer under vejledningens afsnit 2.

En certificeringsordnings anvendelsesområde, herunder certificeringskriterierne, kan enten være specifikt eller af mere generel karakter. Du kan læse mere herom under vejledningens afsnit 3.2.

Hvis en virksomhed eller en myndighed opnår en certificering, vil den pågældende virksomhed eller myndighed modtage et certifikat, der erklærer, hvilke specifikke behandlingsaktiviteter i virksomhedens eller myndighedens produkt, proces eller tjeneste, som er dækket af certificeringen, ligesom det vil fremgå af certifikatet, hvor længe certificeringen er gyldig.

En virksomhed eller myndighed, der har opnået en certificering vil formentlig – alt efter certificeringsordningens bestemmelser – også kunne fremvise et mærke eller logo, som demonstrerer, at virksomheden eller myndigheden overholder de krav og kriterier, som er indeholdt i den pågældende certificeringsordning.

## 1.2 Hvad er formålet med en certificeringsordning?

Certificering – som er et frivilligt værktøj – kan som nævnt være med til at demonstrere, at virksomheders eller myndigheders behandlingsaktiviteter finder sted i overensstemmelse med reglerne i databeskyttelsesforordningen.

Formålet med certificeringsordninger hænger derfor også fint sammen med databeskyttelsesforordningens fokus på ansvarlighed (”accountability”).

Udover at hjælpe med at demonstrere overholdelse af databeskyttelsesreglerne over for Datatilsynet, kan en certificeringsordning også hjælpe med at demonstrere overholdelse af databeskyttelsesreglerne over for offentligheden, forretningspartnere og eventuelle andre interessenter. Certificering kan nemlig bruges som et middel til hurtigt at kunne vurdere niveauet af databeskyttelse for en virksomheds eller myndigheds produkter, processer eller tjenester, og det kan samtidig være med til at skabe gennemsigtighed både for borgere og i eventuelle forretningsmæssige forhold.

Ifølge databeskyttelsesforordningen kan certificering bruges som et element til at:

- Påvise, at den dataansvarlige lever op til sine forpligtelser efter forordningen[5].
- Påvise overholdelse af databeskyttelsesforordningens krav om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger[6]
- Påvise, at en databehandler stiller de fornødne garantier[7]
- Påvise virksomheders eller myndigheders overholdelse af databeskyttelsesforordningens krav om passende sikkerhed[8]
- Sikre fornødne garantier i forbindelse med overførsel af personoplysninger til et usikkert tredjeland[9]

3 EØS er forkortelsen for Det Europæiske Økonomiske Samarbejdsområde, som blev etableret ved en aftale mellem EU og tre af EFTA-landene, nemlig Norge, Island og Liechtenstein i 1994. EØS-aftalen betyder, at EU’s bestemmelser om det indre marked, herunder databeskyttelsesforordningen (GDPR), også gælder i disse tre lande.
4 DANAK er det danske akkrediteringsorgan, der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008. Se mere om DANAK her: http://portal.danak.dk/mappe-3
5 Jf. databeskyttelsesforordningens artikel 24, stk.3
6 Jf. databeskyttelsesforordningens artikel 25, stk. 3.
7 Jf. databeskyttelsesforordningens artikel 28, stk. 5.
8 Jf. databeskyttelsesforordningens artikel 32, stk. 3
9 Jf. databeskyttelsesforordningens artikel 46, stk. 2, litra f.

Herudover vil tilslutning til og overholdelse af en godkendt certificeringsordning kunne inddrages som en formildende eller skærpende omstændighed i tilfælde af overtrædelse af de databeskyttelsesretlige regler, både i forhold til om der skal pålægges en bøde, og når det skal afgøres, hvor stor en eventuel bøde skal være.

Det er dog 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. Overholdelse af en godkendt certificeringsordning kan dermed heller ikke fritage en dataansvarlig eller databehandler for ansvar.

## Kort fortalt

**1.** Certificering kan være med til at demonstrere, at virksomheder og myndigheder overholder databeskyttelsesreglerne og kan være med til at øge gennemsigtigheden omkring niveauet for databeskyttelse i forbindelse med bestemte produkter, processer eller tjenester.

**2.** Certificeringskriterier skal godkendes af Datatilsynet. Hvis der er tale om en fællescertificering, som kan benyttes i alle EØS-lande, skal kriterierne derimod godkendes af Databeskyttelsesrådet (EDPB).

**3.** Certificering kan kun udstedes af et akkrediteret certificeringsorgan.

**4.** I Danmark godkendes enhver certificeringsordning af den danske akkrediteringsfond, DANAK, i forbindelse med akkrediteringen af certificeringsorganet, så det sikres, at ordningen lever op til kravene til akkrediteret certificering.

**5.** Certificering udstedes til dataansvarlige og databehandlere i forhold til specifikke behandlingsaktiviteter.

**6.** Det er frivilligt, om man vil ansøge om at blive certificeret. Hvis der er en godkendt certificeringsordning, som dækker din organisations behandlingsaktiviteter, kan du overveje at få certificeret dine behandlingsaktiviteter, da det kan hjælpe med at demonstrere overholdelse af databeskyttelsesreglerne over for Datatilsynet, offentligheden, forretningspartnere og andre eventuelle interessenter.

## Vil du vide mere?

De relevante bestemmelser i databeskyttelsesforordningen er artikel 42, 43 og 83 og præambelbetragtninger nr. 81 og 100.

**EDPB's vejledning om certificering og certificeringskriterier**

EDPB har udarbejdet og vedtaget en vejledning om certificering og udarbejdelse af certificeringskriterier (Retningslinjer 1/2018 vedrørende certificering og identifikation af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordningen).

**EDPB's vejledning om akkreditering af certificeringsorganer**

EDPB har udarbejdet og vedtaget en vejledning om akkreditering af certificeringsorganer (Vejledning 4/2018 om akkreditering af certificeringsorganer).

**DANAK's akkrediteringsmeddelelse vedr. akkreditering efter databeskyttelsesforordningen (AMC 31)**

DANAK og Datatilsynet har udarbejdet en akkrediteringsmeddelelse (AMC 31), som beskriver roller, ansvar og fremgangsmåden i forhold til akkreditering af certificeringsorganer efter databeskyttelsesforordningen. Akkrediteringsmeddelelsen kan tilgås DANAK's hjemmeside.

# 2. Hvad skal til for at kunne udbyde en certificeringsordning?

I dette afsnit finder du en kort beskrivelse af certificering og akkreditering. Afsnittet henvender sig primært til myndigheder og virksomheder, som overvejer at tilbyde en certificeringsordning og i den forbindelse ønsker at blive et akkrediteret (godkendt) certificeringsorgan, idet størstedelen af afsnittet vedrører den danske akkrediteringsproces og de krav, organisationer skal opfylde i den forbindelse. Hvis du alene ønsker at udarbejde et sæt kriterier til en certificeringsordning, men ønsker at lade en anden organisation være det akkrediterede certificeringsorgan, kan du med fordel springe videre til vejledningens afsnit 3.

## 2.1 Certificering og akkreditering – kort om processerne

En certificering er en form for blåstempling af, at en virksomhed eller myndighed lever op til nogle specifikke krav i en bestemt certificeringsordning. Som nævnt i vejledningens indledende afsnit indebærer certificering, at en uafhængig tredjepart (et certificeringsorgan) attesterer for, at en virksomhed eller en myndighed – der har anmodet om at blive certificeret – lever op til certificeringsordningens kriterier. Kun certificeringsorganer, der er akkrediteret (bedømt af et akkrediteringsorgan) må udføre certificeringen.

Hvis en virksomhed eller en myndighed ønsker at udbyde en certificeringsordning, er det et krav, at de kriterier, som ordningen baseres på, først er godkendt af Datatilsynet (eller af EDPB, hvis der er tale om en fælles certificering, som gælder i alle EØS-lande).

Når Datatilsynet har godkendt certificeringsordningens kriterier, vil virksomheden eller myndigheden skulle godkendes (akkrediteres) som certificeringsorgan gennem den danske akkrediteringsfond, DANAK, før virksomheden eller myndigheden kan udbyde ordningen.

Databeskyttelsesforordningens bestemmelser om certificering indeholder ingen anvisninger af, hvem der skal tage initiativ til at udarbejde en certificeringsordning og giver således mulighed for, at flere forskellige interessenter kan udvikle certificeringsordninger, herunder Datatilsynet, certificeringsorganer eller andre interessenter.

Selvom databeskyttelsesreglerne giver mulighed for, at Datatilsynet kan oprette sin egen certificeringsordning, har tilsynet på nuværende tidspunkt ikke planer om at gøre dette. Datatilsynets fokus på dette stadie er i stedet at sikre, at tilsynet har de nødvendige processer på plads, som letter muligheden for databeskyttelsescertificering i Danmark.

Datatilsynet forventer, at certificeringsordninger primært vil blive udarbejdet af certificeringsorganer – eventuelt i samarbejde med andre interessenter der designer og udvikler certificeringskriterierne.

Hvis din organisation alene ønsker at designe eller udvikle kriterierne for en certificeringsordning, kan du med fordel springe videre til vejledningens afsnit 3, som omhandler udarbejdelse af certificeringskriterier.

Hvis din organisation ønsker at blive et akkrediteret (godkendt) certificeringsorgan, kan du læse mere om godkendelsesprocessen nedenfor under afsnit 2.2-2.6.

## Overblik over parter som er involveret i certificering og akkreditering:

**Datatilsynet** som står for at godkende kriterierne i certificeringsordninger, og som har udarbejdet en række supplerende akkrediteringskrav til certificeringsorganer.

**DANAK** som har til opgave at akkreditere (godkende) de virksomheder eller myndigheder, som ønsker at blive certificeringsorganer, herunder godkende at certificeringsordningen lever op til kravene om akkrediteret certificering.

**Det Europæiske Databeskyttelsesråd (EDPB)**[10] som er det uafhængige europæiske organ, som bidrager til en ensartet anvendelse af databeskyttelsesforordningen i hele EU, herunder træffer afgørelser om certificeringskriterierne i nationale og fælleseuropæiske certificeringsordninger. Rådet består af repræsentanter for de nationale datatilsyn og Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). EØS-landenes tilsynsmyndigheder (Island, Liechtenstein og Norge) deltager også som medlemmer, dog uden stemmeret.

**Certificeringsordningsejere/designere** som er interessenter, der udarbejder og/eller ejer certificeringsordninger.

**Certificeringsorganer** som er de organisationer, der vurderer, om virksomheders eller myndigheders behandlingsaktiviteter opfylder kravene i certificeringsordninger, og som herefter udsteder certificeringer, hvis kravene er opfyldt.

**Certificeringskunder (virksomheder og myndigheder)**, som er dataansvarlige eller databehandlere), og som ønsker at få deres behandlingsaktiviteter certificeret.

## 2.2 Hvordan bliver man et certificeringsorgan?

I praksis vil et certificeringsorgan formentlig typisk være en virksomhed, der kan se et forretningspotentiale i at lade sig akkreditere som certificeringsorgan i forhold til en eller flere specifikke behandlingsaktiviteter. 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.

Et certificeringsorgan skal akkrediteres, før organet kan udstede certificeringer. Akkrediteringen skal ske i den medlemsstat, hvor certificeringsorganets hovedsæde er hjemmehørende – hvis altså det kun er hovedsædet, som udsteder certificering. Hvis certificeringsorganet har flere etableringer eller kontorer, som også skal udstede certificering, skal disse etableringer eller kontorer også akkrediteres i den medlemsstat, hvor de er hjemmehørende.

I Danmark sker akkrediteringen gennem DANAK (Den Danske Akkrediteringsfond).

Inden DANAK kan tildele akkreditering, skal DANAK evaluere certificeringsordningen. Evalueringen af ordningen skal sikre, at der kan udføres akkrediteret certificering efter ordningen.

10 Se mere om EDPB på Datatilsynets hjemmeside her eller på rådets egen hjemmeside her.

DANAK evaluerer certificeringsordninger efter de krav, som er fastsat af European Accreditation (EA) i proceduren EA-1/22 og DANAK's akkrediteringsbestemmelse AB 21.

Når DANAK skal vurdere, om en virksomhed eller myndighed kan blive akkrediteret som certificeringsorgan, vil DANAK se på, om virksomheden lever op til kriterierne i databeskyttelsesforordningens artikel 43, stk. 2. For at blive akkrediteret, skal virksomheden eller myndigheden også leve op til de krav, som følger af ISO/IEC 17065/2012 og Datatilsynets supplerende akkrediteringskrav. En akkreditering kan udstedes for en periode på højst 5 år[11], og den vil kunne blive forlænget, hvis certificeringsorganet fortsat lever op til de fastsatte krav.

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

### 2.2.1 Hvad skal vi vide, før vi beslutter os for at ansøge om at blive et certificeringsorgan?

For at være kvalificeret til at være et certificeringsorgan, skal din organisation blandt andet kunne opfylde følgende betingelser:

- ✓ Din organisation skal være en juridisk enhed eller en del af en juridisk enhed, som kan holdes ansvarlig for alle sine certificeringsaktiviteter.
- ✓ For at sikre upartiskhed ved behandlingen af ansøgninger om certificeringer, må der ikke være nogen relevant forbindelse mellem certificeringsorganet og ansøgerne. Din organisation må eksempelvis ikke både levere konsulentydelser og certificeringer til ansøgerne.
- ✓ Din organisation skal være i stand til at kunne demonstrere, at jeres certificeringsprocedurer, herunder særligt jeres håndtering af personoplysninger i forbindelse med certificeringsprocessen, lever op til reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Din organisation skal blandt andet kunne bekræfte over for DANAK, at den ikke er genstand for undersøgelser eller afgørelser fra Datatilsynet, som betyder, at organisationen muligvis ikke kan leve op til dette krav.
- ✓ Din organisation skal kunne påvise ekspertise med hensyn til databeskyttelse og certificeringsordningens anvendelsesområde.
- ✓ Din organisation skal have fastlagt procedurer for udstedelse, regelmæssig gennemgang og tilbagetrækning af databeskyttelsescertificeringer og -mærker.
- ✓ Din organisation skal have fastlagt procedurer for behandling af klager vedrørende de certificeringsaktiviteter, som din organisation – som certificeringsorgan – er ansvarlig for. Der stilles også krav om, at disse procedurer skal gøres offentligt tilgængelige og lettilgængelige for borgere.

Ovenstående er blot eksempler på nogle af de betingelser, som din organisation skal opfylde for at kunne blive et akkrediteret certificeringsorgan. Du kan læse mere om, hvordan man bliver akkrediteret på DANAK's hjemmeside.

Som nævnt skal din organisation for at kunne blive godkendt som et certificeringsorgan generelt kunne leve op til de krav, som følger af databeskyttelsesforordningens artikel 43, stk. 2. For at blive akkrediteret skal din organisation også leve op til kravene om akkrediteret certificering, herunder kravene i EN-ISO/IEC 17065/2012 og de supplerende akkrediteringskrav, som er udarbejdet af Datatilsynet.

11 Jf. databeskyttelsesforordningens artikel 43, stk. 4, hvoraf det fremgår, at akkreditering kan gives til maksimalt 5 år. Hos DANAK er akkrediteringsperioden dog 4 år.

Du kan finde Datatilsynets supplerende akkrediteringskrav på tilsynets hjemmeside på dansk og engelsk.

Du kan finde DANAK's krav til akkrediteret certificering af produkter, processer og tjenester på DANAK's hjemmeside. Inden din organisation ansøger om at blive et certificeringsorgan, skal du endvidere være opmærksom på, at DANAK kræver betaling for akkreditering. Du kan finde flere informationer om akkrediteringsprocessen og eventuelle omkostninger på DANAK's hjemmeside.

## 2.3 Hvordan ansøger vi om at blive et certificeringsorgan?

Når du har fundet ud af, hvilken certificeringsordning din organisation ønsker at udbyde, og ordningens kriterier er godkendt af Datatilsynet, kan du ansøge om at blive akkrediteret som certificeringsorgan hos DANAK.

Processen for ansøgning om akkreditering er nærmere beskrevet på DANAK's hjemmeside.

Ansøgning om akkreditering foretages ved hjælp af DANAK's ansøgningsblanket (vælg blanketten vedrørende produktcertificering), som kan findes på DANAK's hjemmeside. DANAK vejleder gerne kommende ansøgere om kravene til certificeringsorganer.

Hvis hensigtsmæssigt kan behandlingen af akkrediteringsansøgningen efter aftale med DANAK foretages parallelt med Datatilsynets behandling af certificeringsordningens kriterier. Akkreditering kan dog ikke udstedes, før Datatilsynet har godkendt kriterierne, og DANAK har godkendt, at certificeringsordningen lever op til kravene om akkrediteret certificering.

## 2.4 Certificeringsorganets forhold til Datatilsynet

Certificeringsorganet skal være opmærksom på, at kriterierne for den certificeringsordning, som certificeringsorganet ønsker at udbyde, skal godkendes af Datatilsynet. Som certificeringsorgan kan man vælge selv at udarbejde ordningen og kriterierne, eller man kan vælge at udbyde kriterier, som er udarbejdet af en tredjepart. Du kan læse mere om certificeringskriterierne nedenfor under afsnit 3.

Når kriterierne for den certificeringsordning, som certificeringsorganet ønsker at udbyde, er blevet godkendt af Datatilsynet, og når certificeringsorganet er blevet akkrediteret af DANAK, vil certificeringsorganet være forpligtet til at informere Datatilsynet om alle de ansøgninger om certificering, som certificeringsorganet modtager[12], og om certificeringsorganets begrundelser for at udstede, forny eller tilbagetrække certificeringer[13].

Certificeringsorganet skal endvidere være opmærksom på, at DANAK efter omstændighederne vil kunne underrette Datatilsynet om følgende forhold:

- Ansøgninger som DANAK modtager om akkreditering.
- Akkrediteringer som DANAK udsteder, fornyer, nægter eller tilbagetrækker.
- Enhver uoverensstemmelse med certificeringsorganet, herunder bl.a. klager over certificeringsorganet, som efter DANAK's vurdering har potentiale til at føre til suspension eller tilbagetrækning af akkreditering, eller som kan resultere i en overtrædelse af databeskyttelsesreglerne.

12 Dette krav følger af pkt. 7.2. i de supplerende akkrediteringskrav, som Datatilsynet har udarbejdet. Du kan finde de supplerende akkrediteringskrav på Datatilsynets hjemmeside her.
13 Jf. databeskyttelsesforordningens artikel 43, stk. 5

## 2.5 Hvordan vil offentligheden vide, at vi er akkrediteret som certificeringsorgan?

DANAK fører – på sin hjemmeside – en liste over de certificeringsorganer, der er blevet akkrediteret af DANAK.

Datatilsynet offentliggør en oversigt over godkendte certificeringskriterier på tilsynets hjemmeside[14]. Samtidig fører EDPB et offentligt tilgængeligt register over alle godkendte certificeringskriterier på rådets hjemmeside.

Ind til videre foreligger der ingen godkendte databeskyttelsesretlige certificeringsordninger på hverken dansk eller europæisk niveau.

## 2.6 Hvilke informationer skal vi offentliggøre som certificeringsorgan?

Som certificeringsorgan vil du være forpligtet til at føre en oversigt over de kunder, som du har udstedt certificering til. Oversigten skal indeholde de oplysninger, som kræves i henhold til EN-ISO/IEC 17065/2012 og de supplerende akkrediteringskrav, som Datatilsynet har udarbejdet. Det inkluderer blandt andet information om certificeringsordningens anvendelsesområde, hvor længe de udstedte certificeringer er gyldige, og under hvilke rammer og betingelser certificeringerne er gyldige. Denne information skal være offentligt tilgængelig.[15]

14 Jf. databeskyttelsesforordningens artikel 43, stk.6, som bestemmer, at Datatilsynet skal offentliggøre godkendte certificeringskriterier i en lettilgængelig form.
15 Dette krav følger af pkt. 7.8. i de supplerende akkrediteringskrav, som Datatilsynet har udarbejdet.

# 3. Hvordan laver man certificeringskriterier?

Dette afsnit henvender sig til myndigheder og virksomheder, som overvejer at tilbyde en certificeringsordning og i den forbindelse ønsker at udarbejde certificeringsordningens kriterier. Her kan du læse om, hvad en certificeringsordning kan omhandle, og hvad din organisation skal være opmærksom på, når certificeringskriterierne for certificeringsordningen skal udarbejdes. Afsnittet indeholder også en beskrivelse af Datatilsynets behandling og godkendelse af certificeringsordningens kriterier.

## 3.1 Generelt om Datatilsynets godkendelse af certificeringskriterier

Hvis en virksomhed eller en myndighed ønsker at tilbyde en certificeringsordning, er det et krav, at ordningens kriterier først er godkendt hos den kompetente tilsynsmyndighed i det EØS-land, hvor virksomheden eller myndigheden ønsker at tilbyde certificering. Hvis din organisation påtænker at udarbejde en certificeringsordning, som skal tilbydes i Danmark, skal certificeringsordningens kriterier således godkendes af Datatilsynet, som er den kompetente tilsynsmyndighed i Danmark.[16]

Herudover skal DANAK godkende, at certificeringsordningen lever op til kravene om akkrediteret certificering, som beskrevet under vejledningens afsnit 2[17]. Dette afsnit beskriver alene Datatilsynets vurdering og godkendelse af certificeringskriterierne.

EDPB har udarbejdet og vedtaget en vejledning om certificering og udarbejdelse af certificeringskriterier. Når du skal udarbejde kriterierne for den certificeringsordning, som din organisation ønsker at tilbyde, skal du være opmærksom på, at kriterierne skal følge denne vejledning for at kunne blive godkendt af Datatilsynet til brug for en certificeringsordning. Du bør derfor læse vejledningen grundigt, før du begynder at udarbejde kriterierne for certificeringsordningen.

## 3.2 Hvad kan en certificeringsordning omhandle?

Inden du påbegynder udarbejdelsen af dine certificeringskriterier, skal du finde ud af, hvad din certificeringsordning skal omhandle (dvs. certificeringsordningens anvendelsesområde).

16 Hvis din organisation bliver akkrediteret som certificeringsorgan i Danmark, og I også får godkendt jeres certificeringskriterier af Datatilsynet, vil I kunne udstede certificering inden for den pågældende ordning i Danmark. Hvis din organisationen også ønsker at tilbyde certificeringen i andre enkelte EØS-lande – men ikke vil tilbyde en fællescertificering, som gælder i hele EØS – skal certificeringsordningens kriterier også godkendes i de øvrige EØS-lande, hvor din organisation ønsker at tilbyde certificeringen.

17 Inden DANAK kan tildele akkreditering, skal DANAK evaluere certificeringsordningen. Evalueringen af ordningen skal sikre, at der kan udføres akkrediteret certificering efter ordningen. DANAK evaluerer certificeringsordninger efter de krav, som er fastsat af European Accreditation (EA) i proceduren EA-1/22 og DANAK's akkrediteringsbestemmelse AB 21. Læs mere herom i denne vejlednings afsnit 2.

Når du skal beslutte dig for, hvad din certificeringsordning skal omhandle, er det først og fremmest vigtigt at overveje, hvordan ordningen vil gavne det marked og de personer, kunder m.v., som bruger det produkt, den proces eller tjeneste, som certificeringen retter sig mod.

En certificeringsordnings anvendelsesområde kan enten være specifikt eller af mere generel karakter.

En specifik certificeringsordning kan eksempelvis være rettet mod en bestemt sektor i forhold til et bestemt type produkt eller en tjeneste, hvor certificeringskriterierne vil være rettet mod behandling af personoplysninger, som almindeligvis finder sted i det pågældende type produkt eller tjenesten.

En generel certificeringsordning kan være gældende for flere forskellige sektorer og finde anvendelse på en række forskellige behandlingsaktiviteter på tværs af forskellige typer af produkter, processer eller tjenester.

For at en certificeringsordning kan være realistisk og håndterbar, og for at den kan give en merværdi, er det dog vigtigt, at ordningens anvendelsesområde er begrænset på en eller anden måde.

En ordning med et generelt anvendelsesområde, som sigter mod at dække mange forskellige aspekter af databeskyttelsesforordningen, og som kan anvendes på adskillige former for behandlingsaktiviteter, skal således stadig være konkret nok til at kunne give en håndterbar og meningsfuld certificering.

Hvis du ønsker at tilbyde en certificeringsordning med et generelt anvendelsesområde, kan du overveje at afgrænse certificeringsordningens område på følgende måder:

- Ordningen dækker mange eller samtlige aspekter af databeskyttelsesforordningen, men retter sig alene mod et bestemt type produkt, en proces eller en tjeneste, eksempelvis lønsystemer eller netbanksløsninger.
- Ordningen finder anvendelse på en række forskellige behandlingsaktiviteter på tværs af forskellige produkter, processer eller tjenester, men dækker alene enkelte aspekter af databeskyttelsesforordningen (dvs. bestemmelser/artikler i forordningen), eksempelvis princippet om gennemsigtighed i databeskyttelsesforordningens artikel 5, stk. 1, litra a, eller brugen af automatiserede afgørelser i henhold til databeskyttelsesforordningens artikel 22.[18]

18 En ordning bør dække de artikler/bestemmelser i databeskyttelsesforordningen, som er relevante for ordningens kontekst. En certificeringsordning, der eksempelvis fokuserer på behandlingssikkerhed, behøver således ikke at dække artikler/bestemmelser, som ikke er relevante for netop dette anvendelsesområde.

## Generelle overvejelser, du bør gøre dig, når du skal fastlægge din certificeringsordnings anvendelsesområde

Når du skal fastlægge, hvad din certificeringsordning skal omhandle, bør du gøre dig nogle overvejelser om:

- Er der nogle generelle eller sektorspecifikke databeskyttelsesretlige problemstillinger, som du ønsker at løse via din certificeringsordning?
- Hvilke typer af organisationer vil efterspørge certificeringsordningen (henvender ordningen sig til en bestemt sektor eller en bestemt virksomhedstype som eksempelvis små- og mellemstore virksomheder?
- Hvordan vil ordningen gavne det marked, som du ønsker, at ordningen skal henvende sig til?
- Hvordan vil ordningen gavne de personer, kunder m.v., som bruger det produkt, den proces eller tjeneste, som certificeringsordningen omhandler? Hvor er det behov for øget tillid?
- Hvilke behandlingsaktiviteter vil kunne certificeres under certificeringsordningen? Retter certificeringsordningen sig mod en specifik type aktiviteter/behandlingsaktiviteter, som eksempelvis behandling af sundhedsjournaler, eller brugen af en bestemt teknologi, som eksempelvis cloud computing tjenester
- Hvordan skal ordningens certifikat eller mærke se ud? Hvordan vil certifikatet eller mærket sikre, at offentligheden let og hurtigt kan forstå, hvad der er certificeret, og hvad certificeringen betyder for dem?
- Hvad skal ordningens navn være? Afspejler ordningens navn ordningens anvendelsesområde, og vil det være forståeligt for offentligheden?

Det kan være en god idé at lave noget research inden for det marked, som du ønsker, at din certificeringsordning skal henvende sig til, for at sikre at ordningen imødekommer et aktuelt behov inden for det pågældende marked.

Resultaterne af disse overvejelser skal være afspejlet i certificeringsordningens kriterier.

## 3.3 Udarbejdelse af certificeringskriterier (kriteriekataloget)

### 3.3.1 Hvad er kravene til certificeringskriterierne?

Certificeringsordninger skal bidrage til at sikre en korrekt anvendelse af forordningens principper og regler ved at angive, hvordan de certificerede virksomheder og myndigheder skal håndtere behandlingen af personoplysninger i forhold til de specifikke behandlingsaktiviteter, som certificeringsordningen vedrører.

Certificeringsordningens kriterier skal således specificere den praktiske og sædvanlige anvendelse af de databeskyttelsesretlige regler i forhold til de behandlingsaktiviteter, som certificeringsordningen vedrører – og altså ikke blot gengive reglerne i databeskyttelsesforordningen. Med andre ord, så skal certificeringskriterierne tilføje en merværdi for de dataansvarlige/databehandlere, som certificeres, og være egnede til at forbedre disses overholdelse af de databeskyttelsesretlige regler.

Når du udarbejder certificeringskriterierne (dvs. kriteriekataloget) skal du som minimum tage de elementer, som er beskrevet i bilag 2 til EDPB's vejledning om certificering og udarbejdelse af certificeringskriterier, med i betragtning, og kriterierne skal således som minimum indeholde følgende afsnit (som alene skal ses som en kort opsummering af de forhold, som fremgår af bilaget til EDPB's vejledning):

1. Et indledende afsnit hvor baggrunden og motivation for certificeringsordningen beskrives, herunder hvordan ordningens kriterier vil forbedre overholdelsen af de databeskyttelsesretlige regler og gavne de registrerede.
2. En beskrivelse af hvad certificeringsordningen omhandler (certificeringsordningens anvendelsesområde og den potentielle 'genstand for certificering'[19]), herunder en beskrivelse af hvordan den potentielle genstand for certificering defineres.
3. Generelle afsnit:
    - Normative referencer (dvs. angivelse af de dokumenter, der er nødvendige for certificeringsordningen, eksempelvis relevant særlovgivning, relevante standarder eller tekniske beskrivelser).
    - Et afsnit vedrørende relevante termer og definitioner.
    - Et afsnit som definerer de databeskyttelsesretlige forpligtelser, procedure og behandlinger, der er omfattet af certificeringsordningens anvendelsesområde.
4. Kriterier som adresserer følgende forhold (i det omgang de er relevante for certificeringsordningen):[20]
    - Lovlig behandling af personoplysninger (artikel 6-10)
    - Principperne for behandling af personoplysninger (artikel 5)
    - Generelle forpligtelser for dataansvarlige og databehandlere (kapitel 4)
    - De registreredes rettigheder (artikel 12-23)
    - Anmeldelse af brud på persondatasikkerheden til Datatilsynet (artikel 33)
    - Databeskyttelse gennem design og standardindstillinger (artikel 25)
    - Vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder, herunder udarbejdelse af konsekvensanalyse (DPIA), hvor dette er påkrævet (artikel 35, stk. 7, litra d)
    - Tekniske og organisatoriske foranstaltninger, som skal sikre beskyttelse af de registreredes rettigheder og frihedsrettigheder, i forhold til den ovennævnte risikovurdering.
    - Tekniske og organisatoriske foranstaltninger, som skal sikre et passende sikkerhedsniveau i (artikel 32)
    - Andre elementer som øger databeskyttelsen
5. Kriterier som har til formål at påvise fornødne garantier i forbindelse med overførsel af personoplysninger til tredjelande (disse kriterier vil blive adresseret i den kommende vejledning fra EDPB om brug af certificeringsordninger og adfærdskodekser som overførselsgrundlag)
6. Supplerende kriterier for et Europæisk Databeskyttelsescertifikat, hvis dette er relevant.

Når du udarbejder dine certificeringskriterier, skal du (i forhold til de kriterier hvor det giver mening) beskrive, hvordan de enkelte kriterier skal gennemføres i praksis, og hvordan dem, der ønsker at blive certificeret, kan påvise over for certificeringsorganet, at de lever op til kriterierne. Se mere om evalueringsmetoder under afsnit 3.3.2 nedenfor.

Herudover skal certificeringsordningens territoriale område være tydeligt defineret i det materiale, som du sender til Datatilsynet sammen med kriterierne. Med andre ord skal det fremgå, i hvilke EØS-lande certificeringsordningen påtænkes udbudt, herunder om der er tale om en fællescertificering, som kan benyttes i alle EØS-lande. På den måde kan Datatilsynet tage

19 I den engelske udgave af EDPB's vejledninger om henholdsvis certificering og udarbejdelse af certificeringskriterier og akkreditering af certificeringsorganer anvendes begreberne 'object of certification' og 'target of evaluation', som forkortes 'ToE'.

20 En certificeringsordning kan være afgrænset til kun at omhandle enkelte aspekter af databeskyttelsesforordningen. Certificeringskriterierne skal således kun adressere de aspekter, som er relevante for den pågældende ordning. Se også pkt. 49 i EDPB's vejledning om certificeringsordninger.

stilling til, om tilsynet er den kompetente myndighed til at godkende kriterierne, og om kriterierne vil skulle godkendes af EDPB i tilfælde af, at der er tale om en fællescertificering.

Certificeringsordningens kriterier skal i øvrigt:

- være ensartede og verificerbare.
- være kontrollerbare (dvs. kriterierne skal specificere certificeringsordningens mål, og hvordan målene kan opnås for at påvise efterlevelse af reglerne).[21]
- være relevante for certificeringsordningens målgruppe.
- tage højde for og, hvor det er relevant, være anvendelige i sammenhæng med andre standarder, som eksempelvis ISO standarder, godkendte adfærdskodekser eller særlovgivning m.v.
- være fleksible og skalerbare til at kunne finde anvendelse for forskellige typer af behandlinger og organisationer.

Certificeringskriterier skal være pålidelige over tid, men samtidig kunne revideres, hvis der er behov herfor. Det vil eksempelvis være nødvendigt at revidere kriterierne, hvis de juridiske rammer (lovgrundlaget) ændrer sig, eller hvis der bliver afsagt EU-retlige domme, som kommer med en ny fortolkning af de bestemmelser, som certificeringsordningen omhandler. Det kan også være relevant at revidere kriterierne, hvis den tekniske standard har udviklet sig inden for det område, ordningen vedrører. Hvis kriterierne skal revideres, forudsætter det ny godkendelse hos Datatilsynet og EDPB. Læs mere om Datatilsynets og EDPB's godkendelse af kriterierne under vejledningens afsnit 3.4.2 og 3.5.

Du skal være opmærksom på, at ejeren af en certificeringsordning (typisk certificeringsorganet, men det kan også være en anden interessent) skal have procedurer på plads for håndtering af ændringer, der kan nødvendiggøre opdatering af certificeringskriterierne. Disse procedurer skal være en defineret del af certificeringsordningen. Idet Datatilsynet er ansvarlig for at gennemgå og godkende opdateringer af certificeringskriterierne, skal det sikres, at certificeringsordningens ejer kommunikerer enhver opdatering af certificeringskriterierne til tilsynet, herunder både større eller mindre opdateringer.

### 3.3.2 Særligt om evalueringsmetoder (kontrol- og testmetoder)

En certificeringsordning består som nævnt af en række certificeringskriterier, herunder evalueringsmetoder. Evalueringsmetoder er metoder, der beskriver, hvordan en evaluator vurderer, at den potentielle 'genstand for certificering'[22] (dvs. de behandlingsaktiviteter som potentielt kan være omfattet af ordningen) lever op til certificeringsordningens kriterier.

Når du sender dine certificeringskriterier til godkendelse hos Datatilsynet, skal du medsende en beskrivelse af evalueringsmetoderne, så vi hos tilsynet kan tage et kig på, om de beskrevne metoder er effektive til at udføre vurderingen af, om de virksomheder eller myndigheder, der har ansøgt om at blive certificeret, lever op til certificeringskriterierne. Dette dokument skal beskrive den mest hensigtsmæssige tilgang til at kontrollere efterlevelse af de enkelte kriterier.

Evalueringsmetoderne må dog ikke tilføje ekstra elementer til certificeringskriterierne, ligesom de heller ikke må være for detaljerede om, hvordan kriterierne skal være implementeret hos de virksomheder eller myndigheder, der har ansøgt om at blive certificeret. Det skal nemlig

21 En evaluator skal være i stand til at kunne kontrollere, om certificeringsordningens kriterier er overholdt eller ej, og det skal sikres, at der kan foretages ensartede og gentagelige evalueringer af de samme kriterier. Evaluatoren er den part, som står for at kontrollere certificeringskundernes efterlevelse af certificeringsordningen, og vil typisk være certificeringsorganet selv, medmindre certificeringsorganet har uddelegeret evalueringsopgaven til en anden part

22 I den engelske udgave af EDPB's vejledninger om henholdsvis certificering og udarbejdelse af certificeringskriterier og akkreditering af certificeringsorganer anvendes begreberne 'object of certification' og 'target of evaluation', som forkortes 'ToE'.

stadig være muligt for virksomhederne og myndighederne at implementere foranstaltninger til efterlevelse af kriterierne, som passer til deres eget miljø.

Du skal være opmærksom på, at ISO/IEC 17065:2012 og de supplerende akkrediteringskrav for certificeringsorganer, som Datatilsynet har udarbejdet, indeholder en række krav til evalueringsmetoderne, som vil blive vurderet af DANAK i forbindelse med akkrediteringsprocessen.

### 3.3.3 Brug af certifikater eller mærker m.v.

Når din certificeringsordning indeholder et certifikat og eventuelt et mærke, som kan bruges af dataansvarlige eller databehandlere til at signalere, at de lever op til certificeringsordningens kriterier, skal du være opmærksom på, at certifikatets eller mærkets design og navn skal kunne hjælpe offentligheden med at forstå betydningen af certificeringen, hvor det er muligt.

For eksempel vil en "Heath Privacy" certificering indikere til offentligheden, at certificeringsordningen omhandler beskyttelse af de registreredes helbredsoplysninger. Derfor vil certificeringskriterierne for denne ordning også skulle være tilstrækkelige til at kunne vurdere efterlevelsen af reglerne i den sammenhæng.

Når du sender dine kriterier til godkendelse hos Datatilsynet, vil tilsynet tage et kig på certificeringsordningens navn og certifikatets/mærkets design med sine databeskyttelsesretlige briller på for at sikre, at navnet eller designet ikke er misvisende i forhold til kriteriernes anvendelsesområde og den potentielle genstand for certificering.

Du skal også være opmærksom på, at ISO/IEC 17065:2012 indeholder nogle specifikke krav vedrørende brug af- og kontrol med certifikater/mærker, som skal være afspejlet i udformningen af certificeringsordningen. DANAK vil vurdere, om disse krav er opfyldt.

### 3.3.4 Bør vi teste vores certificeringsordning?

Du bør overveje at teste din certificeringsordning over for en række frivillige organisationer m.fl., da det kan hjælpe dig med at sikre, at certificeringsordningen kan bruges til det tiltænkte formål.

## 3.4 Hvordan kan Datatilsynet hjælpe?

Udarbejdelse af en certificeringsordning kan være en svær og omfattende proces. Datatilsynet bistår derfor gerne med vejledning i form af mødedeltagelse og lignende til organer, der overvejer at udarbejde en certificeringsordning.

Du er velkommen til at kontakte Datatilsynet på dt@datatilsynet.dk.

### 3.4.1 Hvilke dokumenter skal vi sende til Datatilsynet?

Inden din organisation akkrediteres hos DANAK, skal kriterierne for den certificeringsordning, som din organisation ønsker at tilbyde, godkendes af Datatilsynet.

Når du er klar til at sende dine certificeringskriterier til godkendelse hos Datatilsynet, bedes du medsende følgende dokumenter:

- En udfyldt ansøgningsblanket med relevante bilag.
- En kopi af certificeringsordningens certifikat/mærke, som kan bruges af dataansvarlige eller databehandlere til at signalere, at de lever op til certificeringsordningens kriterier, hvis dette er relevant for ordningen.
- Et kriteriekatalog, som beskriver certificeringsordningens kriterier, og som tager højde for de elementer, som er beskrevet under denne vejlednings afsnit 3.
- Et dokument, der beskriver, hvordan det vurderes, at den potentielle 'genstand for certificering' (dvs. de behandlingsaktiviteter som potentielt kan være omfattet af ordningen) lever op til certificeringsordningens kriterier (se mere om evalueringsmetoder under afsnit 3.3.2. oven for).
- En såkaldt "use case" (dvs. et eksempel fra virkeligheden eller et teoretisk eksempel), som demonstrerer, hvordan certificeringskriterierne kan anvendes i praksis.
- Detaljer af eventuel research, som du har udført i forbindelse med udviklingen af dine certificeringskriterier eller din certificeringsordning, jf. denne vejlednings afsnit 3.2.

- Resultaterne af eventuelle tests, som du har udført, jf. denne vejlednings afsnit 3.3.4.

Som led i godkendelsen af kriterierne er Datatilsynet forpligtet til at sende sit udkast til afgørelse til EDPB, så EDPB kan komme med en udtalelse vedrørende denne. Med henblik på at lette arbejdet i den forbindelse, bedes du også sende ovennævnte dokumenter på engelsk til Datatilsynet. Du kan læse mere om EDPB's udtalelse til Datatilsynets udkast til afgørelse vedr. godkendelse af certificeringskriterierne under vejledningens afsnit 3.5.

### 3.4.2 Hvordan vil Datatilsynet vurdere og godkende certificeringskriterierne?

EDPB's vejledning om certificering og udarbejdelse af certificeringskriterier, herunder særligt vejledningens bilag 2, indeholder retningslinjer for Datatilsynets – og EDPB's hvis der er tale en fælles certificering (Den Europæiske Databeskyttelsesmærkning) – gennemgang og vurdering af certificeringskriterier, når tilsynet skal tage stilling til, om certificeringskriterier kan godkendes.

I sidste ende vil Datatilsynets godkendelse af kriterierne afhænge af, om certificeringsordningen, herunder kriterierne, vil være egnet til at forbedre overholdelsen af databeskyttelsesreglerne hos de relevante dataansvarlige og databehandlere, og om certificeringen vil medføre en fordel for de registreredes tryghed i forhold til behandlingen af deres personoplysninger.

I forbindelse med vurderingen af certificeringsordningens kriterier kan det være, at Datatilsynet indkalder til et møde med henblik på uddybende drøftelser omkring kriteriernes indhold.

Hvis Datatilsynet kommer frem til, at certificeringsordningens kriterier ikke kan godkendes i den foreliggende form, vil tilsynet sende en udtalelse til certificeringsordningens ejer, hvori tilsynet vil redegøre for, hvorfor kriterierne ikke vil kunne godkendes.

Certificeringsordningens ejer har herefter mulighed for at sende et revideret udkast til Datatilsynet med henblik på, at tilsynet tager stilling til kriterierne på ny.

Når certificeringsordningens ejer har foretaget alle nødvendige ændringer, og kriterierne efter Datatilsynets vurdering opfylder kravene, laver tilsynet et udkast til en afgørelse vedrørende godkendelse af kriterierne, som forelægges EDPB, jf. afsnit 3.5.

## 3.5 Det Europæiske Databeskyttelsesråds udtalelse til Datatilsynets udkast til afgørelse vedr. godkendelse af certificeringskriterierne

For at sikre ensartethed på tværs af EØS i forhold til udarbejdelse af databeskyttelsesretlige certificeringsordninger er Datatilsynet forpligtet til at sende tilsynets udkast til afgørelse vedrørende godkendelse af certificeringskriterierne til EDPB, hvorefter EDPB vil komme med en udtalelse vedrørende udkastet til afgørelsen[23].

Ifølge EDPB's procedureregler[24] vil rådet komme med en udtalelse til Datatilsynets udkast inden for 8-14 uger fra, at tilsynet har sendt udkastet til rådet.

EDPB anbefaler dog, at tilsynsmyndighederne – før udkastet til afgørelsen vedrørende godkendelsen af kriterierne sendes til EDPB – deltager i nogle uformelle møder (såkaldte certificeringssessioner) med de øvrige EØS-lande med henblik på at drøfte certificeringsordningens kriterier. Selvom dette medfører en længere godkendelsesproces, giver det Datatilsynet en god mulighed for at få feedback på kriterierne fra de andre EØS-lande, ligesom det giver mulighed for, at certificeringsordningens ejer kan foretage eventuelle nødvendige ændringer i ordningen, inden udkastet til afgørelse sendes til EDPB.

Når først udkastet til afgørelsen er sendt til EDPB, vil der ikke længere være mulighed for at foretage ændringer i certificeringsordningen, før EDPB har afgivet en udtalelse til udkastet. På

23 Jf. databeskyttelsesforordningens artikel 64, stk. 1, litra c, og artikel 64, stk. 7

24 EDPB rules of procedure version 7: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/rules-procedure_en

den måde er den uformelle proces også med til at sikre et positivt resultat for certificeringsordningen.

## 3.6 Hvordan vil folk vide, at vores certificeringskriterier er blevet godkendt?

Når certificeringskriterierne er endeligt godkendt af Datatilsynet, vil de blive offentliggjort på tilsynets hjemmeside og i EDPB's register over godkendte certificeringsordninger på rådets hjemmeside.

Det bemærkes i den forbindelse, at det er et krav, at certificeringskriterierne gøres offentligt tilgængelige[25].

25 Jf. databeskyttelsesforordningens artikel 43, stk. 6, som foreskriver, at tilsynsmyndighederne skal offentliggøre certificeringskriterierne i lettilgængelig form.

# 4. Hvordan kan man blive certificeret?

Dette afsnit henvender sig til myndigheder og virksomheder, som overvejer at blive certificeret. Her kan du blandt andet læse om, hvordan din organisation kan blive certificeret, og hvilke overvejelser din organisationer bør gøre sig, inden der ansøges om certificering hos et certificeringsorgan.

## 4.1 Hvordan bliver vi certificeret?

På nuværende tidspunkt foreligger der ingen godkendte certificeringsordninger på hverken dansk eller europæisk niveau. Når Datatilsynet godkender de første certificeringskriterier, vil det blive offentliggjort på tilsynets hjemmeside.

Certificeringer udstedes af certificeringsorganer, som er blevet akkrediteret af DANAK i forhold til de pågældende certificeringsordninger. Hvis din organisation ønsker at blive certificeret inden for en godkendt certificeringsordning, skal organisationen ansøge om certificering hos det/de certificeringsorganer, der udbyder den pågældende certificeringsordning. Certificeringsorganet vil herefter vurdere, om din organisation lever op til certificeringsordningens kriterier.

Hvis din organisation er interesseret i at ansøge om certificering, skal du gøre følgende:

- **Find en certificeringsordning** – Du skal finde en certificeringsordning, der passer til organisationens behov i forhold til det produkt eller den tjeneste eller proces, som ønskes certificeret, og som passer til organisationens karakter.
- **Find et certificeringsorgan** – Du skal finde et akkrediteret certificeringsorgan, der udbyder en certificeringsordning, som passer til din organisations behov. Din organisation vil skulle ansøge om certificering direkte hos det relevante certificeringsorgan. Du kan finde en oversigt over akkrediterede certificeringsorganer på DANAK's hjemmeside.
- **Find ud af hvilket produkt eller hvilken proces eller tjeneste, du gerne vil have certificeret** – Certificering efter databeskyttelsesforordningen kan anvendes til en bestemt behandling af personoplysninger (dvs. behandlingsaktiviteter) indeholdt i et produkt, en proces eller en tjeneste.
- **Få et overblik over de behandlingsaktiviteter, der er indeholdt i det produkt eller den proces eller tjeneste, som du ønsker certificeret** – Du skal kortlægge de behandlingsaktiviteter, der er knyttet til det produkt eller den proces eller tjeneste, som du ønsker certificeret. Det skyldes, at du skal fastslå, hvilke specifikke behandlingsaktiviteter, der skal være omfattet af certificeringen. Dette kaldes 'genstanden for certificering'.[26]

## 4.2 Hvad skal vi vide, før vi ansøger om certificering?

Inden din organisation ansøger et certificeringsorgan om at blive certificeret, bør I bl.a. være opmærksomme på følgende forhold:

26 I den engelske udgave af EDPB's vejledninger om henholdsvis certificering og udarbejdelse af certificeringskriterier og akkreditering af certificeringsorganer anvendes begreberne 'object of certification' og 'target of evaluation', som forkortes 'ToE'.

- I forbindelse med ansøgningsprocessen vil din organisation være forpligtet til at oplyse certificeringsorganet om eventuelle afgørelser og reaktioner, som din organisation har modtaget fra Datatilsynet eller andre tilsynsmyndigheder, hvis disse vedrører behandling af personoplysninger, som er relateret til certificeringsordningens anvendelsesområde og genstanden for certificering (dvs. de behandlingsaktiviteter som er omfattet af certificeringsordningen). Certificeringsorganet vil få bekræftet oplysningerne hos tilsynet, hvor dette er hensigtsmæssigt. Hvis certificeringsorganet bliver bekendt med, at din organisation ikke har oplyst certificeringsorganet om afgørelser og reaktioner fra Datatilsynet m.v., kan det resultere i, at din organisation ikke kan blive certificeret.[27]
- Efter din organisation er blevet certificeret, vil din organisation være forpligtet til at underrette certificeringsorganet om eventuelle ændringer, der kan påvirke certificeringen. Hvis din organisation eksempelvis har et brud på persondatasikkerheden, som vedrører områder inden for certificeringen, vil organisationen således være forpligtet til at underrette certificeringsorganet om bruddet, så certificeringsorganet kan vurdere, om organisationen fortsat opfylder certificeringsordningens kriterier.[28]
- Hvis Datatilsynet bliver bekendt med et problem i forhold til din organisations efterlevelse af databeskyttelsesreglerne, som vil kunne påvirke din organisations certificering, kan det være, at tilsynet underretter certificeringsorganet herom, hvorefter certificeringsorganet vil være forpligtet til at vurdere, om din organisation fortsat opfylder certificeringsordningens kriterier.
- Hvis det vurderes, at din organisation ikke længere lever op til certificeringsordningens kriterier, kan din organisations certificering blive trukket tilbage.

Certificeringsorganet er forpligtet til at oplyse om certificeringsbetingelser og certificeringsprocessen. Du kan læse om kravene til det akkrediterede certificeringsorgan på DANAK's hjemmeside.

## 4.3 Hvad koster det at blive certificeret?

Du skal kontakte det relevante certificeringsorgan for at finde ud af, hvor meget det vil koste for din organisation at blive certificeret. Certificeringsorganer opkræver normalt et beløb ud fra en bestemt sats for at foretage certificeringsvurderingen. Omkostningerne for certificering kan derfor afhænge af bl.a. størrelsen på din organisation og omfanget og kompleksiteten af de behandlingsaktiviteter, som certificeringsorganet skal vurdere i henhold til certificeringskriterierne.

## 4.4 Hvordan vil folk vide, at vores produkt, proces eller tjeneste er certificeret?

Når certificeringsorganet har vurderet, at din organisation lever op til ordningens kriterier m.v., vil certificeringsorganet udstede et certifikat til dig. Certifikatet vil erklære, hvilke specifikke behandlingsaktiviteter i dit produkt eller din proces eller tjeneste, som er dækket af certificering, ligesom det vil fremgå af certifikatet, hvor længe certificeringen er gyldig.

Når din organisation har opnået certificering, vil I formentlig – alt efter certificeringsordningens bestemmelser – kunne fremvise et mærke eller logo, som demonstrerer, at organisationen er bedømt efter de krav og kriterier, som er indeholdt i certificeringsordningen.

Certificeringsorganet er forpligtet til at føre en offentlig oversigt over de myndigheder eller virksomheder, som certificeringsorganet har udstedt databeskyttelsesretlige certificeringer til.[29]

27 Du kan læse mere herom under pkt. 7.2 i Datatilsynets supplerende akkrediteringskrav
28 Du kan læse mere herom under pkt. 7.10 i Datatilsynets supplerende akkrediteringskrav.
29 Se pkt. 4.6 og 7.8 i Datatilsynets supplerende akkrediteringskrav

Certificeringsorganet skal også offentliggøre et resumé af de evalueringsrapporter, som udarbejdes for hver certificering. Dette resumé indeholder en beskrivelse af følgende:

- Certificeringsordningens anvendelsesområde og genstanden for certificering (dvs. hvilke behandlingsaktiviteter der certificeres).
- Certificeringsordningens kriterier.
- Certificeringsorganets evalueringsmetoder (dvs. hvordan certificeringsorganet vurderer, at en virksomhed eller myndighed lever op til ordningens kriterier m.v.).
- Kontroller/tests/audits, som certificeringsorganet har gennemført, og resultaterne af disse.

Certificeringsorganet sender også dette resumé til Datatilsynet, før de udsteder certificeringen.

**Vejledning**


Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

**Datatilsynet**
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk