## Baggrund

I forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)[1] samt den supplerende danske databeskyttelseslov[2], tilskyndes medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen til fastlæggelse af certificeringsmekanismer (i vores termer certificeringsordninger) for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder denne forordning.

Persondataforordningen angiver at godkendte certificeringer kan anvendes som retningslinjer til den dataansvarlige eller databehandleren om implementering af passende foranstaltninger og som et led i påvisning af vedkommendes overholdelse af forordningen, navnlig for så vidt angår identificering af risikoen i forbindelse med behandlingen, deres vurdering med hensyn til risikoens oprindelse, karakter, sandsynlighed og alvor og om identificering af bedste praksis med henblik på at begrænse denne risiko.

En godkendt certificeringsmekanisme kan desuden bruges som et element til at påvise, at den dataansvarlige overholder sine forpligtelser i forbindelse med behandling, der foretages af en ekstern databehandler på vegne af den dataansvarlige.

Datatilsynet har udgivet en vejledning[3] om adfærdskodekser og certificeringsordninger, der giver eksempler på brug af certificeringsmekanismer.

## Godkendelse af certificeringsordning

Inden akkreditering skal den specifikke certificeringsordning godkendes af Datatilsynet. Datatilsynet vil ved godkendelsen vurdere, i hvilket omfang certificeringsordningen kan anvendes til at påvise overholdelse af databeskyttelsesforordningen (EU) 2016/679. Certificering skal iht. forordningen være under akkreditering til ISO/IEC 17065.

Ved ansøgning om godkendelse skal følgende sendes til Datatilsynet:

- Entydig identifikation og beskrivelse af certificeringsordningen, herunder kriterierne.
- Angivelse af hvilke behandlingsaktiviteter certificeringen omfatter.
- Angivelse af hvilke krav certificeringen kan blive brugt som et element til at påvise overholdelse af.
- Angivelse af hvilken type og størrelse virksomhed kriterierne kan anvendes på.
- Erklæring om, at ejeren af certificeringsordningen er bekendt med, at kriterierne efter godkendelse vil blive offentliggjort af Databeskyttelsesrådet.
- Certificeringen skal indeholde en bestemmelse, som erklærer, at certificeringen overholder artikel 42 stk. 4 i databeskyttelsesforordningen.
- Beskrivelse af hvordan certificeringen medfører en klar og tydelig fordel for:
    - dataansvarliges/databehandleres påvisning af overholdelse af databeskyttelsesforordningen;

[1] http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016R0679&from=DA
[2] http://www.ft.dk/samling/20171/lovforslag/l68/index.htm
[3] https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_adfaerdskodekser_og_certificeringsordninger__som_offentliggjort_II_.pdf

- de registreredes tryghed ved at behandlingen af deres personoplysninger overholder databeskyttelsesforordningen.

Datatilsynet vil på baggrund heraf vurdere, om certificeringsordningen sikrer opfyldelse af forordningens krav under de givne betingelser. Er der tale om en certificeringsordning, der gælder i alle EU-lande, skal certificeringsordningen godkendes af Databeskyttelsesrådet. Datatilsynet står i den forbindelse for formidlingen til Databeskyttelsesrådet.

Som alternativ hertil kan der, når de bliver udarbejdet, anvendes kriterier godkendt af Databeskyttelsesrådet.

Certificering udstedes for en periode på højst 3 år.

Spørgsmål vedrørende krav til certificeringsordning kan rettes til Datatilsynet.

DANAK vil desuden vurdere om ordningen opfylder kravene til akkreditering ift. akkrediteringsstandard, sikring af entydige resultater m.v. ud fra krav i ISO/IEC 17011:2017 og EA-1/22 A.

**Akkrediteringskrav**

Certificeringsorganet skal være akkrediteret i overensstemmelse med ISO/IEC 17065:2012 og med de supplerende krav, der er fastsat af Datatilsynet.

Certificeringsorganet skal ifølge forordning (EU) 2016/679 have følgende, der helt eller delvist dækkes af krav i ISO/IEC 17065:2012:

- Et passende ekspertiseniveau for så vidt angår databeskyttelse.
- Påvist sin uafhængighed og ekspertise med hensyn til certificeringens genstand.
- 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.
- Fastlagt procedurer for udstedelse, regelmæssig revision og tilbagetrækning af databeskyttelsescertificeringer, -mærkninger og –mærker.
- 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.
- Sikret at dens opgaver og pligter ikke fører til en interessekonflikt.

Akkrediteringen udstedes for en periode på 4 år jfr. DANAK's Akkrediteringsbestemmelse AB 1.

Certificeringsorganet skal i henhold til databeskyttelsesforordningens artikel 43 punkt 5 give Datatilsynet oplysninger om begrundelsen for at udstede eller tilbagetrække en certificering, der er anmodet om, og sikre sig aftaler med kunderne herom.

Certificeringsorganet skal trække et certifikat tilbage, hvis det bliver pålagt af Datatilsynet.

Akkreditering af certificeringsorganer finder sted på grundlag af kriterier, der er godkendt af Datatilsynet. Disse krav supplerer kravene i forordning (EF) nr. 765/2008 (i praksis ISO/IEC 17065:2012) og de tekniske

regler, der beskriver krav til certificeringsorganer. Der er i øjeblikket ikke fastlagt supplerende krav, ud over de i forordningen angivne og ovenfor refererede.

**Område for certificeringen**

En godkendt certificeringsordning kan blive brugt som et element til at påvise overholdelse af bestemmelserne i databeskyttelsesforordningen, herunder:

- Artikel 24 Den dataansvarliges ansvar;
- Artikel 25 Databeskyttelse gennem design og standardindstillinger;
- Artikel 28 Databehandler stk. 1 og 4;
- Artikel 32 Behandlingssikkerhed stk. 1.

Certificeringsområdet skal omfatte følgende:

- en entydig identifikation af certificeringsordningen;
- hvilke behandlingsaktiviteter certificeringen omfatter;
- hvilke krav certificeringen kan blive brugt som et element til at påvise overholdelse af (f.eks. relevant artikel i databeskyttelsesforordningen);
- erklæring fra certificeringsorganet om, at certificeringen ikke strider mod dansk lovgivning;
- erklæring fra certificeringsorganet om, at certificeringen er i overensstemmelse med principperne i databeskyttelsesforordningen;
- en beskrivelse af hvordan certificeringen medfører en klar og tydelig fordel for:
    - dataansvarliges/databehandleres påvisning af overholdelse af databeskyttelsesforordningen;
    - de registreredes tryghed ved at behandlingen af deres personoplysninger overholder databeskyttelsesforordningen.

**Ansøgning om akkreditering**

Ansøgning om akkreditering foretages vha. DANAKs ansøgningsblanket. Ansøgningen skal, ud over det i ansøgningsblanketten angivne, vedlægges dokumentation for certificeringsordningen og godkendelse fra Datatilsynet heraf.

Hvis hensigtsmæssigt kan behandlingen af akkrediteringsansøgningen efter aftale foretages parallelt med Datatilsynets behandling, idet akkreditering dog ikke kan udstedes, før Datatilsynet har godkendt ordningen.