Datatilsynets supplerende akkrediteringskrav for certificeringsorganer

Marts 2021

DATATILSYNET

Indhold

Forord

Det følger af databeskyttelseslovens § 25, at både Datatilsynet og den danske akkrediteringsfond (DANAK) er bemyndiget til at akkreditere certificeringsorganer efter databeskyttelsesforordningens artikel 43, stk. 1, litra a og b.

I praksis vil det dog være DANAK, der har ansvaret for at akkreditere certificeringsorganer, idet DANAK har stor erfaring med at foretage akkreditering på andre områder. Det er derfor DANAK, som en virksomhed (eller en offentlig myndighed) skal tage kontakt til, hvis de ønsker at blive akkrediteret som certificeringsorgan.

Vilkårene for samarbejdet mellem Datatilsynet og DANAK som det danske nationale akkrediteringsorgan er beskrevet nærmere i en akkrediteringsmeddelelse, som er udarbejdet af Datatilsynet og DANAK. Akkrediteringsmeddelelsen beskriver roller, ansvar og fremgangsmåden i forhold til akkreditering af certificeringsorganer efter databeskyttelsesforordningen. Akkrediteringsmeddelelsen kan tilgås via Datatilsynets og DANAK's hjemmeside.

Hvis Datatilsynet på et tidspunkt beslutter sig for at bruge sin bemyndigelse til at foretage akkreditering i henhold til databeskyttelseslovens § 25, vil tilsynet akkreditere certificeringsorganer i overensstemmelse med ISO 17065 og disse supplerende akkrediteringskrav med de nødvendige tilpasninger. Nødvendige tilpasninger vil i den forbindelse primært bestå i at henvise til Datatilsynet de steder, hvor de supplerende krav på nuværende tidspunkt henviser til akkrediteringsorganet.

1. Anvendelsesområde

Dette dokument indeholder supplerende krav til ISO 17065 til brug for vurdering af certificeringsorganers kompetence, pålidelige drift og upartiskhed.

Anvendelsesområdet for ISO 17065 finder anvendelse i overensstemmelse med databeskyttelsesforordningen. For yderligere information henvises til Det Europæiske Databeskyttelsesråds (EDPB) vejledninger om akkreditering[1] og certificering[2].

Det brede anvendelsesområde for ISO 17065, som dækker produkter, processer og tjenester, sænker eller tilsidesætter ikke kravene i databeskyttelsesforordningen. Certificering skal således vedrøre behandlingsaktiviteter. Selvom et styringssystem (eksempelvis et informationssikkerhedsstyringssystem[3]) kan indgå som en del af en certificeringsmekanisme, kan det ikke være det eneste element i en certificeringsmekanisme, idet certificeringen skal omfatte behandling af personoplysninger.

Anvendelsesområdet for en certificeringsmekanisme (eksempelvis certificering af behandlingsaktiviteter i en cloudtjeneste) skal tages i betragtning i forbindelse med akkrediteringsorganets vurdering under akkrediteringsprocessen, især med hensyn til kriterier, ekspertise og evalueringsmetode.

Endelig kan databeskyttelsescertificering efter databeskyttelsesforordningens artikel 42, stk. 1, kun udstedes i forhold til behandlingsaktiviteter, der udføres af dataansvarlige og databehandlere.

1 Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
2 Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation
[3] Privacy Information Management System (PIMS), som beskrevet I ISO/IEC 27701

2. Normative referencer

Databeskyttelsesforordningen har forrang frem for ISO 17065. Hvis der i de supplerende akkrediteringskrav eller i forbindelse med en certificeringsmekanisme henvises til andre ISO-standarder, skal disse fortolkes i overensstemmelse med kravene i databeskyttelsesforordningen.

3. Relevante begreber og definitioner

Vilkårene og definitionerne i EDPB's vejledninger om akkreditering og certificering finder anvendelse og har forrang frem for ISO-definitioner. For at lette henvisningen er de vigtigste definitioner, der anvendes i dette dokument, anført nedenfor.

Databeskyttelsesforordningen: 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 om ophævelse af direktiv 95/46/EF.

Databeskyttelsesloven: Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Vejledning om akkreditering: EDPB's vejledning om akkreditering af certificeringsorganer (Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR (2016/679))

Vejledning om certificering: EDPB's vejledning om certificering og udarbejdelse af certificeringskriterier (Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR)

ISO 17065: ISO/IEC 17065/2012

Certificering: Et certificeringsorgans uvildige vurdering af og attestering for, at behandlingsaktiviteter, som udføres af en dataansvarlig eller databehandler, opfylder et sæt foruddefinerede certificeringskriterier.

Akkreditering: Et nationalt akkrediteringsorgans og/eller en kompetent tilsynsmyndigheds attestering for, at et certificeringsorgan er kvalificeret til at foretage certificering i henhold til databeskyttelsesforordningens artikel 42 og artikel 43 under hensyntagen til ISO 17065 og de supplerende akkrediteringskrav, som er fastsat af den kompetente tilsynsmyndighed eller af EDPB. For yderligere information om fortolkningen af akkreditering efter forordningens artikel 43 henvises til afsnit 3 i EDPB's vejledning om akkreditering.

Det nationale akkrediteringsorgan: Det eneste organ i en medlemsstat, som er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008, og som foretager akkreditering med bemyndigelse fra staten. I Danmark er det nationale akkrediteringsorgan den danske akkrediteringsfond (DANAK).

Akkrediteringsorgan: Et organ, som foretager akkreditering. I dette dokument forstås begrebet som DANAK. Hvis Datatilsynet på et tidspunkt beslutter sig for at gøre brug af sin bemyndigelse til at foretage akkreditering i overensstemmelse med databeskyttelseslovens § 25, skal begrebet forstås som Datatilsynet.

Certificeringsorgan: Et tredjeparts overensstemmelsesvurderingsorgan, der anvender en certificeringsordning.

Certificeringskriterier: De kriterier, som en organisations behandlingsaktiviteter vurderes i forhold til i en certificeringsordning.

Certificeringsordning: Et certificeringssystem som vedrører specifikke produkter, processer eller tjenester, der er omfattet af samme specifikke krav, regler og procedurer. En certificeringsordning består af certificeringskriterier og vurderingsmetode.

Certificeringsmekanisme: En godkendt certificeringsordning, som er tilgængelig for ansøgeren. Det er en service, som tilbydes af et akkrediteret certificeringsorgan, og som er baseret på godkendte certificeringskriterier og vurderingsmetode. Det er gennem denne mekanisme, at en dataansvarlig eller databehandler bliver certificeret.

Kompetent tilsynsmyndighed: Hvor der henvises til den kompetente tilsynsmyndighed i dette dokument, vil det betyde Datatilsynet.

Genstand for certificering: Når det omhandler certificering efter databeskyttelsesforordningen, vil genstanden for certificering være de behandlingsaktiviteter, som den dataansvarlige eller databehandleren ønsker at få vurderet og certificeret.

Ansøger: Den organisation, som har anmodet om at få sine behandlingsaktiviteter certificeret.

Kunde[4]**:** Den organisation, som er blevet certificeret (tidligere ansøgeren).

[4] Når begrebet 'kunde' bruges i den Internationale Standard (ISO/IEC 17065/2012), dækker det bade over 'ansøger' og 'kunde', medmindre andet fremgår.

4. Generelle krav til akkreditering

4.1 Juridiske og kontraktmæssige forhold

4.1.1 Retligt ansvar

Et certificeringsorgan skal (til enhver tid) være i stand til at kunne påvise over for akkrediteringsorganet, at det har tidssvarende procedurer, som demonstrerer efterlevelse af det retlige ansvar, som er fastsat i akkrediteringsbetingelserne, herunder de supplerende akkrediteringskrav i forhold til anvendelsen af databeskyttelsesforordningen.

Certificeringsorganet skal kunne påvise, at dets procedurer og foranstaltninger vedrørende styring og håndtering af ansøger- og kundeorganisationers personoplysninger som en del af certificeringsprocessen overholder reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Certificeringsorganet skal således kunne fremlægge dokumentation for efterlevelse af reglerne som krævet under akkrediteringsprocessen.

Dette indebærer blandt andet, at certificeringsorganet skal bekræfte over for akkrediteringsorganet, at certificeringsorganet ikke er – eller tidligere har været – genstand for undersøgelser eller afgørelser fra Datatilsynet, som kan betyde, at certificeringsorganet muligvis ikke opfylder dette krav og dermed kan forhindre akkreditering. Inden akkrediteringsprocessen fortsætter, vil akkrediteringsorganet kontakte Datatilsynet for at få bekræftet disse oplysninger. Datatilsynet vil herefter bekræfte oplysningerne, hvor det er hensigtsmæssigt.

Certificeringsorganet skal også bekræfte over for akkrediteringsorganet, at certificeringsorganet ikke er – eller tidligere har været – genstand for undersøgelser eller afgørelser fra andre tilsynsmyndigheder, som vedrører behandling af personoplysninger, og som kan betyde, at certificeringsorganet muligvis ikke opfylder dette krav og dermed kan forhindre akkreditering.

Certificeringsorganet skal straks oplyse akkrediteringsorganet om relevante overtrædelser af databeskyttelsesforordningen eller databeskyttelsesloven, som er fastslået af Datatilsynet, andre tilsynsmyndigheder eller kompetente retslige myndigheder, og som kan have betydning for certificeringsorganets akkreditering.

Før certificeringsorganet udsteder eller fornyer certificeringer, skal det kræves, at certificeringsorganet underrette Datatilsynet i medfør af databeskyttelsesforordningens artikel 43, stk. 1.

Datatilsynet kan beslutte at fastsætte yderligere krav og procedurer med henblik på kontrol af certificeringsorganers efterlevelse af databeskyttelsesreglerne forud for akkreditering.

4.1.2 Certificeringsaftale

Certificeringsorganet skal ud over kravene I ISO 17065 påvise, at dets certificeringsaftaler:

1. kræver, at ansøgeren altid overholder både de generelle certificeringskrav som defineret under punkt 4.1.2.2 (a) i ISO 17065 og de certificeringskriterier, som er godkendt af Datatilsynet eller EDPB i medfør af databeskyttelsesforordningens artikel 43, stk. 2, litra b, og artikel 42, stk. 5,

2. kræver, at ansøgeren tillader Datatilsynet fuld indsigt/gennemsigtighed i certificeringsproceduren, herunder også materiale, som er fortroligt ifølge kontrakt eller ved lov, vedrørende overholdelse af databeskyttelsesreglerne i henhold til tilsynets opgaver efter databeskyttelsesforordningens artikel 42, stk. 7, og artikel 58, stk. 1, litra c,

3. ikke reducerer ansøgerens ansvar for efterlevelse af databeskyttelsesforordningen og ikke påvirker opgaverne og beføjelserne hos de tilsynsmyndigheder, som er kompetente i henhold til databeskyttelsesforordningens artikel 42, stk. 5,

4. kræver, at ansøgeren giver certificeringssorganet alle oplysninger om og adgang til de behandlingsaktiviteter, der er nødvendige for at gennemføre certificeringsproceduren i overensstemmelse med databeskyttelsesforordningens artikel 42, stk. 6,

5. kræver, at ansøgeren overholder de gældende frister og procedurer. Certificeringsaftalen skal fastsætte, at frister og procedurer, som følger af eksempelvis certificeringsprogrammet eller andre bestemmelser, skal iagttages og overholdes,

6. med henvisning til punkt 4.1.2.2. (c) (1) i ISO 17065 fastsætter regler vedrørende gyldighed, fornyelse og tilbagetrækning efter databeskyttelsesforordningens artikel 42, stk. 7, og artikel 43, stk. 4, herunder regler som fastsætter passende intervaller for reevaluering eller overvågning (regelmæssighed) i overensstemmelse med databeskyttelsesforordningens artikel 42, stk. 7 og afsnit 7.9 i disse supplerende akkrediteringskrav,

7. giver certificeringsorganet mulighed for at fremlægge alle oplysninger til Datatilsynet, som er nødvendige for udstede certificering i henhold til databeskyttelsesforordningens artikel 42, stk. 8, og artikel 43, stk. 5,

8. indeholder regler om de nødvendige forholdsregler i forbindelse med undersøgelse af klager, som dette er beskrevet under pkt. 4.1.2.2 (c)(2) og (j) i ISO 17065, og derudover indeholder eksplicitte erklæringer om strukturen og proceduren for håndtering af klager i overensstemmelse med databeskyttelsesforordningens artikel 43, stk. 2, litra d,

9. ud over minimumskravene under pkt. 4.1.2.2 i ISO 17065 adresserer konsekvenserne for kunden, hvis en eventuel tilbagetrækning eller suspension af certificeringsorganets akkreditering vil have betydning for kunden,

10. kræver, at ansøgeren underretter certificeringsorganet ved væsentlige ændringer i ansøgerens aktuelle eller juridiske situation og i de af ansøgerens produkter, processer eller tjenester, som er omfattet af certificeringen,

11. indeholder bindende evalueringsmetoder vedrørende genstanden for certificering.

4.1.3 Brug af databeskyttelsescertifikater og -mærker

Certifikater og mærker må kun anvendes i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 42 og artikel 43 og EDPB's vejledninger om akkreditering og certificering.

4.2 Håndtering af upartiskhed

Akkrediteringsorganet skal ud over kravene under pkt. 4.2. i ISO 17065 sikre, at:

1. certificeringsorganet efterlever de supplerende akkrediteringskrav, som er udarbejdet af Datatilsynet i medfør af databeskyttelsesforordningens artikel 43, stk. 1, litra b

    a. i overensstemmelse med databeskyttelsesforordningens artikel 43, stk. 2, litra a, fremlægger særskilt dokumentation for sin uafhængighed. Dette gælder navnlig i forhold til dokumentation vedrørende certificeringsorganets finansiering, i det omfang det vedrører sikring af uafhængighed,

    b. dets opgaver og forpligtelser ikke fører til en interessekonflikt i henhold til databeskyttelsesforordningens artikel 43, stk. 2, litra e.

2. certificeringsorganet ikke har nogen relevant forbindelse med den kunde, som det vurderer, herunder eksempelvis:

a. Enhver type af økonomisk relation mellem certificeringsorganet og dets kunde kan – alt afhængigt af relationens karakter – påvirke uafhængigheden af certificeringsorganets certificeringsaktiviteter.

b. Certificeringsorganet må ikke tilhøre samme koncern eller juridiske enhed, som den kunde, det vurderer.

c. Certificeringsorganet må ikke på nogen måde være underlagt kontrol af den kunde, som det vurderer.

d. Certificeringsorganet må ikke indgå i en dataansvarlig/databehandler relation med den kunde, som det vurderer.

4.3 Erstatningsansvar og finansiering

Akkrediteringsorganet skal ud over kravet under pkt. 4.3.1. i ISO 17065 regelmæssigt sikre, at certificeringsorganet har truffet passende foranstaltninger (eksempelvis forsikring eller reserver) til dækning af erstatningsansvar i de geografiske områder, hvor certificeringsorganet er aktivt.

4.4 Ikke-diskriminerende forhold

Kravene i ISO 17065 finder anvendelse.

4.5 Fortrolighed

Kravene i ISO 17065 finder anvendelse.

4.6 Offentligt tilgængelig information

Ud over kravet under pkt. 4.6. i ISO 17065 skal akkrediteringsorganet kræve fra certificeringsorganet, at:

1. alle versioner (gældende og tidligere) af de godkendte certificeringskriterier i henhold til databeskyttelsesforordningens artikel 42, stk. 5, og alle certificeringsprocedurer offentliggøres og er let tilgængelige for offentligheden og generelt angiver gyldighedsperioden.

2. information omkring procedurer for håndtering af klager og anker gøres offentlig i henhold til databeskyttelsesforordningens artikel 43, stk. 2, litra d.

5. Krav til opbygning - og forordningens artikel 43, stk. 4 (“korrekt vurdering”)

5.1 Organisatorisk opbygning og topledelse

Kravene i ISO 17065 finder anvendelse.

5.2 Mekanisme til varetagelse af upartiskhed

Kravene i ISO 17065 finder anvendelse.

6. Ressourcekrav

6.1 Certificeringsorganets personale

Ud over kravet under pkt. 6 i ISO 17065 skal akkrediteringsorganet for hvert certificeringsorgan sikre, at dets personale, som foretager overensstemmelsesvurderingsopgaver:

1. har påvist passende og tidssvarende ekspertise (viden og erfaring) med hensyn til databeskyttelse i henhold til databeskyttelsesforordningens artikel 43, stk. 1,

2. er uafhængigt og besidder tidssvarende ekspertise med hensyn til genstanden for certificering i henhold til databeskyttelsesforordningens artikel 43, stk. 2, litra a, og ikke har nogen interessekonflikter i henhold til forordningens artikel 43, stk. 2, litra e,

3. påtager sig at respektere certificeringskriterierne, som beskrevet i databeskyttelsesforordningens artikel 42, stk. 5, i henhold til forordningens artikel 43, stk. 2, litra b,

4. har relevant og passende kendskab til og erfaring med anvendelse af databeskyttelseslovgivningen,

5. har relevant og passende kendskab til og erfaring med tekniske og organisatoriske databeskyttelsesforanstaltninger i det omfang, det er relevant,

6. er i stand til at kunne påvise erfaring inden for de områder, der er nævnt i disse supplerende akkrediteringskrav, herunder særligt:

   For så vidt angår personale med teknisk ekspertise:

   - Har erhvervet en kvalifikation på et relevant område inden for teknisk ekspertise på mindst EQF[5] niveau 6 eller en anerkendt beskyttet titel (eksempelvis Dipl. Ing.) inden for det relevante lovregulerede erhverv eller har væsentlig erhvervserfaring.

   - *Personale med ansvar for certificeringsbeslutninger* skal have væsentlig erhvervserfaring inden for databeskyttelseslovgivningen, herunder med at identificere og gennemføre databeskyttelsesforanstaltninger, eller have adgang til nogen med denne ekspertise, og passende faglige kvalifikationer/ uddannelsesmæssigt kvalifikationsniveau.

   - *Personale med ansvar for evalueringer* skal have relevant og aktuel erhvervserfaring og kendskab til teknisk databeskyttelse og erfaring inden for sammenligningsprocedurer (eksempelvis certificering/revision) samt passende faglige kvalifikationer i det omfang, det er relevant.

   Personalet skal påvise, at de holder deres områderelateret viden inden for tekniske og revisionsmæssige færdigheder ajour gennem løbende faglig udvikling.

   For så vidt angår personale med juridisk ekspertise:

   - Har gennemført juridiske studier ved et europæisk- eller statsanerkendt universitet af en varighed på mindst otte semestre inklusiv en kandidatgrad (LL.M) eller tilsvarende, eller har væsentlig erhvervserfaring.

[5] Se værktøj til sammenligning af nationale kvalifikationsrammer i hele Europa på https://ec.europa.eu/ploteus/en/compare

- *Personale med ansvar for certificeringsbeslutninger* skal påvise væsentlig erhvervserfaring inden for databeskyttelseslovgivning, herunder med at identificere og gennemføre databeskyttelsesforanstaltninger, eller have adgang til nogen med denne ekspertise, og passende faglige kvalifikationer/uddannelsesmæssigt kvalifikationsniveau.

- *Personale med ansvar for evalueringer* skal påvise mindst to års erhvervserfaring inden for databeskyttelseslovgivning og viden og erfaring inden for teknisk databeskyttelse og sammenligningsprocedurer (eksempelvis certificering/revision), og passende faglige kvalifikationer i det omfang, det er relevant.
    - Personalet skal påvise, at de holder deres områderelateret viden inden for tekniske og revisionsmæssige færdigheder ajour gennem løbende faglig udvikling

Certificeringsorganet skal være i stand til at kunne definere og forklare over for akkrediteringsorganet, hvilke krav til erhvervserfaring, der anses for passende i forhold til certificeringsordningens anvendelsesområde og den omhandlede genstand for certificering.

I forhold til personale med ansvar for certificeringsbeslutninger bibeholder certificeringsorganet ansvaret for certificeringsbeslutningerne, også når certificeringsorganet anvender eksterne eksperter. Eksterne aktører bør ikke involveres i beslutningsprocessen.

6.2 Ressourcer til evaluering

Kravene i ISO 17065 finder anvendelse.

7. Proceskrav, forordningens artikel 43, stk. 2, litra c og d

7.1 Generelt

Ud over kravet under pkt. 7.1. i ISO 17065 skal akkrediteringsorganet sikre følgende:

1. Certificeringsorganer efterlever Datatilsynets supplerende akkrediteringskrav (i henhold til databeskyttelsesforordningens artikel 43, stk. 1, litra b), når de indgiver ansøgningen, således at opgaver og forpligtelser ikke fører til en interessekonflikt i henhold til databeskyttelsesforordningens artikel 43, stk. 2, litra e.

2. Den relevante kompetente tilsynsmyndighed underrettes i overensstemmelse med databeskyttelsesforordningens artikel 43, stk. 1, inden certificeringsorganets etableringer/kontorer begynder at anvende en godkendt europæisk fællescertificering i en ny medlemsstat.[6]

3. Certificeringsorganer har fastlagt procedurer til at underrette Datatilsynet umiddelbart forud for udstedelse, fornyelse eller tilbagetrækning af certificeringer og give en begrundelse for disse beslutninger. Dette inkluderer at give Datatilsynet en kopi af resuméet af den evalueringsrapport, der refereres til under afsnit 7.8 i dette dokument

4. I tilfælde hvor kunden eller Datatilsynet underretter certificeringsorganet om væsentlige og relevante undersøgelser eller afgørelser fra Datatilsynet eller andre tilsynsmyndigheder, som drager tvivl om kundens efterlevelse af databeskyttelsesreglerne, er certificeringsorganet forpligtet til at foretage en vurdering af, om kunden stadig lever op til certificeringskriterierne. Certificeringsorganerne vil give Datatilsynet en forudgående redegørelse om udfaldet af denne vurdering. Vurderingen vil relatere sig certificeringens anvendelsesområde og genstanden for certificering.

7.2 Ansøgning

Ud over pkt. 7. 2 i ISO 17065 skal certificeringsorganet kræve, at ansøgningen:

1. indeholder en detaljeret beskrivelse af genstanden for certificering. Dette inkluderer også grænseflader og overførsler til andre systemer og organisationer, protokoller og andre garantier,

2. specificerer om der anvendes databehandlere, og hvis ansøgeren er databehandler, skal dennes ansvarsområder og opgaver beskrives, og ansøgningen skal indeholde de relevante databehandleraftaler,

3. specificerer om der er fælles dataansvar i forbindelse med behandlingsaktiviteterne, og hvis ansøgeren er fælles dataansvarlig skal dennes ansvarsområder og opgaver beskrives, og ansøgningen skal indeholde de relevante indgåede aftaler om fælles dataansvar, og

4. oplyser om alle igangværende eller tidligere undersøgelser eller afgørelser fra Datatilsynet eller andre tilsynsmyndigheder, som ansøgeren har været genstand for, hvis disse undersøgelser/afgørelser vedrører behandling af personoplysninger, som relaterer sig til certificeringens anvendelsesområde og genstanden for certificering.

6 Se mere herom i EDPB's vejledning om certificering (Guidelines 1/2018) pkt. 44.

Certificeringsorganet skal påkræves at informere Datatilsynet skriftligt, når certificeringsorganet modtager en ansøgning.

7.3 Gennemgang af ansøgning

Ud over pkt. 7.3 i ISO 17065 skal akkrediteringsorganet kræve, at:

1. bindende evalueringsmetoder vedrørende genstanden for certificering er fastlagt i certificeringsaftalen,

2. vurderingen under pkt. 7.3.1.(e) af, hvorvidt der er tilstrækkelig ekspertise, til en passende grad tager højde for både teknisk og juridisk ekspertise inden for databeskyttelse.

7.4 Evaluering

Ud over pkt. 7.4 i ISO 17065 skal certificeringsmekanismer beskrive evalueringsmetoder, der er tilstrækkelige i forhold til at vurdere, om behandlingsaktiviteterne opfylder certificeringskriterierne, herunder eksempelvis:

1. en metode til vurdering af, om behandlingsaktiviteterne er nødvendige og proportionale i forhold til formålet og de berørte registrerede,

2. en metode til at evaluere dækning, sammensætning og vurdering af alle risici, der tages i betragtning af den dataansvarlige og databehandleren med hensyn til de retlige konsekvenser i henhold til databeskyttelsesforordningens artikel 30, artikel 32, artikel 35 og artikel 36, og med hensyn til definitionen af tekniske og organisatoriske foranstaltninger i henhold til forordningens artikel 24, artikel 25 og artikel 32, i det omfang de nævnte artikler er anvendelige for genstanden for certificering, og

3. en metode til at vurdere de afhjælpende foranstaltninger, herunder garantier, sikkerhedsforanstaltninger og procedurer, der har til formål at sikre beskyttelsen af personoplysninger i forbindelse med den behandling, som genstanden for certificering underkastes. og med henblik på at påvise, at de retlige krav, som er fastlagt i de godkendte certificeringskriterier er opfyldt, og

4. dokumentation for metoder og resultater.

Certificeringsorganet skal være forpligtet til at sikre, at disse evalueringsmetoder er standardiserede og anvendes konsekvent. Dette indebærer, at der anvendes sammenlignelige evalueringsmetoder for sammenlignelige genstande for certificering. Enhver afvigelse fra denne procedure skal begrundes af certificeringsorganet.

Ud over pkt. 7.4.2 i ISO 17065 kan evalueringen udføres af underleverandører, som er blevet anerkendt af certificeringsorganet, og som lever op til samme personalemæssige krav jf. afsnit 6 i dette dokument. Hvis evalueringen udføres af en underleverandør, skal underleverandøren opfylde de respektive krav i ISO 17065 og de supplerende akkrediteringskrav, som er udarbejdet af Datatilsynet. Brugen af underleverandører fritager ikke certificeringsorganet for dets ansvar.

Ud over pkt. 7.4.5 i ISO 17065 skal det foreskrives, at eksisterende certificeringer, som vedrører den samme genstand for certificering, kan blive taget i betragtning som en del af en ny evaluering. Certifikatet alene vil dog ikke være tilstrækkelig dokumentation, og certificeringsorganet skal derfor forpligtes til at kontrollere overholdelsen af certificeringskriterierne i forhold til genstanden for certificering. Den fulde evalueringsrapport og andre relevante oplysninger, der muliggør evaluering af den eksisterende certificering og dens resultater, skal tages i betragtning for at kunne træffe en velunderbygget beslutning.

I sager, hvor en eksisterende certificering tages i betragtning som en del af en ny evaluering, skal denne certificerings anvendelsesområde også underlægges en detaljeret vurdering med hensyn til dennes overholdelse af de relevante certificeringskriterier.

Ud over pkt. 7.4.6. i ISO 17065 skal det kræves, at certificeringsorganet i sin certificeringsordning beskriver detaljeret, hvordan oplysningerne, som kræves i henhold til pkt. 7.4.6, informerer certificeringsansøgeren om manglende overensstemmelse med certificeringsordningen. I den forbindelse skal karakteren og timingen af denne information som minimum defineres. Certificeringsorganet skal beskrive dette i et skriftligt dokument, som enten kan være certificeringsordningen eller – hvis certificeringsorganet ikke er ejeren af certificeringsordningen – et andet dokument, der vedrører certificeringsprocessen.

Ud over pkt. 7.4.9 i ISO 17065 skal det kræves, at dokumentationen for evalueringen gøres fuldt tilgængelig for Datatilsynet, hvis der anmodes herom.

7.5 Gennemgang

Ud over pkt. 7.5 i ISO 17065 kræves der procedurer for udstedelse, regelmæssig gennemgang og tilbagetrækning af de pågældende certificeringer i henhold til databeskyttelsesforordningens artikel 43, stk. 2 og 3.

7.6 Beslutning om certificering

Ud over pkt. 7.6.1 i ISO 17065 skal det kræves, at certificeringsorganet i dets procedurer redegør detaljeret for, hvordan dets uafhængighed og ansvar i forhold til individuelle certificeringsbeslutninger sikres.

Ud over kravene i ISO 17065 skal det kræves, at certificeringsorganet umiddelbart inden udstedelse eller fornyelse af certificeringer skal forelægge et udkast til godkendelse, herunder et resumé af evalueringsrapporten, for Datatilsynet. Dette resumé skal tydeligt beskrive, hvordan certificeringskriterierne er opfyldt, ligesom det skal angive begrundelserne for udstedelsen eller fornyelsen af certificeringen. Hensigten med dette krav er at øge gennemsigtighed, og kravet medfører ikke kontrol af udkastet til godkendelse.

Ud over den kontrol, som udføres under ansøgningsstadiet, skal det kræves, at certificeringsorganet inden udstedelse af certificeringer får bekræftet fra ansøgeren, at denne ikke er genstand for nogle undersøgelser eller afgørelser fra Datatilsynet, som relaterer sig til genstanden for certificering, og som kan forhindre udstedelse af certificering. Datatilsynet vil, hvor det er hensigtsmæssigt, bekræfte dette, inden certificeringsorganet udsteder eller fornyer en certificering.

Det skal også kræves, at certificeringsorganet får bekræftet fra ansøgeren, at denne ikke er genstand for nogle undersøgelser eller afgørelser fra andre tilsynsmyndigheder, hvis disse undersøgelser eller afgørelser vedrører behandling af personoplysninger og kan forhindre udstedelse af certificering.

Hvis det konstateres, at en ansøger ikke har delt disse oplysninger med certificeringsorganet, kan det resultere i, at certificering ikke udstedes.

7.7 Certificeringsdokumentation

Ud over pkt. 7.7.1 (e) i ISO 17065 og i henhold til databeskyttelsesforordningens artikel 42, stk. 7, skal det kræves, at certificeringers gyldighedsperiode ikke må overstige 3 år.

Ud over pkt. 7.7.1 (e) i ISO 17065 skal det kræves, at den planlagte overvågningsperiode i henhold til afsnit 7.9 også dokumenteres.

Ud over pkt. 7.7.1 (f) i ISO 17065 skal det kræves, at certificeringsorganet identificerer genstanden for certificering i certificeringsdokumentationen (med angivelse af versionens status eller lignende egenskaber, hvis det er relevant).

Ved udstedelse af certifikater skal det kræves. at certificeringsorganet giver Datatilsynet en kopi af den certificeringsdokumentation, som der henvises til under pkt. 7.7.1 i ISO 17065.

7.8 Fortegnelse over certificerede produkter

Ud over pkt. 7.8 i ISO 17065 skal det kræves, at certificeringsorganet opbevarer oplysninger om certificerede produkter, processer og tjenester, så de er tilgængelige både internt og offentligt.

Certificeringsorganet stiller resuméet af evalueringsrapporten til rådighed for offentligheden.

Hensigten med dette resumé er at bidrage til gennemsigtighed omkring, hvad der er blevet certificeret, og hvordan dette blev vurderet. Resuméet vil eksempelvis uddybe følgende:

a) certificeringens anvendelsesområde og en meningsfuld beskrivelse af genstanden for certificering

b) de respektive certificeringskriterier (herunder version og funktionsstatus)

c) evalueringsmetoderne og udførte kontroller

d) resultatet/resultaterne

Ud over pkt. 7.8 i ISO 17065 og i henhold til databeskyttelsesforordningens artikel 43, stk. 5, skal certificeringsorganet informere Datatilsynet skriftligt om grundlaget for at udstede eller tilbagetrække den ønskede certificering.

7.9 Overvågning

Ud over pkt. 7.9.1, 7.9.2 og 7.9.3 i ISO 17065 og i henhold til databeskyttelsesforordningens artikel 43, stk. 2, litra c, skal det kræves, at regelmæssige overvågningsforanstaltninger er obligatoriske for at opretholde certificeringen i overvågningsperioden. Sådanne foranstaltninger bør være risikobaserede og proportionale, og den maksimale periode mellem overvågningsaktiviteterne bør ikke overstige 12 måneder.

7.10 Ændringer, der påvirker certificering

Ud over pkt. 7.10.1 og 7.10.2 i ISO 17065 inkluderer ændringer, der påvirker certificering, som certificeringsorganet skal tage stilling til, følgende:

- alle brud på persondatasikkerheden eller overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven, der er fastslået af Datatilsynet, andre tilsynsmyndigheder eller retslige myndigheder, som vedrører certificeringen, og som rapporteres af kunden eller Datatilsynet.
- ændringer i det aktuelle tekniske niveau (hvis det er relevant for den fremtidige certificering og overvågning),
- ændringer i databeskyttelseslovgivningen,
- vedtagelse af delegerede retsakter fra Europa-Kommissionen i overensstemmelse med databeskyttelsesforordningens artikel 43, stk. 8 og 9,
- afgørelser, udtalelser, vejledninger, anbefalinger, bedste praksis eller andre dokumenter, som er vedtaget af EDPB og
- retsafgørelser vedrørende databeskyttelse.

De ændringsprocedurer, som skal implementeres af certificeringsorganet, skal blandt andet indeholde: Overgangsperioder, godkendelsesprocesser med den kompetente tilsynsmyndighed, revurdering af genstanden for certificering og passende foranstaltninger til tilbagetrækning af certificering, hvis den certificerede behandlingsaktivitet ikke længere opfylder de ajourførte certificeringskriterier.

7.11 Ophør, begrænsning, suspension eller tilbagetrækning af certificering

Ud over pkt. 7.11.1 i ISO 17065 og afsnit 7.1.3 i dette dokument skal det kræves, at certificeringsorganet, hvor det er relevant, straks informerer Datatilsynet og akkrediteringsorganet skriftligt om trufne foranstaltninger og om videreførelse, begrænsning, suspension og tilbagetrækning af certificering.

I henhold til databeskyttelsesforordningens artikel 58, stk. 2, litra h, skal det kræves, at certificeringsorganet accepterer afgørelser og påbud fra Datatilsynet om at tilbagetrække eller ikke at udstede certificering til en kunde (ansøger), hvis kravene for certificering ikke er eller ikke længere er opfyldt.

7.12 Registreringer

Ud over kravene i ISO 17065 er certificeringsorganet forpligtet til at opbevare al dokumentation i fuldendt, forståelig, ajourført og revisionsegnet form.

7.13 Klager og anker, forordningens artikel 43, stk. 2, litra d

Ud over pkt. 7.13.1 i ISO 17065 skal certificeringsorganet forpligtes til at fastsætte:

a) hvem der kan indgive klager eller anke,

b) hvem der behandler klager eller anker på certificeringsorganets vegne,

c) hvilke kontroller, der finder sted i den forbindelse, og

d) mulighederne for høring af interesserede parter

Ud over pkt. 7.13.2 i ISO 17065 skal certificeringsorganet forpligtes til at fastsætte:

a) hvordan og til hvem, en sådan bekræftelse skal gives,

b) tidsfristerne for dette og

c) hvilke processer, der skal iværksættes efterfølgende.

Certificeringsorganet skal forpligtes til at gøre dets procedurer for håndtering af klager offentligt tilgængelige og let tilgængelige for registrerede.

Certificeringsorganet skal forpligtes til at informere klagere om klagens fremgang og resultatet af klagen inden for rimelig tid.

Ud over pkt. 7.13.1 i ISO 17065 skal certificeringsorganet fastsætte, hvordan det sikres, at certificeringsaktiviteter og behandling af anker og klager holdes adskilt.

8. Krav til ledelsessystemet

Ifølge kapitel 8 i ISO 17065 er det et generelt krav til ledelsessystemet, at gennemførelsen af alle krav fra de foregående kapitler inden for rammerne af det akkrediterede certificeringsorgans anvendelse af certificeringsmekanismen dokumenteres, evalueres, kontrolleres og overvåges uafhængigt.

Det grundlæggende princip for ledelse er at skabe et system, som fastsætter målene reelt og effektivt, især gennemførelsen af certificeringstjenesterne, ved hjælp af egnede specifikationer. Dette kræver, at certificeringsorganets implementering af akkrediteringskravene er gennemsigtig og kontrollerbar, og at kravene overholdes permanent.

I den henseende skal ledelsessystemet indeholde en metode til at overholde og kontrollere disse krav efter databeskyttelsesreglerne og til løbende at følge op på kravene med det akkrediterede certificeringsorgan.

Ud over kravene i ISO 17065 skal ledelsesprincipperne og deres dokumenterede gennemførelse være gennemsigtig og til enhver tid kunne fremlægges af det akkrediterede certificeringsorgan efter anmodning fra Datatilsynet i forbindelse med databeskyttelsesrevisioner i henhold til databeskyttelsesforordningens artikel 58, stk. 1, litra b, eller ved gennemgang af certificeringer, som er udstedt i overensstemmelse med forordningens artikel 42, stk. 7, i henhold til forordningens artikel 58, stk. 1, litra c.

Procedurer i forbindelse med suspension eller tilbagekaldelse af akkreditering skal være en integreret del af certificeringsorganets ledelsessystem, herunder underretning af kunder og ansøgere.

Certificeringsorganet skal som en integreret del af ledelsessystemet fastsætte en proces for håndtering af klager med den nødvendige grad af uafhængighed, som særligt skal implementere kravene under pkt. 4.1.2.2(c), 4.1.2.2(j), 4.6(d) og 7.13 i ISO 17065. Relevante klager og anker bør deles med den kompetente tilsynsmyndighed.

8.1 Generelt

Kravene i ISO 17065 finder anvendelse.

8.2 Generel dokumentation af ledelsessystemet

Kravene i ISO 17065 finder anvendelse.

8.3 Styring af dokumenter

Kravene i ISO 17065 finder anvendelse.

8.4 Styring af registreringer

Kravene i ISO 17065 finder anvendelse.

8.5 Ledelsens evaluering

Kravene i ISO 17065 finder anvendelse.

8.6 Interne audits

Kravene i ISO 17065 finder anvendelse.

8.7 Korrigerende handlinger

Kravene i ISO 17065 finder anvendelse.

8.8 Forebyggende handlinger

Kravene i ISO 17065 finder anvendelse.

9. Yderligere supplerende krav

9.1 Ajourføring af evalueringsmetoder

Certificeringsorganet skal fastlægge procedurer til at styre ajourføringen af evalueringsmetoderne for ansøgninger som led i den evaluering, der omtales under pkt. 7.4 i ISO 17065 og dette dokument. Ajourføring skal finde sted ved ændringer i det retlige grundlag, de relevante risici, det aktuelle tekniske niveau og de omkostninger, der er forbundet med implementering af tekniske og organisatoriske foranstaltninger.

9.2 Opretholdelse af ekspertise

Certificeringsorganer skal fastlægge procedurer, der sikrer uddannelse af dets ansatte med henblik på at ajourføre de ansattes kvalifikationer under hensyntagen til udviklingen anført under afsnit 9.1. i dette dokument.

9.3 Ansvar og kompetencer

9.3.1 Kommunikation mellem certificeringsorganet og dets kunder og ansøgere

Der skal være procedurer for gennemførsel af passende procedurer og kommunikationsstrukturer mellem certificeringsorganet og dets kunde. Dette skal inkludere:

1. At certificeringsorganet opbevarer dokumentation for opgaver og ansvar med henblik på:

    a) besvarelse af anmodninger om oplysninger, eller

    b) at muliggøre kontakt i tilfælde af en klage over en certificering

2. At registrere en ansøgningsproces med henblik på:

    a) Oplysninger om status på en ansøgning

    b) Evalueringer foretaget af den kompetente tilsynsmyndighed med hensyn til:

        i. Feedback

        ii. Afgørelser, som er truffet af den kompetente tilsynsmyndighed.

9.3.2 Dokumentation for evalueringsaktiviteter

Der skal være systemer for implementering af passende procedurer og kommunikationsstrukturer mellem certificeringsorganet og Datatilsynet. Dette skal inkludere en struktur for at underrette tilsynet:

- om detaljer vedrørende en ansøger ved modtagelsen af ansøgningen med henblik på at give Datatilsynet mulighed for at kontrollere ansøgerens historik for overholdelse af databeskyttelsesreglerne, jf. afsnit 7.6 i dette dokument;
- om grundlaget for at udstede eller tilbagetrække certificeringer efter databeskyttelsesforordningens artikel 43, stk. 5, umiddelbart inden udstedelse, fornyelse, suspension eller tilbagetrækning af certificeringer, jf. afsnit 7.1 (3) i dette dokument.

.

Datatilsynets supplerende akkrediteringskrav for certificeringsorganer

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