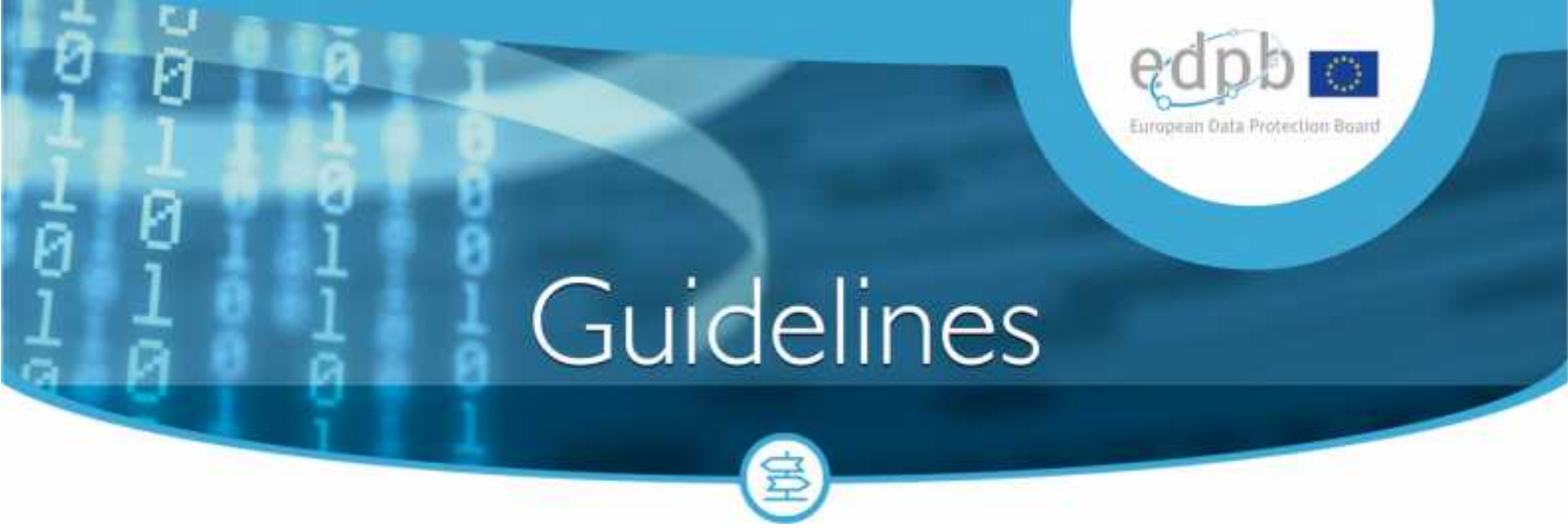

Vejledning 4/2018 om akkreditering af certificeringsorganer i henhold til artikel 43 i den generelle forordning om databeskyttelse (2016/679)

Version 3.0

4. juni 2019

Translations proofread by EDPB Members. This language version has not yet been proofread.

Vedtaget

Versionshistorik

Version 3.0	4. juni 2019	Optagelse af bilag 1 (version 2,0 af bilag 1 vedtaget den 4. juni 2019 efter offentlig høring)
Version 2.0	4. december 2018	Vedtagelse af retningslinjerne efter offentlig høring — Bilag 1 (version 1,0) blev samme dag vedtaget med henblik på offentlig høring
Version 1.0	6. februar 2018	Artikel 29-Gruppens vedtagelse af retningslinjerne (version med henblik offentlig høring). Denne version er blevet godkendt af Det Europæiske Databeskyttelsesråd den 25. maj 2018

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra e), i 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,

under hensyntagen til resultaterne af den offentlige høring om retningslinjerne, der fandt sted i februar 2018, og den om bilaget, som fandt sted mellem den 14. december 2018 og den 1. februar 2019, jf. artikel 70, stk. 4, i databeskyttelsesforordningen —

VEDTAGET FØLGENDE RETNINGSLINJER

1 INDLEDNING

1. Den generelle forordning om databeskyttelse (forordning (EU) 2016/679, "databeskyttelsesforordningen"), som træder i kraft den 25. maj 2018, udgør en moderniseret ramme, som bygger på ansvarlighed og overholdelse af de grundlæggende rettigheder i forbindelse med databeskyttelse i Europa. En række foranstaltninger, som har til formål at fremme overholdelsen af databeskyttelsesforordningens bestemmelser, er afgørende for denne nye ramme. De omfatter obligatoriske krav under specifikke omstændigheder (herunder udnævnelsen af databeskyttelsesrådgivere og udførelse af konsekvensanalyser vedrørende databeskyttelse) og frivillige foranstaltninger som f.eks. adfærdskodekser og certificeringsmekanismer.

2. Som en del af fastlæggelsen af certificeringsmekanismer for databeskyttelse samt oprettelsen af databeskyttelsesmærkninger og -mærker indeholder artikel 43, stk. 1, i databeskyttelsesforordningen krav om, at medlemsstaterne sikrer, at de certificeringsorganer, der udsteder certifikater i henhold til artikel 42, stk. 1, akkrediteres af enten den kompetente tilsynsmyndighed eller det nationale akkrediteringsorgan eller af dem begge. Hvis akkrediteringen udføres af det nationale akkrediteringsorgan i overensstemmelse med ISO/IEC 17065/2012, skal de supplerende krav, som er fastsat af den kompetente tilsynsmyndighed, også anvendes.

3. Fornuftige certificeringsmekanismer kan forbedre overholdelsen af databeskyttelsesforordningen og gennemsigtigheden for registrerede og i business to business-forhold, f.eks. mellem dataansvarlige og databehandlere. Dataansvarlige og databehandlere vil drage fordel af en uafhængig attestering foretaget af tredjemand med henblik på at påvise, at deres behandlingsaktiviteter overholder reglerne[1].

[1] I betragtning 100 i databeskyttelsesforordningen anføres det, at fastlæggelsen af certificeringsmekanismer kan forbedre gennemsigtigheden og overholdelsen af forordningen og sætte registrerede i stand til at vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester.

4. I denne forbindelse anerkender Det Europæiske Databeskyttelsesråd, at det er nødvendigt at opstille retningslinjer for akkreditering. Den særlige værdi af og formålet med akkrediteringen består i, at den giver en autoritativ erklæring om certificeringsorganernes kompetence, der giver mulighed for at skabe tillid til certificeringsmekanismen.

5. Formålet med retningslinjerne er at vejlede om, hvordan man skal fortolke og gennemføre bestemmelserne i artikel 43 i databeskyttelsesforordningen. De tager navnlig sigte på at hjælpe medlemsstaterne, tilsynsmyndighederne og de nationale akkrediteringsorganer med at etablere et sammenhængende og ensartet grundlag for akkreditering af certificeringsorganer, som udsteder certificering i overensstemmelse med databeskyttelsesforordningen.

2 RETNINGSLINJERNES ANVENDELSESOMRÅDE

6. Disse retningslinjer:

- fastsætter formålet med akkreditering i forbindelse med databeskyttelsesforordningen
- forklarer de valgmuligheder, der er med henblik på akkreditering af certificeringsorganer i overensstemmelse med artikel 43, stk. 1, og identificerer de vigtigste spørgsmål, der skal tages i betragtning
- danner en ramme for fastsættelsen af supplerende akkrediteringskrav, når akkrediteringen varetages af det nationale akkrediteringsorgan og
- danner en ramme for fastsættelsen af akkrediteringskrav, når akkrediteringen varetages af tilsynsmyndigheden.

7. Retningslinjerne udgør ikke en procedurehåndbog for akkreditering af certificeringsorganer i overensstemmelse med databeskyttelsesforordningen. De udvikler ikke en ny teknisk standard for akkreditering af certificeringsorganer med henblik på databeskyttelsesforordningen.

8. Retningslinjerne er rettet mod:

   - de medlemsstater, som skal sikre, at certificeringsorganerne er akkrediteret af tilsynsmyndigheden og/eller det nationale akkrediteringsorgan
   - de nationale akkrediteringsorganer, der foretager akkreditering af certificeringsorganer i henhold til artikel 43, stk. 1, litra b)
   - den kompetente tilsynsmyndighed, der præciserer "supplerende krav" til kravene i ISO/IEC 17065/2012[2], når akkrediteringen foretages af det nationale akkrediteringsorgan i henhold til artikel 43, stk. 1, litra b)
   - Det Europæiske Databeskyttelsesråd, når det afgiver udtalelse om og godkender kompetente tilsynsmyndigheders akkrediteringskrav i henhold til artikel 43, stk. 3, artikel 70, stk. 1, litra p) og artikel 64, stk. 1, litra c)
   - den kompetente tilsynsmyndighed, der specificerer akkrediteringskravene, når akkreditering udføres af tilsynsmyndigheden i henhold til artikel 43, stk. 1, litra a)

[2] Den internationale Standardiseringsorganisation: Overensstemmelsesvurdering — Krav til organer, der certificerer produkter, processer og tjenester.

- andre interessenter, f.eks. kommende certificeringsorganer eller ejere af certificeringsordninger, der giver mulighed for certificeringskriterier og -procedurer[3].

9. Definitioner

10. Følgende definitioner har til formål at fremme en fælles forståelse af de grundlæggende elementer i akkrediteringsprocessen. De skal betragtes som referencepunkter og kan anfægtes. Definitionerne er baseret på eksisterende lovgivningsmæssige rammer og standarder, navnlig de relevante bestemmelser i databeskyttelsesforordningen og ISO/IEC 17065/2012.

11. I disse retningslinjer gælder følgende definitioner:

12. "*akkreditering*" af certificeringsorganer, se afsnit 3 om fortolkning af akkreditering med henblik på artikel 43 i databeskyttelsesforordningen

13. "*supplerende krav*" betyder de krav, der er fastsat af den tilsynsmyndighed, der er kompetent, og som er genstand for en akkreditering[4]

14. "*certificering*" betyder, at der foretages en vurdering, samt at en uvildig tredjepart attesterer[5], at det kan dokumenteres, at certificeringskriterierne er opfyldt

15. "*certificeringsorgan*" betyder en tredjeparts overensstemmelsesvurderingsorgan[67], der anvender en certificeringsmekanisme[8]

16. "*certificeringsordning*" betyder et certificeringssystem i forbindelse med nærmere angivne produkter, processer og tjenester, der er omfattet af de samme specifikke krav, regler og procedurer[9]

17. "kriterier" eller "certificeringskriterier" betyder de kriterier, mod hvilke der udføres en certificering (overensstemmelsesvurdering)[10]

---

[3] En ejer af en ordning er en identificerbar organisation, som har opstillet certificeringskriterier og de krav, der skal lægges til grund for vurderingen af overensstemmelsen. Akkrediteringen er af den organisation, der foretager vurderinger (artikel 43, stk. 4), i forhold til kravene i certificeringsordningen, og som udsteder certificeringen (dvs. certificeringsorganet, også kaldet overensstemmelsesvurderingsorganet). Den organisation, der foretager vurderingerne, kan være den samme organisation, som har udviklet og ejer ordningen, men der kan være ordninger, hvor en organisation ejer ordningen, og en anden (eller flere) udfører vurderingerne.

[4] Artikel 43, stk. 1, 3 og 6.

[5] Bemærk, at tredjeparts attestering (certificering) ifølge ISO 17000 er "anvendelig på alle genstande i forbindelse med overensstemmelsesvurdering" 5.5) "bortset fra de overensstemmelsesvurderingsorganer, som akkrediteringen gælder for" (5.6).

[6] Tredjeparts overensstemmelsesvurderingsaktiviteter udføres af en organisation, der er uafhængig af den person eller organisation, der leverer genstanden, og af brugernes interesser i genstanden, jf. ISO 17000, 2.4.

[7] Se ISO 17000, 2.5: "organ, der udfører overensstemmelsesvurderingsopgaver"; ISO 17011: "organ, der udfører overensstemmelsesvurderingsopgaver, og som kan gøres til genstand for akkreditering"; ISO 17065, 3.12.

[8] Artikel 42, stk.1 og 5, i databeskyttelsesforordningen.

[9] Se punkt 3.9 sammenholdt med bilag B til ISO 17065.

[10] Se artikel 42, stk. 5.

18. "nationalt akkrediteringsorgan" betyder det eneste organ i en medlemsstat, der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 for så vidt angår akkreditering med statslig bemyndigelse[11].

3 FORTOLKNING AF "AKKREDITERING" MED HENBLIK PÅ ARTIKEL 43 I DATABESKYTTELSESFORORDNINGEN

19. Databeskyttelsesforordningen definerer ikke "akkreditering". I artikel 2, stk. 10, i forordning (EF) nr. 765/2008, som indeholder generelle krav til akkreditering, defineres akkreditering som:

20. "en attestering foretaget af et nationalt akkrediteringsorgan af, at et overensstemmelsesvurderingsorgan opfylder de krav, der er fastsat i de harmoniserede standarder, og i givet fald alle andre supplerende krav, herunder dem, der er fastsat i de relevante sektorordninger om at udføre en specifik overensstemmelsesvurderingsaktivitet"

21. I henhold til ISO/IEC 17011

22. "akkreditering henviser til tredjepartserklæring vedrørende et overensstemmelsesvurderingsorgan, der formelt dokumenterer dets kompetence til at udføre specifikke overensstemmelsesvurderingsopgaver."

23. I artikel 43, stk. 1, bestemmes følgende:

24. "Uden at dette berører den kompetente tilsynsmyndigheds opgaver og beføjelser i henhold til artikel 57 og 58, udsteder og forlænger certificeringsorganer, der har et passende ekspertiseniveau for så vidt angår databeskyttelse, certificering, efter at have underrettet tilsynsmyndigheden for at gøre det muligt for den at udøve sine beføjelser i henhold til artikel 58, stk. 2, litra h), hvis det er nødvendigt. Medlemsstaterne sikrer, at disse certificeringsorganer akkrediteres af en eller begge af følgende:

    (a) den tilsynsmyndighed, der er kompetent i henhold til artikel 55 eller 56
    (b) det nationale akkrediteringsorgan, der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 i overensstemmelse med ISO/IEC 17065/2012, og de supplerende krav, der er fastsat af den tilsynsmyndighed, der er kompetent i henhold til artikel 55 eller 56."

25. Med hensyn til databeskyttelsesforordningen vil akkrediteringskravene være styret af:

- ISO/IEC 17065/2012 og "supplerende krav" fastlagt af den tilsynsmyndighed, der er kompetent i henhold til artikel 43, stk. 1, litra b), når akkrediteringen udføres af det nationale akkrediteringsorgan, og af tilsynsmyndigheden, når denne selv udfører akkrediteringen.

26. I begge tilfælde skal de konsoliderede krav omfatte de krav, der er nævnt i artikel 43, stk. 2.

27. Det Europæiske Databeskyttelsesråd anerkender, at formålet med akkreditering er at give en autoritativ erklæring om et organs kompetence til at udføre certificering

[11] Se artikel 2, stk. 11, i forordning 765/2008/EF.

(overensstemmelsesvurderingsaktiviteter)[12]. Akkreditering i henhold til databeskyttelsesforordningen skal forstås som følgende:

28. en attestering[13] foretaget af et nationalt akkrediteringsorgan og/eller af en tilsynsmyndighed af, at et certificeringsorgan[14] er kvalificeret til at udføre certificering i henhold til artikel 42 og 43 i databeskyttelsesforordningen, under hensyntagen til ISO/IEC 17065/2012 og de supplerende krav, der er fastsat af tilsynsmyndigheden og/eller af Databeskyttelsesrådet.

4 AKKREDITERING I OVERENSSTEMMELSE MED ARTIKEL 43, STK. 1, I DATABESKYTTELSESFORORDNINGEN

29. I artikel 43, stk. 1, anerkendes det, at der er flere muligheder for akkreditering af certificeringsorganer. Databeskyttelsesforordningen kræver, at tilsynsmyndighederne og medlemsstaterne fastlægger proceduren for akkreditering af certificeringsorganer. I dette afsnit redegøres for de i artikel 43 omhandlede forløb for akkreditering.

4.1 Medlemsstaternes rolle

30. I henhold til artikel 43, stk. 1, skal medlemsstaterne *sikre*, at certificeringsorganer akkrediteres, men hver medlemsstat gives mulighed for at afgøre, hvem der skal være ansvarlig for at foretage den vurdering, der fører til akkreditering. Der er på grundlag af artikel 43, stk. 1, tre muligheder for, hvordan der foretages akkreditering:

(1) udelukkende af tilsynsmyndigheden på grundlag af dens egne krav
(2) udelukkende af det nationale akkrediteringsorgan, der er udpeget i overensstemmelse med forordning (EF) nr. 765/2008 og på grundlag af ISO/IEC 17065/2012, og med supplerende krav, som er fastsat af den kompetente tilsynsmyndighed eller
(3) både af tilsynsmyndigheden og det nationale akkrediteringsorgan (og i overensstemmelse med alle krav anført i punkt 2 ovenfor).

31. Det er op til den enkelte medlemsstat at afgøre, om det nationale akkrediteringsorgan eller tilsynsmyndigheden eller begge vil gennemføre disse akkrediteringsaktiviteter, men under alle omstændigheder bør den sikre, at der er tilstrækkelige ressourcer til rådighed[15].

4.2 Samspil med forordning (EF) 765/2008

32. Det Europæiske Databeskyttelsesråd bemærker, at artikel 2, stk. 11, i forordning (EF) nr. 765/2008 definerer et nationalt akkrediteringsorgan som "det *eneste* organ i en medlemsstat med statslig bemyndigelse til at foretage akkreditering".

33. Artikel 2, stk. 11, kan anses for at være i strid med artikel 43, stk. 1, i databeskyttelsesforordningen, som tillader akkreditering foretaget af et andet organ end det nationale akkrediteringsorgan i medlemsstaten. Det Europæiske Databeskyttelsesråd mener, at hensigten med EU-lovgivningen har været at afvige fra det generelle princip om, at akkrediteringen udelukkende skal foretages af den nationale akkrediteringsmyndighed, ved

[12] Jf. betragtning 15 i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008.
[13] Jf. artikel 2, stk. 10, i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter.
[14] Jf. definitionen af "akkreditering" i henhold til ISO 17011.
[15] Jf. artikel 4, stk. 9, i forordning (EF) nr. 765/2008.

at give tilsynsmyndighederne samme beføjelser med hensyn til akkreditering af certificeringsorganer. Artikel 43, stk. 1, er derfor lex specialis i forhold til artikel 2, stk. 11, i forordning (EF) nr. 765/2008.

4.3 Det nationale akkrediteringsorgans rolle

34. I henhold til artikel 43, stk. 1, litra b), akkrediterer det nationale akkrediteringsorgan certificeringsorganer i henhold til ISO/IEC 17065/2012 og med de supplerende krav, der er fastsat af den kompetente tilsynsmyndighed.

35. Med henblik på en præcisering bemærker Det Europæiske Databeskyttelsesråd, at den specifikke henvisning til artikel 43, stk. 3, punkt 1, litra b), indebærer, at "disse krav" henviser til de "supplerende krav", der er fastsat af den kompetente tilsynsmyndighed i henhold til artikel 43, stk. 1, litra b), og kravene i artikel 43, stk. 2.

36. De nationale akkrediteringsorganer anvender ved akkrediteringen de supplerende krav, som tilsynsmyndighederne stiller.

37. Et certificeringsorgan med eksisterende akkreditering på grundlag af ISO/IEC 17065/2012 for certificeringsordninger, der ikke er omfattet af databeskyttelsesforordningen, og som ønsker at udvide omfanget af sin akkreditering til at omfatte certificering, der er udstedt i overensstemmelse med databeskyttelsesforordningen, skal opfylde de supplerende krav, der er fastsat af tilsynsmyndigheden, hvis akkreditering håndteres af det nationale akkrediteringsorgan. Hvis akkreditering med henblik på certificering i henhold til databeskyttelsesforordningen kun tilbydes af den kompetente tilsynsmyndighed, skal et certificeringsorgan, der ansøger om akkreditering, opfylde de krav, der er fastsat af den pågældende tilsynsmyndighed.

4.4 Tilsynsmyndighedernes rolle

38. Det Europæiske Databeskyttelsesråd bemærker, at tilsynsmyndigheden i henhold til artikel 57, stk. 1, litra q), foretager akkrediteringen af et certificeringsorgan i henhold til artikel 43 som "tilsynsmyndighed" i henhold til artikel 57, og at tilsynsmyndigheden i henhold til artikel 58, stk. 3, litra e), har bemyndigelse og rådgivningsbeføjelse til at akkreditere certificeringsorganer i henhold til artikel 43. Ordlyden i artikel 43, stk. 1, giver en vis fleksibilitet, og tilsynsmyndighedens akkrediteringsfunktion bør kun forstås som en opgave, hvor det er relevant. Medlemsstaternes lovgivning kan anvendes til at præcisere dette punkt. I forbindelse med akkreditering foretaget af et nationalt akkrediteringsorgan er certificeringsorganet dog i henhold til artikel 43, stk. 2, litra a), forpligtet til at påvise sin uafhængighed og ekspertise med hensyn til certificeringens genstand til den kompetente tilsynsmyndigheds tilfredshed[16].

39. Hvis en medlemsstat kræver, at certificeringsorganerne skal akkrediteres af tilsynsmyndigheden, bør tilsynsmyndigheden fastsætte akkrediteringskrav, som omfatter, men ikke er begrænset til, kravene i artikel 43, stk. 2. I forhold til forpligtelserne vedrørende nationale akkrediteringsorganers akkreditering af certificeringsorganer, gives der i artikel 43 mindre vejledning om kravene til akkreditering, når tilsynsmyndigheden selv foretager akkrediteringen. For at bidrage til en harmoniseret tilgang til akkreditering, bør de akkrediteringskriterier, som anvendes af tilsynsmyndigheden, fastsættes på grundlag af

[16] De supplerende krav, der fastsættes af tilsynsmyndigheden i henhold til artikel 43, stk. 1, litra b), bør indeholde krav om uafhængighed og ekspertise. Se også bilag 1 i retningslinjerne.

ISO/IEC 17065 og suppleres af de supplerende krav, som en tilsynsmyndighed fastsætter i henhold til artikel 43, stk. 1, litra b). Det Europæiske Databeskyttelsesråd bemærker, at artikel 43, stk. 2, litra a) til e), afspejler og specificerer krav i ISO 17065, som vil bidrage til konsistens.

40. Hvis en medlemsstat kræver, at certificeringsorganerne skal akkrediteres af de nationale akkrediteringsorganer, bør tilsynsmyndigheden fastsætte supplerende krav, der supplerer de eksisterende akkrediteringskonventioner, der er fastsat i forordning (EF) nr. 765/2008 (hvor artikel 3-14 vedrører organisation og akkreditering af overensstemmelsesvurderingsorganer), og de tekniske regler, der beskriver certificeringsorganernes metoder og procedurer. I lyset heraf indeholder forordning (EF) 765/2008 yderligere vejledning: I artikel 2, stk. 10, defineres akkreditering, og der henvises til "harmoniserede standarder" og "supplerende krav, herunder dem, der er fastsat i de relevante sektorordninger". Det følger heraf, at de supplerende krav, som tilsynsmyndigheden har fastsat, bør omfatte specifikke krav og fokusere på at lette vurderingen af bl.a. uafhængigheden og niveauet af databeskyttelsesekspertise hos certificeringsorganer, f.eks. deres evne til at evaluere og certificere dataansvarliges og databehandleres behandling af personoplysninger i henhold til artikel 42 stk. 1. Dette omfatter kompetence, som er nødvendig i forbindelse med sektorordninger og med hensyn til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger[17]. Bilaget til disse retningslinjer kan bidrage til at informere de kompetente tilsynsmyndigheder i forbindelse med fastsættelsen af "supplerende krav" i overensstemmelse med artikel 43, stk. 1, litra b), og artikel 43, stk. 3.

41. I artikel 43, stk. 6, hedder det, at "de i denne artikels stk. 3 omhandlede krav og de i artikel 42, stk. 5, omhandlede kriterier [offentliggøres] i lettilgængelig form". For at sikre gennemsigtighed offentliggøres derfor alle kriterier og krav, der er godkendt af en tilsynsmyndighed. Med hensyn til kvalitet og tillid til certificeringsorganerne ville det være hensigtsmæssigt, at alle kravene til akkreditering var let tilgængelige for offentligheden.

4.5 Tilsynsmyndighed, der fungerer som certificeringsorgan

42. I henhold til artikel 42, stk. 5, kan en tilsynsmyndighed udstede certificeringer, men databeskyttelsesforordningen kræver ikke, at den skal være akkrediteret for at opfylde kravene i forordning (EF) nr. 765/2008. Det Europæiske Databeskyttelsesråd bemærker, at artikel 43, stk. 1, litra a), og i særdeleshed artikel 58, stk. 2, litra h), samt stk. 3, litra a), e) og f), bemyndiger tilsynsmyndighederne til at udføre både akkreditering og certificering og samtidig yde rådgivning og, hvor det er relevant, tilbagekalde certificeringer eller pålægge certificeringsorganer at afholde sig fra at udstede certificeringer.

43. Der kan være situationer, hvor det er hensigtsmæssigt eller nødvendigt at adskille akkrediterings- og certificeringsroller og -opgaver, f.eks. hvis en tilsynsmyndighed og andre certificeringsorganer eksisterer side om side i en medlemsstat, og begge udsteder det samme udvalg af certificeringer. Tilsynsmyndighederne bør derfor træffe tilstrækkelige organisatoriske foranstaltninger med henblik på at adskille de opgaver, der udføres i henhold til databeskyttelsesforordningen, for at forankre og lette certificeringsmekanismerne, og samtidig træffe forholdsregler for at undgå interessekonflikter, der måtte opstå som følge af disse opgaver. Derudover bør medlemsstaterne og tilsynsmyndighederne holde sig det

[17] Artikel 1, stk. 2, i databeskyttelsesforordningen.

harmoniserede europæiske niveau for øje, når de udarbejder national lovgivning og procedurer vedrørende akkreditering og certificering i overensstemmelse med databeskyttelsesforordningen.

4.6 Akkrediteringskrav

44. Bilaget til disse retningslinjer indeholder vejledning om, hvordan der kan fastlægges supplerende akkrediteringskrav. I bilaget peges på de relevante bestemmelser i databeskyttelsesforordningen, og det indeholder forslag til krav, som tilsynsmyndigheder og nationale akkrediteringsorganer bør overveje for at sikre overensstemmelse med databeskyttelsesforordningen.

45. Som fastslået ovenfor, vil ISO/IEC 17065/2012, hvis certificeringsorganer er akkrediteret af det nationale akkrediteringsorgan i henhold til forordning (EF) nr. 765/2008, være den relevante akkrediteringsstandard suppleret med de supplerende krav, der er fastsat af tilsynsmyndigheden. Artikel 43, stk. 2, afspejler de generiske bestemmelser i ISO/IEC 17065/2012 i lyset af beskyttelsen af grundlæggende rettigheder i databeskyttelsesforordningen. I bilaget danner artikel 43, stk. 2, og ISO/IEC 17065/2012 grundlag for indkredsningen af krav samt yderligere kriterier vedrørende vurderingen af certificeringsorganernes ekspertise på databeskyttelsesområdet og deres evne til at respektere fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandlingen af personoplysninger som fastsat i databeskyttelsesforordningen. Det Europæiske Databeskyttelsesråd bemærker, at det især fokuserer på at sikre, at certificeringsorganerne har et passende niveau af ekspertise inden for databeskyttelse i overensstemmelse med artikel 43, stk. 1.

46. De supplerende akkrediteringskrav, der fastsættes af tilsynsmyndigheden, finder anvendelse på alle certificeringsorganer, der ansøger om akkreditering. Akkrediteringsorganet vurderer, om certificeringsorganet er kompetent til at udføre certificeringsaktiviteterne i overensstemmelse med de supplerende krav og genstanden for certificering. Der skal være referencer til specifikke sektorer eller certificeringsområder, som certificeringsorganet er akkrediteret til.

47. Det Europæiske Databeskyttelsesråd bemærker også, at den særlige ekspertise inden for databeskyttelse også er påkrævet ud over ISO/IEC 17065/2012, hvis andre eksterne organer, f.eks. laboratorier og revisorer, udfører dele eller komponenter i forbindelse med certificeringsaktiviteter på vegne af et akkrediteret certificeringsorgan. I disse tilfælde er akkreditering af disse eksterne organer i henhold til databeskyttelsesforordningen ikke mulig. For at sikre, at disse organer er egnede til at udføre deres aktiviteter på vegne af de akkrediterede certificeringsorganer, er det imidlertid nødvendigt, at det akkrediterede certificeringsorgan sikrer, at den ekspertise inden for databeskyttelse, der kræves for det akkrediterede organ, også er på plads og dokumenteret for det eksterne organs vedkommende for så vidt angår den pågældende aktivitet.

48. Rammerne for indkredsning af de supplerende akkrediteringskrav, der fremgår af bilaget til disse retningslinjer, udgør ikke en procedurehåndbog for den akkrediteringsproces, der udføres af det nationale akkrediteringsorgan eller tilsynsmyndigheden. De indeholder vejledning om struktur og metodologi og dermed en værktøjskasse til tilsynsmyndighederne med henblik på at identificere de supplerende krav til akkreditering.

BILAG 1

Bilag 1 indeholder vejledning angående fastsættelsen af "supplerende" akkrediteringskrav med hensyn til ISO/IEC 17065/2012 og i overensstemmelse med artikel 43, stk. 1, litra b), og artikel 43, stk. 3, i databeskyttelsesforordningen.

I dette bilag fremlægges forslag til krav, som en tilsynsmyndighed for databeskyttelse skal udarbejde udkast til, og som finder anvendelse i forbindelse med det nationale akkrediteringsorgans eller den kompetente tilsynsmyndigheds akkreditering af et certificeringsorgan[18]. Disse supplerende krav skal meddeles Det Europæiske Databeskyttelsesråd, inden de godkendes i henhold til artikel 64, stk. 1, litra c).

Dette bilag bør læses i sammenhæng med ISO/IEC 17065/2012. De afsnitsnumre, der anvendes her, svarer til dem, der anvendes i ISO/IEC 17065/2012. I tilfælde, hvor tilsynsmyndigheder foretager akkreditering i henhold til artikel 43, stk. 1, litra a), vil det være god praksis at følge denne fremgangsmåde, hvis det er praktisk muligt. Dette vil understøtte en harmoniseret akkreditering i EU.

Den kompetente myndighed kan, uanset den følgende vejledning eller manglende vejledning vedrørende punkter i ISO/IEC 17065/2012, formulere supplerende krav vedrørende disse punkter, hvis de er i overensstemmelse med den nationale lovgivning.

0 PRÆFIKS

[Dette afsnit omhandler eventuelle samarbejdsbetingelser, som det nationale akkrediteringsorgan og tilsynsmyndigheden for databeskyttelse måtte have aftalt, hvis det er relevant, f.eks. med hensyn til, hvem der bør have ansvaret for at modtage ansøgninger, eller hvordan anerkendelsen af godkendte kriterier tilrettelægges som en del af akkrediteringsprocessen.]

1 ANVENDELSESOMRÅDE[19]

Anvendelsesområdet for ISO/IEC 17065/2012 finder anvendelse i overensstemmelse med databeskyttelsesforordningen. Retningslinjerne vedrørende akkreditering og certificering indeholder yderligere oplysninger. Det nationale akkrediteringsorgan og den kompetente tilsynsmyndighed bør i deres vurdering under akkrediteringsprocessen tage hensyn til en certificeringsmekanismes anvendelsesområde (for eksempel certificering af behandlingsaktiviteter i forbindelse med cloud-tjenester), navnlig med hensyn til kriterier, ekspertise og evalueringsmetode. ISO/IEC 17065/2012's brede anvendelsesområde, der dækker produkter, processer og tjenester, bør ikke sænke eller tilsidesætte kravene i databeskyttelsesforordningen, f.eks. kan en styringsmekanisme ikke være det eneste element i en certificeringsmekanisme, fordi certificeringen skal omfatte behandling af personoplysninger, dvs. behandlingsaktiviteterne. I henhold til artikel 42, stk. 1, finder certificering under databeskyttelsesforordningen kun anvendelse på dataansvarliges og databehandleres behandlingsaktiviteter.

[18] Oplysninger om godkendelsesprocessen for certificeringskriterier findes i afsnit 4 i certificeringsretningslinjerne.
[19] Nummereringen henviser til ISO/IEC 17065/2012.

2 NORMATIV REFERENCE

Databeskyttelsesforordningen har forrang frem for ISO/IEC 17065/2012. Hvis der i de supplerende krav eller ved en certificeringsmekanisme henvises til andre ISO-standarder, fortolkes disse i overensstemmelse med kravene i databeskyttelsesforordningen.

3 BEGREBER OG DEFINITIONER

Inden for rammerne af dette bilag finder begreberne og definitionerne i retningslinjerne for akkreditering (WP 261) og certificering (EDPB 1/2018) anvendelse og har forrang frem for ISO-definitioner.

4 GENERELLE KRAV TIL AKKREDITERING

4.1 Retlige og kontraktmæssige spørgsmål

4.1.1 Retligt ansvar

Et certificeringsorgan bør (til enhver tid) være i stand til at dokumentere overfor det nationale akkrediteringsorgan og den kompetente tilsynsmyndighed, at dets procedurer er tidssvarende og lever op til det retlige ansvar, der er fastsat i akkrediteringsbetingelserne, herunder de supplerende krav med hensyn til anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2016/679. Bemærk, at fordi certificeringsorganet selv er dataansvarlig/databehandler, skal det som led i certificeringsprocessen kunne fremlægge dokumentation for, at dets procedurer og foranstaltninger, som specifikt vedrører styring og håndtering af kundeorganisationens personoplysninger, overholder Europa-Parlamentets og Rådets forordning (EU) 2016/679.

Den kompetente tilsynsmyndighed kan forud for akkrediteringen beslutte at tilføje yderligere krav og procedurer med henblik på at kontrollere certificeringsorganernes overholdelse af databeskyttelsesforordningen.

4.1.2 Certificeringsaftale

Minimumskravene til en certificeringsaftale suppleres med følgende punkter:

Certificeringsorganet skal ud over at overholde kravene i ISO/IEC 17065/2012 dokumentere, at dets certificeringsaftaler:

1. kræver, at ansøgeren altid overholder både de generelle certificeringskrav som defineret i 4.1.2.2, litra a), i ISO/IEC 17065/2012 og de kriterier, der er godkendt af den kompetente tilsynsmyndighed eller Det Europæiske Databeskyttelsesråd i overensstemmelse med artikel 43, stk. 2, litra b), og artikel 42, stk. 5
2. kræver, at ansøgeren giver den kompetente tilsynsmyndighed fuld indsigt i certificeringsproceduren, herunder kontraktligt fortrolige spørgsmål vedrørende overholdelse af databeskyttelsesreglerne i henhold til artikel 42, stk. 7, og artikel 58, stk. 1, litra c)
3. ikke mindsker ansøgerens ansvar for overholdelse af Europa-Parlamentets og Rådets forordning (EU) 2016/679 og ikke berører de opgaver og beføjelser, hører under de tilsynsmyndigheder, som er kompetente i henhold til artikel 42, stk. 5

4. kræver, at ansøgeren giver certificeringsorganet alle oplysninger og adgang til de behandlingsaktiviteter, som er nødvendige for at gennemføre certificeringsproceduren i henhold til artikel 42, stk. 6
5. kræver, at ansøgeren overholder de gældende frister og procedurer. Certificeringsaftalen skal præcisere, at frister og procedurer, som eksempelvis hidrører fra certificeringsprogrammet eller andre bestemmelser, skal følges og overholdes,
6. for så vidt angår 4.1.2.2, litra c), nr. 1, i ISO/IEC 17065/2012 fastsætter reglerne for gyldighed, fornyelse og tilbagekaldelse i henhold til artikel 42, stk. 7, og artikel 43, stk. 4, herunder regler om passende intervaller for genevaluering eller revision (regularitet) i overensstemmelse med artikel 42, stk. 7
7. giver certificeringsorganet mulighed for at fremlægge alle de oplysninger, der er nødvendige for at udstede en certificering i henhold artikel 42, stk. 8, og artikel 43, stk. 5,
8. omfatter regler om de nødvendige forholdsregler i forbindelse med undersøgelse af klager i overensstemmelse med 4.1.2.2, litra c), nr. 2, og litra j), og derudover også indeholder eksplicitte erklæringer om strukturen og proceduren for behandling af klager i overensstemmelse med artikel. 43, stk. 2, litra d)
9. sikrer, at der i tilfælde, hvor konsekvenserne af en tilbagetrækning eller suspension af akkrediteringen påvirker kunden, også bliver taget hånd om disse konsekvenser ud over de minimumskrav, der henvises til i 4.1.2.2 i ISO/IEC 17065/2012
10. kræver, at ansøgeren underretter certificeringsorganet i tilfælde af væsentlige ændringer af vedkommendes faktiske eller retlige stilling samt processer og tjenesteydelser, der er berørt af certificeringen.

4.1.3 Anvendelse af databeskyttelsesmærkninger og -mærker

Certifikater, mærkninger og mærker må kun anvendes i overensstemmelse med artikel 42 og 43 og retningslinjerne for akkreditering og certificering.

4.2 Forvaltning af uvildighed

Akkrediteringsorganet sikre ud over overholdelsen af kravet i artikel 4.2. i ISO/IEC 17065/2012, at certificeringsorganet

1. overholder den kompetente tilsynsmyndigheds supplerende krav (i henhold til artikel 43, stk. 1, litra b))
    - **a.** i overensstemmelse med artikel 43, stk. 2, litra a) fremlægger separat dokumentation for sin uafhængighed. Dette gælder navnlig dokumentation vedrørende finansieringen af certificeringsorganet for så vidt angår sikringen af uvildighed
    - **b.** sikrer, at dets opgaver og forpligtelser ikke fører til en interessekonflikt i henhold til artikel 43, stk. 2, litra e)
2. at certificeringsorganet ikke har nogen relevant forbindelse til den kunde, det vurderer.

4.3 Erstatningsansvar og finansiering

Akkrediteringsorganet skal ud over at opfylde kravet i 4.3.1 i ISO/IEC 17065/2012 regelmæssigt sikre, at certificeringsorganet har truffet passende foranstaltninger (f.eks. forsikring eller reserver) til dækning af erstatningsansvar i de geografiske områder, hvor det er aktivt.

4.4 Ikke-diskriminerende vilkår

Tilsynsmyndigheden kan formulere supplerende krav, hvis dette er i overensstemmelse med den nationale lovgivning.

4.5 Fortrolighed

Tilsynsmyndigheden kan formulere supplerende krav, hvis dette er i overensstemmelse med den nationale lovgivning.

4.6 Offentligt tilgængelige oplysninger

Akkrediteringsorganet skal ud over overholdelsen af kravet i 4.6 i ISO/IEC 17065/2012 som minimum kræve af certificeringsorganet, at

1. alle versioner (aktuelle og tidligere) af de godkendte kriterier, der har fundet anvendelse i henhold til artikel 42, stk. 5, publiceres og gøres let tilgængelige for offentligheden, samt at den relevante gyldighedsperiode generelt fremgår af alle certificeringsprocedurer
2. oplysninger om procedurer for behandling af klager og anker offentliggøres i henhold til artikel 43, stk. 2, litra d).

5 STRUKTURELLE KRAV, ARTIKEL 43, STK. 4 ["PASSENDE" VURDERING]

5.1 Organisationsstruktur og topledelse

Tilsynsmyndigheden kan formulere supplerende krav.

5.2 Mekanismer til sikring af uvildighed

Tilsynsmyndigheden kan formulere supplerende krav.

6 RESSOURCEKRAV

6.1 Certificeringsorganets personale

Akkrediteringsorganet skal ud over overholdelsen af kravet i afsnit 6 i ISO/IEC 17065/2012 sikre, at personalet i hvert enkelt certificeringsorgan:

1. har fremlagt dokumentation for relevant og tidssvarende ekspertise (viden og erfaring) med hensyn til databeskyttelse i henhold til artikel 43, stk. 1
2. er uafhængigt og besidder tidssvarende ekspertise med hensyn til genstanden for certificering i henhold til artikel 43, stk. 2, litra a), og ikke har nogen interessekonflikter i henhold til artikel 43, stk. 2, litra e)
3. i henhold til artikel 43, stk. 2, litra b), påtager sig at opfylde kravene i artikel 42, stk. 5
4. har relevant og passende kendskab til og erfaring med anvendelse af databeskyttelseslovgivning
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 dokumentere erfaring inden for de områder, der er nævnt i de supplerende krav, særlig 6.1.1, 6.1.4, og 6.1.5.

Personale med teknisk ekspertise:

- har erhvervet en kvalifikation på et relevant område inden for teknisk ekspertise på mindst EQF-niveau 6[20] eller en anerkendt beskyttet titel (f.eks. Dipl. Ing.) inden for det relevante lovregulerede erhverv eller har væsentlig erhvervserfaring
- *Personale med ansvar for certificeringsbeslutninger* skal have væsentlig erfaring med at identificere og gennemføre databeskyttelsesforanstaltninger
- *Personale med ansvar for evalueringer* skal have erfaring med teknisk databeskyttelse og viden og erfaring med sammenligningsprocedurer (f.eks. certificering/revision) og være registreret som relevant

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

Personale med juridisk ekspertise:

- Jurastudier ved et europæisk eller statsanerkendt universitet af en varighed på mindst otte semestre inklusiv den akademiske grad Master (LL.M.) eller tilsvarende eller væsentlig erhvervserfaring
- *Personale med ansvar for certificeringsafgørelser* skal dokumentere væsentlig erfaring med databeskyttelseslovgivning og være registreret som krævet af medlemsstaten
- *Personale med ansvar for evalueringer* skal dokumentere, at de har mindst to års erhvervserfaring med databeskyttelseslovgivning samt kendskab til og ekspertise inden for sammenligningsprocedurer (f.eks. certificering/revision) og være registreret, hvis det kræves af medlemsstaten
    - Personalet skal dokumentere, at de holder deres områderelaterede viden inden for tekniske og revisionsmæssige færdigheder ajour gennem løbende faglig udvikling.

6.2 Ressourcer til evaluering

Tilsynsmyndigheden kan formulere supplerende krav, hvis dette er i overensstemmelse med den nationale lovgivning.

7 PROCESKRAV, ARTIKEL 43, STK. 2, LITRA C) OG D)

7.1 Generelt

Akkrediteringsorganet skal ud over overholdelse af kravet i afsnit 7.1 i ISO/IEC 17065/2012 sikre følgende:

1. at certificeringsorganer overholder den kompetente tilsynsmyndigheds supplerende krav (i henhold til artikel 43, stk. 1, litra b)), når de indgiver ansøgningen, således at opgaver og forpligtelser ikke medfører en interessekonflikt i henhold til artikel 43, stk. 2, litra b)
2. at informere de relevante kompetente tilsynsmyndigheder, inden et certificeringsorgan begynder at anvende et godkendt europæisk databeskyttelsessegl i en ny medlemsstat fra et satellitkontor.

7.2 Anvendelse

Ud over punkt 7.2 i ISO/IEC 17065/2012 bør det kræves, at

[20] Se sammenligningsværktøjet i tilknytning til referencerammen for kvalifikationer på https://ec.europa.eu/ploteus/da/compare?

1. certificeringsobjektet (evalueringsmålet) er beskrevet i detaljer i ansøgningen. Dette omfatter også grænseflader og overførsler til andre systemer og organisationer, protokoller og andre garantier
2. det af ansøgningen fremgår, om der anvendes databehandlere, og i tilfælde, hvor ansøgeren er databehandlere, skal deres ansvarsområder og opgaver beskrives, og ansøgningen indeholde de(n) relevante kontrakt(er) for dataansvarlige/databehandlere.

7.3 Gennemgang af ansøgninger

Ud over punkt 7.3 i ISO/IEC 17065/2012 bør det kræves, at

1. der fastsættes bindende evalueringsmetoder med hensyn til evalueringsmålet i certificeringsaftalen
2. der i vurderingen i 7.3 litra e), med hensyn til, om niveauet af ekspertise er tilstrækkeligt, tages passende hensyn til både teknisk og juridisk ekspertise inden for databeskyttelse.

7.4 Evaluering

Ud over punkt 7.4 i ISO/IEC 17065/2012 skal certificeringsmekanismerne beskrive evalueringsmetoder, der er tilstrækkelige til at vurdere, om behandlingsaktiviteterne opfylder certificeringskriterierne, herunder eksempelvis, hvis det er relevant:

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, som tages i betragtning af den dataansvarlige og databehandleren, med hensyn til de retlige konsekvenser i henhold til artikel 30, 32, 35 og 36 i databeskyttelsesforordningen, og med hensyn til definitionen af tekniske og organisatoriske foranstaltninger i henhold til artikel 24, 25 og 32 i databeskyttelsesforordningen, i det omfang de nævnte artikler finder anvendelse på evalueringsobjektet, og
3. en metode til at vurdere de afhjælpende foranstaltninger, herunder garantier, beskyttelsesforanstaltninger og procedurer, som har til formål at sikre beskyttelsen af personoplysninger i forbindelse med den behandling, som certificeringsobjektet underkastes, og med henblik på at dokumentere, at de retlige krav, som er fastsat i kriterierne, er opfyldt og
4. dokumentation for metoder og resultater.

Det bør kræves af certificeringsorganet, at det sikrer, at disse evalueringsmetoder er standardiserede og generelt anvendelige. Dette betyder, at der anvendes sammenlignelige evalueringsmetoder til sammenlignelige evalueringsmål. Afvigelser fra denne procedure skal begrundes af certificeringsorganet.

Ud over punkt 7.4.2 i ISO/IEC 17065/2012 bør der gives tilladelse til, at evalueringen udføres af eksterne eksperter, som er anerkendt af certificeringsorganet.

Ud over punkt 7.4.5 i ISO/IEC 17065/2012 bør der stilles krav om, at databeskyttelsescertificering i overensstemmelse med artikel 42 og 43 i databeskyttelsesforordningen, som allerede dækker en del af certificeringens genstand, kan indføjes i en eksisterende certificering. Dette vil dog ikke være tilstrækkeligt til helt at erstatte (delvise) evalueringer. Certificeringsorganet er forpligtet til at kontrollere, at kriterierne overholdes. Anerkendelse kræver under alle omstændigheder en fuldstændig evalueringsrapport eller oplysninger, der muliggør en evaluering af den hidtidige certificeringsaktivitet og resultaterne heraf. En certificeringserklæring eller lignende certificeringscertifikater bør ikke betragtes som fyldestgørende erstatning for en rapport.

Ud over punkt 7.4.6 i ISO/IEC 17065/2012 bør der stilles krav om, at certificeringsorganet i sin certificeringsmekanisme i detaljer redegør for, hvordan de oplysninger, som punkt 7.4.6 indeholder krav om, oplyser kunden (certificeringsansøgeren) om afvigelser fra en certificeringsmekanisme. I denne sammenhæng bør sådanne oplysningers karakter og timing som minimum fastlægges.

Ud over punkt 7.4.9 i ISO/IEC 17065/2012 bør der stilles krav om, at dokumentation efter anmodning gøres fuldt tilgængelig for tilsynsmyndigheden for databeskyttelse.

7.5 Evaluering

Ud over punkt 7.5 i ISO/IEC 17065/2012 er der behov for procedurer for tildeling, løbende evaluering og tilbagekaldelse af de respektive certificeringer i henhold til artikel 43, stk. 2 og 3.

7.6 Certificeringsafgørelse

Ud over punkt 7.6.1 i ISO/IEC 17065/2012 bør der stilles krav om, at certificeringsorganet i sine procedurer i detaljer redegør for, hvordan dets uafhængighed og ansvar med hensyn individuelle afgørelser sikres.

7.7 Certificeringsdokumentation

Ud over punkt 7.7.1.e i ISO/IEC 17065/2012 og i overensstemmelse med artikel 42, stk. 7, i databeskyttelsesforordningen bør der stilles krav om, at certificeringers gyldighedsperiode ikke må overstige tre år.

Ud over punkt 7.7.1.e i ISO/IEC 17065/2012 bør der stilles krav om, at den planlagte overvågningsperiode som defineret i afsnit 7.9 også dokumenteres.

Ud over punkt 7.7.1.f i ISO/IEC 17065/2012 bør der stilles krav om, at certificeringsorganet identificerer certificeringsobjektet i certificeringsdokumentationen (med angivelse af versionens status eller lignende egenskaber, hvis det er relevant).

7.8 Register over certificerede produkter

Ud over punkt 7.8 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til at opbevare oplysningerne om tilgængelige certificerede produkter, processer og tjenester internt og offentligt tilgængelige. Certificeringsorganet skal fremlægge et resumé af evalueringsrapporten for offentligheden. Formålet med dette resumé er at bidrage til gennemsigtigheden med hensyn til, hvad der er blevet certificeret, og hvordan det blev vurderet. Det vil indeholde redegørelser om bl.a.:

(a) certificeringens anvendelsesområde og en meningsfuld beskrivelse af certificeringsobjektet (evalueringsmålet)

(b) de respektive certificeringskriterier (herunder version eller funktionsstatus)

(c) evalueringsmetoder og gennemførte test og

(d) resultat(er).

Ud over punkt 7.8 i ISO/IEC 17065/2012 og i henhold til artikel 43, stk. 5, i databeskyttelsesforordningen informerer certificeringsorganet de kompetente tilsynsmyndigheder om grundlaget for tildeling eller tilbagekaldelse af den ønskede certificering.

7.9 Overvågning

Ud over punkt 7.9.1, 7.9.2 og 7.9.3 i ISO/IEC 17065/2012 og i henhold til artikel 43, stk. 2, litra c), i databeskyttelsesforordningen bør der stilles krav om regelmæssige overvågningsforanstaltninger med henblik på at opretholde certificeringen i overvågningsperioden.

7.10 Ændringer, der påvirker certificeringen

Ud over punkt 7.10.1 og 7.10.2 i EN ISO/IEC 17065/2012 omfatter ændringer, der påvirker certificering, som certificeringsorganet skal tage stilling til, følgende: ændringer af databeskyttelseslovgivningen, vedtagelse af delegerede retsakter fra Europa-Kommissionen i overensstemmelse med artikel 43, stk. 8 og 9, Det Europæiske Databeskyttelsesråds afgørelser og retsafgørelser vedrørende databeskyttelse. De ændringsprocedurer, som der skal indgås aftale om her, omfatter bl.a.: overgangsperioder, godkendelsesprocesser med kompetente tilsynsmyndigheder, revurdering af det relevante certificeringsobjekt og passende foranstaltninger til tilbagekaldelse en certificering, hvis den certificerede behandlingsaktivitet ikke længere opfylder de ajourførte kriterier.

7.11 Ophævelse, begrænsning, suspension eller tilbagetrækning af certificering

Ud over kapitel 7.11.1 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til, hvis det er relevant, omgående og skriftligt at underrette den kompetente tilsynsmyndighed og det nationale akkrediteringsorgan om trufne foranstaltninger og om videreførelse, begrænsning, suspension og tilbagetrækning af certificering.

Ifølge artikel 58, stk. 2, litra h), er certificeringsorganet forpligtet til at modtage afgørelser og påbud fra den kompetente tilsynsmyndighed om at tilbagetrække eller undlade at udstede certificering til en kunde (ansøger), hvis certificeringskravene ikke eller ikke længere er opfyldt.

7.12 Register

Certificeringsorganet bør være forpligtet til at opbevare al dokumentation i fuldstændig, forståelig, ajourført og revisionsegnet form.

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

Ud over punkt 7.13.1 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til at fastsætte:

(a) hvem der kan indgive klager eller indsigelser

(b) hvem der behandler dem på certificeringsorganets vegne

(c) hvilke kontroller, der finder sted i denne forbindelse og

(d) mulighederne for høring af interesserede parter.

Ud over punkt 7.13.2 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til at fastsætte:

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

(b) de hermed forbundne frister og

(c) hvilke processer der skal iværksættes efterfølgende.

Ud over punkt 7.13.1 i ISO/IEC 17065/2012 skal certificeringsorganet fastsætte, hvordan det sikres, at certificeringsaktiviteter og behandling af anker og klager holdes adskilt.

8 KRAV TIL FORVALTNINGSSYSTEM

Et generelt krav til forvaltningssystemet er ifølge kapitel 8 i ISO/IEC 17065/2012, 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 forvaltningsprincip er at skabe et system, hvor målene fastsættes på en effektiv måde, især: gennemførelsen af certificeringstjenesterne ved hjælp af egnede specifikationer. Dette kræver, at certificeringsorganets gennemførelse af akkrediteringskravene er gennemsigtig og kontrollerbar, og at kravene overholdes permanent.

Med henblik herpå skal forvaltningssystemet indeholde en metode til i overensstemmelse med bestemmelserne om databeskyttelse at opfylde og kontrollere disse krav og til løbende at følge op på dem med det akkrediterede organ.

Disse forvaltningsprincipper og den dokumenterede gennemførelse heraf skal være gennemsigtige og offentliggøres af det akkrediterede certificeringsorgan i overensstemmelse med akkrediteringsproceduren i henhold til artikel 58 og derefter på anmodning af databeskyttelsesmyndigheden til enhver tid i løbet af en undersøgelse i form af databeskyttelsesevalueringer i henhold til artikel 58, stk. 1, litra b), eller en evaluering af de certificeringer, der er udstedt i overensstemmelse med artikel 42, stk. 7, i henhold til artikel 58, stk. 1, litra c).

Det akkrediterede certificeringsorgan skal navnlig permanent og løbende offentliggøre, hvilke certificeringer der er udført på hvilket grundlag (eller certificeringsmekanismer eller -ordninger), hvor længe certificeringerne er gyldige inden for hvilke rammer og på hvilke betingelser (betragtning 100).

8.1 Krav til det generelle forvaltningssystem

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.2 Dokumentation for forvaltningssystem

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.3 Dokumentstyring

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.4 Styring af registreringer

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.5 Gennemgang af ledelsesforhold

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.6 Intern revision

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.7 Korrigerende foranstaltninger

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

8.8 Forebyggende foranstaltninger

Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.

9 YDERLIGERE SUPPLERENDE KRAV21

9.1 Ajourføring af evalueringsmetoder

Certificeringsorganet opretter procedurer med det formål at styre ajourføringen af evalueringsmetoderne med henblik på anvendelse i forbindelse med evalueringen under punkt 7.4. Ajourføringen skal finde sted i forbindelse med ændringer af de retlige rammer, de relevante risici, den nyeste viden og de omkostninger, der er forbundet med gennemførelsen af tekniske og organisatoriske foranstaltninger.

9.2 Opretholdelse af ekspertise

Certificeringsorganer indfører procedurer for at sikre uddannelse af deres ansatte med henblik på at ajourføre deres kvalifikationer under hensyntagen til udviklingerne på listen i punkt 9.1.

9.3 Ansvar og kompetencer

9.3.1 Kommunikation mellem certificeringsorganet og dets kunder

Der skal indføres procedurer for gennemførelsen af passende procedurer og kommunikationsstrukturer mellem certificeringsorganet og dets kunde. Dette omfatter:

1. at certificeringsorganet opbevarer dokumentation for opgaver og ansvarsområder med henblik på:
    a. 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 for en ansøgning
    b. evalueringer foretaget af den kompetente tilsynsmyndighed med hensyn til:
        i. feedback
        ii. afgørelser truffet af den kompetente tilsynsmyndighed.

9.3.2 Dokumentation for evalueringsaktiviteter

Tilsynsmyndigheden kan formulere supplerende krav.

9.3.3 Forvaltning af klagebehandling

Som en integrerende del af forvaltningssystemet skal der indføres en klagebehandlingsprocedure, som navnlig har til formål at sikre, at kravene i punkt 4.1.2.2, litra c), 4.1.2.2, litra j), 4.6, litra d), og 7.13 i ISO/IEC 17065/2012 gennemføres.

Relevante klager og indsigelser bør deles med den kompetente tilsynsmyndighed.

9.3.4 Forvaltning af tilbagetrækning

Procedurerne i tilfælde af suspension eller tilbagetrækning af akkrediteringen skal integreres i certificeringsorganets forvaltningssystem, og dette gælder også for underretning af kunderne.

[21] Den kompetente tilsynsmyndighed kan fastsætte og tilføje yderligere krav, hvis dette er i overensstemmelse med den nationale lovgivning.