Udtalelse 26/2020 om udkast til afgørelse fra Danmarks kompetente tilsynsmyndigheder vedrørende godkendelse af krav til akkreditering af et certificeringsorgan i medfør af artikel 43, stk. 3 (GDPR)

Vedtaget den 7. december 2020

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 63, artikel 64, stk. 1, litra c), og stk. 3-8, samt artikel 43, stk. 3, 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 (i det følgende benævnt "databeskyttelsesforordningen"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 dertil, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018,[1]

under henvisning til artikel 10 og artikel 22 i forretningsordenen af 25. maj 2018, og

ud fra følgende betragtninger:

(1) Databeskyttelsesrådets vigtigste rolle er at sikre ensartet anvendelse af forordning 2016/679 (i det følgende benævnt "databeskyttelsesforordningen") i hele Det Europæiske Økonomiske Samarbejdsområde. Databeskyttelsesrådet afgiver i overensstemmelse med artikel 64, stk. 1, i databeskyttelsesforordningen en udtalelse, når en kompetent tilsynsmyndighed har til hensigt at godkende kravene til akkreditering af certificeringsorganer i henhold artikel 43. Formålet med denne udtalelse er således at udarbejde en harmoniseret tilgang med hensyn til de krav, som en datatilsynsmyndighed eller det nationale akkrediteringsorgan vil anvende ved akkreditering af et certificeringsorgan. Selv om databeskyttelsesforordningen ikke pålægger et enkelt sæt krav til akkreditering, fremmer den dog ensartethed. Databeskyttelsesrådet søger i første omgang at nå dette mål med sine udtalelser ved at tilskynde tilsynsmyndigheder til at udarbejde et udkast til deres krav til akkreditering i henhold til strukturen i Databeskyttelsesrådets retningslinjer for akkreditering af certificeringsorganer, og i anden omgang ved at analysere dem på baggrund af en skabelon fra Databeskyttelsesrådet, der giver mulighed for at sammenholde kravene (reguleret af ISO 17065 og af Databeskyttelsesrådets retningslinjer for akkreditering af certificeringsorganer).

(2) For så vidt angår artikel 43 i databeskyttelsesforordningen vedtager de kompetente tilsynsmyndigheder krav til akkreditering. De anvender sammenhængsmekanismen for at skabe tillid til certificeringsmekanismen, navnlig ved at fastsætte krav på et højt niveau.

(3) Krav til akkreditering er underlagt sammenhængsmekanismen, det betyder imidlertid ikke, at kravene skal være identiske. De kompetente tilsynsmyndigheder har skønsbeføjelser for så vidt angår den nationale eller regionale sammenhæng, og de bør tage den lokale lovgivning i betragtning. Formålet med Databeskyttelsesrådets udtalelse er ikke at nå et fælles sæt EU-krav men snarere at undgå betydelige uoverensstemmelser, som f.eks. kan påvirke tilliden til akkrediterede certificeringsorganers uafhængighed.

(4) "Vejledning 4/2018 om akkreditering af certificeringsorganer i henhold til artikel 43 i den generelle forordning om databeskyttelse (2016/679)" (i det følgende benævnt "vejledningen") og "Retningslinjer 1/2018 vedrørende certificering og identifikation af certificeringskriterier i

[1] Henvisninger til "Unionen" i denne udtalelse skal forstås som henvisninger til "EØS".

overensstemmelse med artikel 42 og 43 i forordningen" vil fungere som rettesnor i forbindelse med sammenhængsmekanismen.

(5) Hvis en medlemsstat fastsætter, at certificeringsorganerne skal akkrediteres af tilsynsmyndigheden, bør tilsynsmyndigheden fastsætte akkrediteringskrav, herunder, men ikke begrænset til, kravene i artikel 43, stk. 2. I forhold til forpligtelserne vedrørende nationale akkrediteringsorganers akkreditering af certificeringsorganer, indeholder artikel 43 færre oplysninger om kravene til akkreditering, når tilsynsmyndigheden selv foretager akkrediteringen. For at bidrage til en harmoniseret tilgang til akkreditering bør de akkrediteringskrav, som anvendes af tilsynsmyndigheden, reguleres af ISO/IEC 17065 og suppleres af de supplerende krav, som en tilsynsmyndighed fastsætter i henhold til artikel 43, stk. 1, litra b). Databeskyttelsesrådet bemærker, at artikel 43, stk. 2, litra a) til e), afspejler og specificerer krav i ISO 17065, som vil bidrage til sammenhæng.[2]

(6) Databeskyttelsesrådets udtalelse vedtages i overensstemmelse med artikel 64, stk. 1, litra c), og stk. 3 og 8, i databeskyttelsesforordningen sammenholdt med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden inden for otte uger regnet fra den første arbejdsdag, efter formanden og den kompetente tilsynsmyndighed har konkluderet, at aktpakken er fuldstændig. Efter formandens afgørelse kan denne frist forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet —

VEDTAGET FØLGENDE UDTALELSE:

1 KORTFATTET FREMSTILLING AF DE FAKTISKE OMSTÆNDIGHEDER

1. Den danske tilsynsmyndighed har indsendt sit udkast til akkrediteringskrav til Databeskyttelsesrådet i medfør af artikel 43, stk. 1, litra b). Sagsakterne blev anset for fuldstændige den 12. oktober 2020. Det danske nationale akkrediteringsorgan udfører akkreditering af certificeringsorganer på baggrund af certificeringskriterierne i databeskyttelsesforordningen. Det betyder, at det nationale akkrediteringsorgan vil benytte ISO 17065 og de supplerende krav, der er fastsat af tilsynsmyndigheden, når denne har godkendt dem, i henhold til en udtalelse fra Databeskyttelsesrådet om udkastet til krav til at akkreditere certificeringsorganer.

2 VURDERING

2.1 Databeskyttelsesrådets generelle ræsonnement vedrørende det indsendte udkast til afgørelse

2. Formålet med denne udtalelse er at vurdere akkrediteringskravene, som er udarbejdet af en tilsynsmyndighed, enten i forbindelse med ISO 17065 eller et komplet sæt krav med henblik på, at et

[2] Retningslinjer 4/2018 om akkreditering af certificeringsorganer i henhold til artikel 43 i den generelle forordning om databeskyttelse, stk. 39. tilgængelig på: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

nationalt akkrediteringsorgan eller en tilsynsmyndighed, i overensstemmelse med artikel 43, stk. 1, i databeskyttelsesforordningen, kan akkreditere et certificeringsorgan, der har ansvar for udstedelse og fornyelse af certificeringer i medfør af artikel 42 i databeskyttelsesforordningen. Dette berører ikke den kompetente tilsynsmyndigheds opgaver og beføjelser. I denne konkrete sag bemærker Databeskyttelsesrådet, at den danske tilsynsmyndighed, selvom den sammen med Den Danske Akkrediteringsfond er bemyndiget til at udstede akkreditering til certificeringsorganer, har besluttet at anvende sit nationale akkrediteringsorgan til udstedelse af akkreditering, og at de har samlet supplerende krav i overensstemmelse med retningslinjerne, som det nationale akkrediteringsorgan skal benytte ved udstedelse af akkreditering.

3. Denne vurdering af den danske tilsynsmyndigheds supplerende akkrediteringskrav har til formål at undersøge afvigelser (tilføjelser eller udeladelser) fra retningslinjerne og navnlig bilag 1. Derudover er Databeskyttelsesrådets udtalelse koncentreret om alle forhold, der kan påvirke en ensartet tilgang for så vidt angår akkrediteringen af certificeringsorganer.

4. Det bør påpeges, at formålet med vejledningen om akkreditering af certificeringsorganer er at bistå tilsynsmyndighederne i deres fastlæggelse af akkrediteringskrav. Bilaget til vejledningen udgør ikke som sådan akkrediteringskrav. Akkrediteringskrav til certificeringsorganer skal derfor fastlægges af tilsynsmyndigheden på en sådan måde, at de kan anvendes i praksis og på en ensartet måde i henhold til det område, hvor tilsynsmyndigheden opererer.

5. Databeskyttelsesrådet anerkender, at nationale akkrediteringsorganer, på grund af deres ekspertise, bør have en vis handlefrihed med hensyn til at fastlægge visse specifikke bestemmelser inden for rammerne af gældende akkrediteringskrav. Databeskyttelsesrådet finder det imidlertid nødvendigt at understrege, at når der fastsættes supplerende krav, skal de fastsættes således, at de kan anvendes i praksis og på en ensartet måde og revideres efter behov.

6. Databeskyttelsesrådet påpeger, at ISO-standarder, navnlig ISO 17065, er genstand for intellektuel ejendomsret, og at det i sin udtalelse derfor ikke vil henvise til ordlyden i det tilknyttede dokument. Databeskyttelsesrådet besluttede derfor, hvor det er relevant, at henvise til de specifikke afsnit i ISO-standarden, uden dog at gengive ordlyden.

7. Endelig har Databeskyttelsesrådet gennemført sin vurdering i henhold til strukturen i bilag 1 til vejledningen (herefter benævnt "bilaget"). Hvor denne udtalelse ikke nævner noget om et specifikt afsnit af den danske tilsynsmyndigheds udkast til akkrediteringskrav, skal det læses, som at Databeskyttelsesrådet ikke har nogen bemærkninger, og at den danske tilsynsmyndighed ikke anmodes om at træffe yderligere foranstaltninger.

8. Denne udtalelse omfatter ikke forhold fremlagt af den danske tilsynsmyndighed, som falder uden for anvendelsesområdet for artikel 43, stk. 2, i databeskyttelsesforordningen, såsom henvisninger til national lovgivning. Ikke desto mindre konstaterer Databeskyttelsesrådet, at national lovgivning bør være i overensstemmelse med databeskyttelsesforordningen, hvor det er påkrævet.

2.2 De vigtigste fokusområder i vurderingen (artikel 43, stk. 2, i databeskyttelsesforordningen og bilag 1 til Databeskyttelsesrådets vejledning) er, at akkrediteringskrav sikrer, at følgende anvendes på en ensartet måde:

a. idet alle centrale områder, der er fremhævet i bilaget til vejledningen, behandles, og enhver afvigelse fra bilaget tages i betragtning

b. certificeringsorganets uafhængighed

c. certificeringsorganets interessekonflikter

d. certificeringsorganets ekspertise

e. passende sikkerhedsforanstaltninger til at sikre, at certificeringskriterierne i databeskyttelsesforordningen anvendes korrekt af certificeringsorganet

f. procedurer for udstedelse, regelmæssig revision og tilbagetrækning af en certificering i medfør af databeskyttelsesforordningen samt

g. gennemsigtig behandling af klager om overtrædelser af certificeringen.

9. Under hensyntagen til at:

a. artikel 43, stk. 2, i databeskyttelsesforordningen indeholder en liste over de akkrediteringspunkter, et certificeringsorgan skal opfylde for at blive akkrediteret

b. artikel 43, stk. 3, i databeskyttelsesforordningen fastsætter, at kravene til akkreditering af certificeringsorganer godkendes af den kompetente tilsynsmyndighed

c. artikel 57, stk. 1, litra p) og q), i databeskyttelsesforordningen, fastsætter, at en kompetent tilsynsmyndighed skal opstille og offentliggøre kravene til akkreditering af certificeringsorganer, og at den kan beslutte selv at foretage akkrediteringen af certificeringsorganer

d. artikel 64, stk. 1, litra c), i databeskyttelsesforordningen fastsætter, at Databeskyttelsesrådet afgiver en udtalelse, når en tilsynsmyndighed har til hensigt at godkende kriterierne for akkreditering af et certificeringsorgan i henhold til artikel 43, stk. 3

e. hvis akkreditering udføres af det nationale akkrediteringsorgan i overensstemmelse med ISO/IEC 17065/2012, skal de supplerende krav, der er fastsat af den kompetente tilsynsmyndighed, også anvendes

f. bilag 1 til vejledningen om akkreditering af certificering indeholder forslag til krav, som en datatilsynsmyndighed skal udarbejde, og som finder anvendelse ved det nationale akkrediteringsorgans akkreditering af et certificeringsorgan

er Databeskyttelsesrådet af følgende holdning:

2.2.1 GENERELLE KRAV TIL AKKREDITERING (afsnit 4 i udkastet til akkrediteringskrav)

10. Med hensyn til stk. 3 i afsnit 4.1.1 "Juridisk ansvar" i den danske tilsynsmyndigheds udkast til akkrediteringskrav er det Databeskyttelsesrådets opfattelse, at certificeringsorganet bør bekræfte over for akkrediteringsorganet, at de ikke blot ikke er genstand for nogen form for undersøgelse eller reguleringsindgreb fra Datatilsynet i Danmark, men at de heller ikke tidligere har været genstand for nogen form for undersøgelse eller reguleringsindgreb. Databeskyttelsesrådet tilskynder derfor den danske tilsynsmyndighed til at præcisere ordlyden i overensstemmelse hermed.

11. Med hensyn til samme afsnit, sidste led, opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til at gøre det klart, at der forud for akkreditering kan tilføjes yderligere krav og

procedurer rettet mod kontrol af certificeringsorganers overholdelse af databeskyttelsesforordningen.

12. Databeskyttelsesrådet understreger vigtigheden af fuld gennemsigtighed fra certificeringsorganets side over for Datatilsynet hvad angår certificeringsproceduren. Styrelsen opfordrer i den forbindelse, for så vidt angår punkt 4.1.2, stk. 2, i certificeringsaftalen, den danske tilsynsmyndighed til at præcisere, hvad der menes med udtrykket "ellers", særligt hvorvidt lovpålagt fortrolighed er omfattet af denne bestemmelse.

13. Med hensyn til afsnit 4.2 "Håndtering af upartiskhed" opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til at give flere eksempler på situationer, hvor certificeringsorganet ikke har nogen relevant tilknytning til den kunde, det vurderer. Specielt kan krav om akkreditering af et certificeringsorgan indsendt af den tyske tilsynsmyndighed og den østrigske myndighed være en hjælp i denne henseende[3].

2.2.2 KRAV TIL RESSOURCER (afsnit 6 i udkastet til akkrediteringskrav)

14. Databeskyttelsesrådet noterer sig, at den danske tilsynsmyndigheds akkrediteringskrav giver mulighed for udlicitering af visse aktiviteter. Med hensyn til adgang til en person med relevant ekspertise og passende kvalifikationer på fagligt niveau ("Certificeringsorganets personale", afsnit 6.1.6), anbefaler Databeskyttelsesrådet den danske tilsynsmyndighed tydeligt at understrege, at certificeringsorganet bevarer ansvaret for beslutningstagningen, selv når den bruger eksterne eksperter [4] . Databeskyttelsesrådet fremhæver, at eksterne aktører ikke bør inddrages i beslutningsprocessen, og at dette skal understreges tydeligt i kravene.

15. For så vidt angår samme afsnit og henvisningen til personale, der er ansvarligt for certificeringsbeslutninger, opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til at tilpasse kravenes ordlyd til retningslinjernes ordlyd, ved at tilføje en henvisning til databeskyttelseslovgivningen, dvs. "væsentlig erhvervserfaring inden for databeskyttelseslovgivning, herunder identifikation og gennemførelse af databeskyttelsesforanstaltninger".

[3] For mulige eksempler se udtalelse 15/2020 om udkastet til afgørelse fra de kompetente tilsynsmyndigheder i Tyskland vedrørende godkendelse af kravene til akkreditering af et certificeringsorgan i henhold til artikel 43, stk. 3 (GDPR) - afsnit 19 eller udtalelse 9/2019 om den østrigske datatilsynsmyndigheds udkast til akkrediteringskrav for et organ til kontrol af godkendte adfærdskodekser i henhold til artikel 41 GDPR - afsnit 20.

[4] Det Europæiske Databeskyttelsesråd udarbejdede dette krav i udtalelse 16/2020 om udkastet til afgørelse fra de kompetente tilsynsmyndigheder i Den Tjekkiske Republik vedrørende godkendelse af kravene til akkreditering af et certificeringsorgan i henhold til artikel 43, stk. 3 (GDPR) - afsnit 24, og udtalelse 5/2020 om den østrigske datatilsynsmyndigheds udkast til akkrediteringskrav for et organ til kontrol af godkendte adfærdskodekser i henhold til artikel 43,3 GDPR - se afsnit 14.

2.2.3 Krav til procedurer, artikel 43, stk. 2, litra c) og d) (afsnit 7 i udkastet til akkrediteringskrav)

16. For så vidt angår punkt 7.2 "Ansøgning" og kravet om at underrette den danske tilsynsmyndighed om en modtaget ansøgning, opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til i sidste punktum at angive, i hvilken form anmeldelsen skal indsendes af certificeringsorganet.

17. For så vidt angår afsnit 7.4 "Evaluering", 3. led, anbefaler Databeskyttelsesrådet den danske tilsynsmyndighed at tilføje ikke blot de respektive krav i ISO 17065, men også den danske tilsynsmyndigheds yderligere krav, som skal opfyldes af underleverandøren, samt for at understrege, at underleverance ikke fritager certificeringsorganet fra dets ansvar.

18. Vedrørende afsnit 7.6 "Certificeringsbeslutning" understreger Databeskyttelsesrådet, at certificeringsorganet bør fastlægge detaljerede procedurer for sikring af dets uafhængighed og ansvar. Af denne grund anbefaler Databeskyttelsesrådet den danske tilsynsmyndighed at tilføje følgende sætning i begyndelsen af punkt 7.6 "Certificeringsbeslutning": "Ud over punkt 7.6.1 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til i sine procedurer detaljeret at fastsætte, hvordan dets uafhængighed og ansvar med hensyn til individuelle certificeringsbeslutninger sikres".

19. Databeskyttelsesrådet understreger vigtigheden af at oplyse om årsager til tildeling eller tilbagekaldelse af certificering. Af denne grund anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed i afsnit 7.8 "Fortegnelse over certificerede produkter" tilføjer henvisningen til certificeringsorganets pligt til at informere om tildeling/tilbagekaldelse af den certificering, der er anmodet om, herunder præcisering af, i hvilken form sådanne oplysninger skal gives.

3 KONKLUSIONER/ANBEFALINGER

20. Den danske tilsynsmyndigheds udkast til krav til akkreditering kan føre til, at certificeringsorganerne anvender akkrediteringen på en usammenhængende måde, og følgende ændringer skal foretages:

21. Vedrørende "ressourcekrav" anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed:

    1) i afsnit 6.1.6 "Certificeringsorganets personale" tydeligt præciserer, at certificeringsorganet bibeholder ansvaret for beslutningstagningen, selv når det bruger eksterne eksperter.

22. Vedrørende "krav til procedurer" anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed:

    1) i afsnit 7.4 "Evaluering", 3. led, ikke blot tilføjer de respektive krav i ISO 17065, men også den danske tilsynsmyndigheds yderligere krav, som skal opfyldes af underleverandøren, samt understreger, at underleverance ikke fritager certificeringsorganet fra dets ansvar.
    2) i afsnit 7.6 "Certificeringsbeslutning" tilføjer følgende sætning: "Ud over punkt 7.6.1 i ISO/IEC 17065/2012 bør certificeringsorganet være forpligtet til i sine procedurer detaljeret at fastsætte, hvordan dets uafhængighed og ansvar med hensyn til individuelle certificeringsbeslutninger sikres".

3) i afsnit 7.8 "Fortegnelse over certificerede produkter" tilføjer henvisningen til certificeringsorganets pligt til at informere om tildeling/tilbagekaldelse af den certificering, der er anmodet om, herunder præcisering af, i hvilken form sådanne oplysninger skal gives.

4 AFSLUTTENDE BEMÆRKNINGER

23. Denne udtalelse er rettet til den danske tilsynsmyndighed og offentliggøres i henhold til artikel 64, stk. 5, litra b), i databeskyttelsesforordningen.

24. I henhold til artikel 64, stk. 7 og 8, i databeskyttelsesforordningen giver den danske tilsynsmyndighed senest to uger efter modtagelsen af udtalelsen formanden elektronisk meddelelse om, hvorvidt den agter at ændre eller fastholde sit udkast til listen. Tilsynsmyndigheden skal inden for samme tidsperiode forelægge det ændrede udkast til afgørelse eller, hvis det helt eller delvist ikke agter at følge udtalelsen fra Databeskyttelsesrådet, give en relevant begrundelse herfor.

25. Den danske tilsynsmyndighed skal meddele sin endelige afgørelse til Databeskyttelsesrådet med henblik på opførelse i registret over afgørelser, der er blevet behandlet i sammenhængsmekanismen, i overensstemmelse med artikel 70, stk. 1, litra y), i databeskyttelsesforordningen.

For Det Europæiske Databeskyttelsesråd —

Formanden

(Andrea Jelinek)