Udtalelse 15/2020 om udkast til afgørelse fra Tysklands kompetente tilsynsmyndigheder vedrørende godkendelse af krav til akkreditering af et certificeringsorgan i medfør af artikel 43, stk. 3 (GDPR)

Vedtaget den 25. maj 2020

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

Vedtaget

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 bilag 1 til Databeskyttelsesrådets vejledning (vejledning 4/2018 om 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 vejledning om 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 yderligere 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 RESUMÉ AF DE FAKTISKE OMSTÆNDIGHEDER

1. De tyske tilsynsmyndigheder i føderationen og delstaterne (herefter benævnt "de tyske tilsynsmyndigheder") har indsendt sine akkrediteringskrav i henhold til artikel 43, stk. 1, litra b), til Databeskyttelsesrådet. Sagsakterne blev anset for fuldstændige den 13. februar 2020. Tysklands nationale akkrediteringsorgan, DAkkS, udfører akkreditering af certificeringsorganer på baggrund af certificeringskriterierne i databeskyttelsesforordningen. Det betyder, at det nationale akkrediteringsorgan vil benytte ISO 17065 og de yderligere krav, der er fastsat af de tyske tilsynsmyndigheder, når disse har godkendt dem, i henhold til en udtalelse fra Databeskyttelsesrådet om udkastet til krav til at akkreditere certificeringsorganer.

2. I overensstemmelse med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden har formanden på grund af det foreliggende spørgsmåls kompleksitet besluttet at forlænge den oprindelige frist for vedtagelse af en udtalelse på otte uger med yderligere seks uger.

[2] Vejledning 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_da

2 VURDERING

2.1 Databeskyttelsesrådets generelle ræsonnement vedrørende det indsendte udkast til afgørelse

3. 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 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 de tyske tilsynsmyndigheder har besluttet at anvende sit nationale akkrediteringsorgan, DAkkS, til fælles akkreditering og den kompetente tilsynsmyndighed til udstedelse af akkreditering, og de har samlet yderligere krav i overensstemmelse med vejledningen, som skal benyttes ved udstedelse af akkreditering.

4. Denne vurdering af de tyske tilsynsmyndigheders yderligere akkrediteringskrav har til formål at undersøge afvigelser (tilføjelser eller udeladelser) fra vejledningen 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.

5. 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 tilsynsmyndighederne på en sådan måde, at de kan anvendes i praksis og på en ensartet måde i henhold til det område, hvor tilsynsmyndighederne opererer.

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

7. 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.

8. 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 de tyske tilsynsmyndigheders udkast til akkrediteringskrav, skal det læses således, at Databeskyttelsesrådet ikke har nogen bemærkninger, og at de tyske tilsynsmyndigheder ikke anmodes om at træffe yderligere foranstaltninger.

9. Denne udtalelse omfatter ikke forhold fremlagt af de tyske tilsynsmyndigheder, 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:

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

2) certificeringsorganets uafhængighed

3) certificeringsorganets interessekonflikter

4) certificeringsorganets ekspertise

5) passende sikkerhedsforanstaltninger til at sikre, at certificeringskriterierne i databeskyttelsesforordningen anvendes korrekt af certificeringsorganet

6) procedurer for udstedelse, regelmæssig revision og tilbagetrækning af en certificering i medfør af databeskyttelsesforordningen samt

7) gennemsigtig behandling af klager om overtrædelser af certificeringen.

10. 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 skal 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 vejledning 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 PRÆFIKS

11. Databeskyttelsesrådet anerkender, at samarbejdsvilkår, der regulerer forholdet mellem et nationalt akkrediteringsorgan og dets datatilsynsmyndighed, ikke i sig selv er et krav til akkrediteringen af certificeringsorganer. Af hensyn til fuldstændighed og gennemsigtighed er Databeskyttelsesrådet dog af den holdning, at sådanne samarbejdsvilkår i givet fald skal offentliggøres i et format, som tilsynsmyndigheden finder passende.

2.2.2 BEGREBER OG DEFINITIONER

12. Databeskyttelsesrådet bemærker, at kapitel 3 ("Definitioner") i de tyske tilsynsmyndigheders udkast til akkrediteringskrav fastlægger, hvilke typer certificeringsordninger der er tilladt, og det angives, at de skal opfylde kravene i DIN EN ISO/IEC 17065. I den forbindelse skal det nævnes, at afsnit 5.1 og 5.2 i Databeskyttelsesrådets vejledning allerede præciserer, hvad der kan certificeres i henhold til databeskyttelsesforordningen på en udtømmende måde. Derfor anerkender Databeskyttelsesrådet, at de tyske tilsynsmyndigheders hensigt ikke er at begrænse det, der er angivet i vejledningen, og at påstandene indeholdt i kapitel 3 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav skal anses for at være gældende i forbindelse med disse akkrediteringskrav.

2.2.3 GENERELLE BEMÆRKNINGER

13. Databeskyttelsesrådet bemærker, at afsnittet "Generelle bemærkninger" i de tyske tilsynsmyndigheders akkrediteringskrav henviser til Databeskyttelsesrådets "autorisation" af certificeringskriterier "i henhold til artikel 63 og 64, stk. 1, litra c), i databeskyttelsesforordningen". Databeskyttelsesrådet bemærker, at databeskyttelsesforordningen ikke giver Databeskyttelsesrådet kompetence til at "autorisere" certificeringskriterier. I henhold til ovennævnte artikler kan Databeskyttelsesrådet dog godkende certificeringskriterier. Derfor anbefaler Databeskyttelsesrådet, at de tyske tilsynsmyndigheder sletter henvisningen til "Databeskyttelsesrådets autorisation" med henblik på at bringe udkastet i overensstemmelse med ordlyden i databeskyttelsesforordningen.

2.2.4 GENERELLE KRAV TIL AKKREDITERING (kapitel 4 i udkastet til akkrediteringskrav)

14. Hvad angår kravene til retligt ansvar (afsnit 4.1 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav), bemærker Databeskyttelsesrådet, at de tyske tilsynsmyndigheder i støttedokumentet forklarer, at der er en forventning om, at certificeringsorganet skal have tidssvarende procedurer, og der er derfor ingen grund til at tilføje flere krav i forbindelse hermed. Databeskyttelsesrådet finder dog, at en forventning ikke forpligter certificeringsorganer til at have sådanne procedurer. Som fastlagt i afsnit 4.1.1 i bilaget til vejledningen skal certificeringsorganer have tidssvarende procedurer, som lever op til det retlige ansvar, der er fastsat i akkrediteringsbetingelserne. Desuden skal certificeringsorganet kunne fremlægge dokumentation for, at dets procedurer og foranstaltninger, som specifikt vedrører styring og håndtering af kundeorganisationens personoplysninger, overholder dataforordningen. Derfor anbefaler Databeskyttelsesrådet de tyske tilsynsmyndigheder at ændre udkastet til krav med henblik på at bringe dem i overensstemmelse med vejledningen.

15. Hvad angår underafsnit 4.1.2.2 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("certificeringsaftale"), bemærker Databeskyttelsesrådet, at de tyske tilsynsmyndigeders udkast til akkrediteringskrav ikke indeholder forpligtelsen til at give den kompetente tilsynsmyndighed fuld

indsigt i certificeringsproceduren, herunder kontraktligt fortrolige spørgsmål. Derudover er der ingen henvisning til ansøgerens forpligtelse til at give certificeringsorganet adgang til vedkommendes behandlingsaktiviteter. Derfor anbefaler Databeskyttelsesrådet de tyske tilsynsmyndigheder at medtage de ovennævnte forpligtelser i deres udkast.

16. Databeskyttelsesrådet bemærker, at den eksplicitte henvisning til den kompetente tilsynsmyndigheds opgaver og beføjelser (3. led i afsnit 4.1.2 i bilaget) ikke fremgår af underafsnit 4.1.2.2 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav. Databeskyttelsesrådet er af den holdning, at denne henvisning skal tilføjes til udkastet til krav og anbefaler derfor de tyske tilsynsmyndigheder at ændre udkastet i overensstemmelse hermed.

17. Desuden indeholder de tyske tilsynsmyndigheders krav vedrørende certificeringsaftalen ikke forpligtelsen til at tillade certificeringsorganet at fremlægge alle de oplysninger, der er nødvendige for at udstede en certificering i henhold artikel 42, stk. 8, og artikel 43, stk. 5, i databeskyttelsesforordningen (7. led i afsnit 4.1.2 i bilaget). Selv om denne forpligtelse fremgår af afsnittet om forvaltning af processer i de tyske tilsynsmyndigheders udkast til akkrediteringskrav, finder Databeskyttelsesrådet, at den skal være en del af certificeringsaftalen med henblik på at understrege dens bindende karakter. Dermed anbefaler Databeskyttelsesrådet de tyske tilsynsmyndigheder at medtage den ovennævnte forpligtelse som en del af elementerne i certificeringsaftalen.

18. I henhold til bilaget skal ansøgeren underrette certificeringsorganet i tilfælde af væsentlige ændringer af vedkommendes faktiske eller retlige stilling samt produkter, processer og tjenesteydelser, der er berørt af certificeringen (10. led i afsnit 4.1.2 i bilaget). I de tyske tilsynsmyndigheders udkast til akkrediteringskrav indeholder 6. led i underafsnit 4.1.2.2 dog kun forpligtelsen til at underrette certificeringsorganet i tilfælde af væsentlige ændringer af den faktiske eller retlige stilling, men det nævner ikke eksplicit produkter, processer og tjenesteydelser. Databeskyttelsesrådet anbefaler de tyske tilsynsmyndigheder at medtage en sådan henvisning i overensstemmelse med bilaget.

19. Hvad angår underafsnit 4.2.7 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("håndtering af uvildighed") anbefaler Databeskyttelsesrådet at understrege kriterier, der gælder for certificeringsorganer, som tilhører eller kontrolleres af en særskilt retslig enhed, på en sådan måde, at der tages hensyn til, at enhver type af økonomiske forbindelser mellem certificeringsorganet og den retlige enhed, afhængigt af dens karakteristika, kan påvirke uvildigheden af dens certificeringsaktiviteter.

20. Hvad angår afsnit 4.6 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("offentligt tilgængelige oplysninger"), bemærker Databeskyttelsesrådet, at der ikke er nogen henvisning til alle versioner af de godkendte kriterier og certificeringsprocedurerne. Derfor opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at ændre udkastet med henblik på eksplicit at nævne, at publikationen omfatter alle versioner af de godkendte kriterier og certificeringsprocedurer. Databeskyttelsesrådet bemærker endvidere, at stk. 2 i afsnit 4.6 angiver, at "certificeringsordningerne, der anvendes af certificeringsorganet de godkendte kriterier i henhold til artikel 42, stk. 5, i databeskyttelsesforordningen, som angiver den autoriserede varighed af anvendelsen, *generelt skal publiceres*". For at undgå enhver tvetydighed opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at slette ordet "generelt" og tilføje et "og" mellem "certificeringsorganet" og "de godkendte kriterier".

2.2.5 RESSOURCEKRAV (kapitel 6 i udkastet til akkrediteringskrav)

21. Hvad angår ekspertisekravene og især afsnit 6.1.2.1 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("krav til menneskelige ressourcer"), bemærker Databeskyttelsesrådet, at den krævede viden inden for de anførte områder ikke specificerer, at den viden skal være relevant og hensigtsmæssig. For at sikre overensstemmelse med ekspertiseniveauet krævet i bilaget anbefaler Databeskyttelsesrådet de tyske tilsynsmyndigheder at bringe ordlyden i overensstemmelse med vejledningen, idet de kræver, at viden er relevant og hensigtsmæssig.

22. Databeskyttelsesrådet bemærker desuden, at kravene til personale med teknisk ekspertise ansvarlig for beslutningstagning omfatter mindst syv års erhvervserfaring eller fem års erhvervserfaring med teknisk databeskyttelse, afhængigt af deres uddannelsesniveau, og personale med ansvar for evalueringer skal have fire års erhvervserfaring eller to års erhvervserfaring med teknisk databeskyttelse og erfaring med testproceduren, afhængigt af deres uddannelsesniveau. Ligeledes skal personale med juridisk ekspertise, som tager beslutninger, have mindst fem års erhvervserfaring med databeskyttelseslovgivning, og personale med ansvar for evalueringer skal have mindst to års erhvervserfaring med databeskyttelseslovgivning og revisionsprocedurer. Databeskyttelsesrådet bemærker, at der er betydelig forskel mellem kravene til, hvor mange års faglig erfaring, der kræves for personale med ansvar for beslutningstagning og for personale med ansvar for evaluering. I den forbindelse finder Databeskyttelsesrådet, at kompetencekravene til evalueringspersonale og beslutningstagere skal skræddersys under hensyntagen til de forskellige opgaver, de udfører, i stedet for antal års erfaring. Databeskyttelsesrådet er af den holdning, at evalueringspersonalet skal have en mere specialiseret ekspertise og erhvervserfaring inden for tekniske procedurer (f.eks. revisioner og certificeringer), hvorimod beslutningstagerne skal have en mere almen og omfattende ekspertise samt faglig erfaring inden for databeskyttelse. I betragtning heraf opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at lægge større vægt på den faktiske viden og/eller erfaring, som er relevant for evalueringspersonale og beslutningstagere samt at mindske forskellene i de antal års erfaring, der kræves for dem.

23. Databeskyttelsesrådet finder endvidere, at viden om forvaltningssystemerne, der er relevante for certificeringsområdet skal udvides til at omfatte ISO/IEC 27701:2019 - Sikkerhedsteknikker – ISO/IEC 27001 og ISO/IEC 27002 udvidet til at omfatte privatlivsbeskyttelse – Krav og vejledning og opfordrer de tyske tilsynsmyndigheder til at medtage en sådan henvisning.

24. For så vidt angår uddannelseskravene til det tekniske personale finder Databeskyttelsesrådet endelig, at listen over personer allerede er skræddersyet til den tekniske ekspertise krævet i bilaget. Derfor opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at slette henvisningen til "naturvidenskaber" fra listen over personer i forbindelse med universitetsuddannelsen for teknisk personale.

2.2.6 PROCESKRAV (kapitel 7 i udkastet til akkrediteringskrav)

25. Databeskyttelsesrådet bemærker, at kapitel 7 i de tyske tilsynsmyndigheder udkast til akkrediteringskrav indeholder adskillige henvisninger til begrebet "dets kriterier" (f.eks. i afsnit 7.4, 7.6, 7.11 og 7.13). Med henblik på at undgå enhver tvetydighed opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at tydeliggøre betydningen af dette begreb, eksempelvis ved at tilføje en forklaring i tillæg 1 (Ordliste).

26. Hvad angår afsnit 7.1 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("generelle oplysninger"), bemærker Databeskyttelsesrådet, at der ikke er nogen eksplicit henvisning til certificeringsorganets forpligtelse til at overholde de yderligere krav. Selv om en sådan forpligtelse kan udledes af teksten til udkastet til kravene, finder Databeskyttelsesrådet, at en eksplicit henvisning til ovennævnte forpligtelse skal medtages. Databeskyttelsesrådet anbefaler derfor, at de tyske tilsynsmyndigheder ændrer udkastet i overensstemmelse hermed.

27. Databeskyttelsesrådet bemærker, at de tyske tilsynsmyndigheders udkast til yderligere krav ikke indeholder nogen henvisning til anvendelsen af et godkendt europæisk databeskyttelsessegl i henhold til afsnit 7.1, punkt 2, i bilaget. Databeskyttelsesrådet er af den holdning, at denne henvisning skal medtages, især under hensyntagen til at akkrediteringen af et certificeringsorgan, der tildeler europæiske databeskyttelsessegl, måske skal udføres i alle medlemsstater, hvor certificeringsorganet er etableret. [3] Databeskyttelsesrådet anbefaler derfor, at de tyske tilsynsmyndigheder ændrer udkastet i overensstemmelse hermed. Udkastet til krav kunne eksempelvis angive følgende: *"Den kompetente tilsynsmyndighed skal informeres, inden et certificeringsorgan begynder at anvende et godkendt europæisk databeskyttelsessegl i en ny medlemsstat fra et satellitkontor".*

28. Databeskyttelsesrådet bemærker, at i afsnit 7.2 ("ansøgning") forudser de tyske tilsynsmyndigheders udkast til akkrediteringskrav situationen, i hvilken databehandlere anvendes til at udføre databehandlingsaktiviteter, i overensstemmelse med bilaget til vejledningen. Databeskyttelsesrådet bemærker dog, at når der anvendes databehandlere, skal ansøgningen indeholde de(n) relevante kontrakt(er) for dataansvarlige/databehandlere, som angivet i bilaget. Derfor anbefaler Databeskyttelsesrådet de tyske tilsynsmyndigheder at bringe ordlyden i overensstemmelse med vejledningen ved at medtage en henvisning til kontrakt(er) for dataansvarlige/databehandlere. Databeskyttelsesrådet opfordrer desuden de tyske tilsynsmyndigheder til at overveje, hvorvidt en henvisning til fælles dataansvarlige og deres særlige ordninger også bør nævnes i denne forbindelse.

29. Databeskyttelsesrådet bemærker, at afsnit 7.2 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav angiver, at "den dataansvarlige og databehandleren har ret til at ansøge om certificering". Databehandleres mulighed for at ansøge om certificering afhænger af den specifikke certificeringsordning. For at undgå forvirring opfordrer Databeskyttelsesrådet derfor de tyske tilsynsmyndigheder til at slette den ovennævnte henvisning eller at tydeliggøre, at databehandleres mulighed for at blive certificeret afhænger af certificeringsordningens omfang.

30. Hvad angår afsnit 7.3 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("evaluering af ansøgninger"), bemærker Databeskyttelsesmyndighederne, at de tyske tilsynsmyndigheders udkast til akkrediteringskrav angiver, at "de planlagte evalueringsmetoder er kontraktmæssigt fastlagt [...]". For at tydeliggøre at dette er et krav, opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at omformulere det første stykke for at tydeliggøre, at evalueringsmetoderne skal fremgå af certificeringsaftalen, dvs. omformulere kravet til følgende "de planlagte evalueringsmetoder skal være kontraktmæssigt fastlagt [...]". Databeskyttelsesrådet opfordrer endvidere de tyske tilsynsmyndigheder til at erstatte henvisningen til punkt 7.3.1.b i ISO 17065 med afsnit 7.3 i ISO 17065 for at bringe ordlyden i overensstemmelse med bilaget. Databeskyttelsesrådet bemærker desuden, at stk. 4 henviser til passende tekniske og juridiske kompetencer. Af hensyn til klarheden opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at tilføje "inden for databeskyttelse".

[3] Se i den forbindelse Vejledning 1/2018, punkt 44.

31. Databeskyttelsesrådet bemærker, at afsnit 7.4 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("evalueringsmetoder") ikke indeholder certificeringsorganets forpligtelse til at beskrive tilstrækkelige evalueringsmetoder til vurdering af, om behandlingsaktiviteten/-erne overholder certificeringskriterierne. Databeskyttelsesrådet anbefaler de tyske tilsynsmyndigheder at ændre udkastet til krav med henblik på at medtage en sådan henvisning. Et eksempel kunne være at tilføje følgende: *"Certificeringsorganet skal sikre, at certificeringsmekanismerne, der anvendes til at udstede en certificering, beskriver evalueringsmetoder, der er tilstrækkelige til at vurdere, om behandlingsaktiviteterne opfylder certificeringskriterierne*". Hvad angår det første område, som skal medtages i evalueringsmetoderne, finder Databeskyttelsesrådet desuden, at nødvendigheden og proportionaliteten også skal vurderes i forhold til de pågældende registrerede, hvor dette er relevant. Endelig bemærker Databeskyttelsesrådet, at der ikke er nogen dokumentation for metoder og resultater. Derfor opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at ændre udkastet og eksplicit medtage en sådan henvisning.

32. Hvad angår eksisterende certificeringer (afsnit 7.4 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav) finder Databeskyttelsesrådet, at 4. led på side 13 fører til forvirring, eftersom det er uklart, hvad forbindelsen mellem gyldighedsperioderne af den nuværende og forrige certificering er, og hvordan de passer sammen. Endvidere synes det ikke at være muligt, at stille spørgsmålstegn ved gyldigheden af certificeringer, der før er blevet udstedt af et andet akkrediteret certificeringsorgan. Alt i alt kan der i det stykke med fordel skabes mere klarhed, hvad angår forholdet mellem de forskellige nævnte elementer. Databeskyttelsesrådet anbefaler de tyske tilsynsmyndigheder at ændre udkastet, især ved at tydeliggøre, at gyldighedsperioden for certificering under databeskyttelsesforordningen ikke skal være betinget af gyldigheden af andre typer certificeringer.

33. Hvad angår afsnit 7.5 ("vurdering") i de tyske tilsynsmyndigheders udkast til akkrediteringskrav, opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at ændre afsnittets overskrift til "gennemgang".

34. For så vidt angår ændringerne, der påvirker certificeringen (afsnit 7.10 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav), bemærker Databeskyttelsesrådet, at de tyske tilsynsmyndigheders udkast til akkrediteringskrav fastlægger, at "kunden informeres rettidigt om ændringer af den retlige rammer, som påvirker vedkommende". I betragtning at behovet for at bevare certificeringsorganets upartiskhed opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at omformulere sætningen for at gøre det klart, at kunden rettidigt får generelle oplysninger om ændringer, der kan påvirke vedkommende. For at sikre en klar forståelse af, hvad der menes med "Databeskyttelsesrådets afgørelser", opfordrer Databeskyttelsesrådet endvidere de tyske tilsynsmyndigheder til at præcisere henvisningen. Den kan for eksempel henvise til "dokumenter vedtaget af Databeskyttelsesrådet".

35. Databeskyttelsesrådet bemærker, at afsnit 7.11 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("ophævelse, restriktion, suspension eller tilbagetrækning af certificering") ikke indeholder certificeringsorganets forpligtelse til at acceptere beslutninger og ordrer fra de tyske tilsynsmyndigheder om at tilbagetrække eller undlade at udstede certificeringer til en ansøger, hvis kravene til certificering ikke eller ikke længere er opfyldt. Databeskyttelsesrådet anbefaler derfor, at de tyske tilsynsmyndigheder medtager en sådan forpligtelse. Databeskyttelsesrådet opfordrer desuden de tyske tilsynsmyndigheder til at erstatte ordet "restriktion" med "begrænsning" i afsnittets overskrift i overensstemmelse med bilaget til vejledningen.

2.2.7 YDERLIGERE SUPPLERENDE KRAV

36. Hvad angår underafsnit 8.11.3 i de tyske tilsynsmyndigheders udkast til akkrediteringskrav ("klagebehandling"), opfordrer Databeskyttelsesrådet de tyske tilsynsmyndigheder til at erstatte henvisningen til "berettigede klager" med "begrundede klager" for at skabe større klarhed.

3 KONKLUSIONER/HENSTILLINGER

37. Udkastet til akkrediteringskrav fra de tyske tilsynsmyndigheder i føderationen og delstaterne kan føre til en usammenhængende anvendelse af akkrediteringen af certificeringsorganer, og følgende ændringer skal foretages:

38. For så vidt angår "generelle bemærkninger" anbefaler Databeskyttelsesrådet, at de tyske tilsynsmyndigheder:

    1) sletter henvisningen til "Databeskyttelsesrådets autorisation" med henblik på at bringe udkastet i overensstemmelse med ordlyden i databeskyttelsesforordningen.

39. For så vidt angår "generelle krav til akkreditering" anbefaler Databeskyttelsesrådet, at de tyske tilsynsmyndigheder:

    1) ændrer kravene vedrørende det retlige ansvar (underafsnit 4.1) med henblik på at bringe dem i overensstemmelse med vejledningen

    2) ændrer underafsnit 4.1.2.2 for i certificeringsaftalen at medtage forpligtelsen til at give de tyske tilsynsmyndigheder fuld indsigt i certificeringsproceduren og give certificeringsorganet adgang til ansøgerens behandlingsaktiviteter

    3) i underafsnit 4.1.2.2 medtager en eksplicit henvisning til den kompetente tilsynsmyndigheds opgaver og beføjelser i overensstemmelse med bilaget

    4) blandt elementerne i certificeringsaftalen medtager forpligtelsen til at tillade certificeringsorganet at fremlægge alle de oplysninger, der er nødvendige for at udstede en certificering i henhold artikel 42, stk. 8, og artikel 43, stk. 5, i databeskyttelsesforordningen

    5) medtager en eksplicit henvisning til "produkter, processer og tjenesteydelser, der er berørt af certificeringen" i 6. led i underafsnit 4.1.2.2

    6) i underafsnit 4.2.7 understreger kriterier, der gælder for certificeringsorganer, som tilhører eller kontrolleres af en særskilt retslig enhed, på en sådan måde, at der tages hensyn til, at enhver type af økonomiske forbindelser mellem certificeringsorganet og den retlige enhed, afhængigt af dens karakteristika, kan påvirke uvildigheden af dens certificeringsaktiviteter.

40. For så vidt angår "ressourcekrav" anbefaler Databeskyttelsesrådet, at de tyske tilsynsmyndigheder:

    1) bringer ordlyden af underafsnit 6.1.2.1 i overensstemmelse med vejledningen ved at kræve, at viden er relevant og hensigtsmæssig.

41. For så vidt angår "procedurekrav" anbefaler Databeskyttelsesrådet, at de tyske tilsynsmyndigheder:

1) ændrer afsnit 7.1, så det indeholder en eksplicit henvisning til certificeringsorganets forpligtelse til at overholde de yderligere krav

2) medtager en henvisning til anvendelsen af et godkendt europæisk databeskyttelsessegl

3) bringer ordlyden i afsnit 7.2 i overensstemmelse med vejledningen, herunder henvisningen til kontrakt(er) for dataansvarlige/databehandlere

4) i afsnit 7.4 medtager certificeringsorganets forpligtelse til at beskrive tilstrækkelige evalueringsmetoder til vurdering af, om behandlingsaktiviteten/-erne overholder certificeringskriterierne.

5) i afsnit 7.4 tydeliggør, at gyldighedsperioden for certificering under databeskyttelsesforordningen ikke skal være betinget af gyldigheden af andre typer certificeringer

6) i afsnit 7.11 medtager certificeringsorganets forpligtelse til at acceptere afgørelser og ordrer fra de tyske tilsynsmyndigheder om at tilbagetrække eller undlade at udstede certificeringer til en ansøger, hvis kravene til certificering ikke eller ikke længere er opfyldt.

4 AFSLUTTENDE BEMÆRKNINGER

42. Denne udtalelse er rettet til de tyske tilsynsmyndigheder i føderationen og delstaterne og offentliggøres i henhold til artikel 64, stk. 5, litra b), i databeskyttelsesforordningen.

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

44. De tyske tilsynsmyndigheder skal meddele deres 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.

På Det Europæiske Databeskyttelsesråds vegne

Formanden

(Andrea Jelinek)