Udtalelse 16/2020 om udkast til afgørelse fra Tjekkiets kompetente tilsynsmyndighed vedrørende godkendelse af krav til akkreditering af et certificeringsorgan i henhold til artikel 43, stk. 3 (databeskyttelsesforordningen)

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 ("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) Selv om kravene til akkreditering er underlagt sammenhængsmekanismen, er det ikke ensbetydende med, 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 eller ekspertise.

(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 om certificering og angivelse af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordning 2016/679" vil fungere som rettesnor i forbindelse med sammenhængsmekanismen.

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

(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 tjekkiske tilsynsmyndighed har indsendt sit udkast til akkrediteringskrav til Databeskyttelsesrådet i medfør af artikel 43, stk. 1, litra b). Sagsakterne blev anset for fuldstændige den 17. februar 2020. Det tjekkiske 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. 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 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

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

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 tjekkiske tilsynsmyndighed har besluttet at anvende sit nationale akkrediteringsorgan til udstedelse af akkreditering, og de har samlet supplerende krav i overensstemmelse med retningslinjerne, som det nationale akkrediteringsorgan skal benytte ved udstedelse af akkreditering.

4. Denne vurdering af den tjekkiske 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.

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

6. 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.

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 den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav, skal det læses, som at Databeskyttelsesrådet ikke har nogen bemærkninger, og at den tjekkiske tilsynsmyndighed ikke anmodes om at træffe yderligere foranstaltninger.

9. Denne udtalelse omfatter ikke forhold fremlagt af den tjekkiske 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.

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 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 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 opfattelse, at sådanne samarbejdsvilkår i givet fald skal offentliggøres i et format, som tilsynsmyndigheden finder passende.

2.2.2 GENERELLE BEMÆRKNINGER

12. Databeskyttelsesrådet bemærker, at udkastet til akkrediteringskrav ikke fuldstændigt følger strukturen i bilag 1 til vejledningen. For eksempel mangler afsnittene om "Anvendelsesområde" samt

"Begreber og definitioner". Af hensyn til klarheden og for at muliggøre en lettere vurdering af kravene finder Databeskyttelsesrådet i denne henseende, at nummereringen og dokumentets overordnede struktur kunne forbedres. Med henblik på at lette vurderingen opfordrer Databeskyttelsesrådet derfor den tjekkiske tilsynsmyndighed til at følge strukturen i bilaget i udkastet til akkrediteringskrav og tilføje de manglende afsnit, idet definitionen af de begreber, der anvendes i hele dokumentet, er af særlig relevans. Endvidere bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav flere gange henviser til det respektive afsnit i ISO 17065 eller til de respektive afsnit i bilaget uden imidlertid at præcisere den pågældende henvisning. Databeskyttelsesrådet opfordrer således den tjekkiske tilsynsmyndighed til at præcisere henvisningerne til afsnittene i ISO 17065 og i bilaget.

13. Databeskyttelsesrådet bemærker, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav flere gange henviser til det "evaluerede objekt" (f.eks. afsnit 3.2.1.2.1.2.10, 3.2.1.2.6.3.1, 3.2.1.2.8.1.6.3, 3.2.1.2.10.4.1, 3.1.2.10.7.3.1, 3.1.2.10.7.3.2 og 3.2.1.2.10.10.2). Databeskyttelsesrådet forstår, at dette begreb anvendes som et synonym for "evalueringsmålet". For at sikre klarhed opfordrer Databeskyttelsesrådet dog den tjekkiske tilsynsmyndighed til at anvende begrebet "evalueringsmål" konsekvent.

14. Databeskyttelsesrådet bemærker, at flere krav ikke er formuleret som certificeringsorganets forpligtelse (f.eks. 3.2.1.2.2 og 3.2.1.2.3). Databeskyttelsesrådet opfordrer den tjekkiske tilsynsmyndighed til at omformulere kravene for at gøre det klart, at de er obligatoriske — dvs. indlede kravet med "certificeringsorganet skal [...]".

2.2.3 GENERELLE KRAV TIL AKKREDITERING

15. Hvad angår certificeringsaftalen (afsnit 3.2.1.2.1.2 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav), bemærker Databeskyttelsesrådet, at underafsnit 3.2.1.2.1.2.2 ikke henviser til de "kontraktligt fortrolige spørgsmål", som tilsynsmyndigheden også skal have adgang til. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed ændrer udkastet ved at medtage forpligtelsen til ligeledes at give tilsynsmyndigheden adgang til kontraktligt fortrolige spørgsmål.

16. Med hensyn til underafsnit 3.2.1.2.1.2.8 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav bemærker Databeskyttelsesrådet, at det er uklart, hvem oplysningerne skal fremlægges for. Databeskyttelsesrådet opfordrer derfor den tjekkiske tilsynsmyndighed til at præcisere, hvem der vil være modtageren af oplysningerne. Endvidere skal de omhandlede oplysninger være "nødvendige for at udstede en certificering", som fastsat i afsnit 4.1.2, punkt 7, i bilaget. Databeskyttelsesrådet anbefaler, at den tjekkiske tilsynsmyndighed erstatter "oplysninger om udstedelse af en certificering" med "oplysninger, der er nødvendige for at udstede en certificering".

17. Vedrørende underafsnit 3.2.1.2.1.2.9 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav er det uklart, hvilken type oplysninger der skal fremlægges direkte for Databeskyttelsesrådet. I henhold til artikel 42, stk. 8, i databeskyttelsesforordningen er Databeskyttelsesrådet forpligtet til at samle, *bl.a.*, alle certificeringsmekanismer. I denne forbindelse antages det, at de kompetente tilsynsmyndigheder vil give de relevante oplysninger til Databeskyttelsesrådet, som derefter vil offentliggøre dem i det offentlige register. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed præciserer underafsnit 3.2.1.2.1.2.9 i udkastet til krav i overensstemmelse med artikel 42, stk. 8, i databeskyttelsesforordningen.

18. Hvad angår underafsnit 3.2.1.2.1.2.12 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav, noterer Databeskyttelsesrådet sig, at den tjekkiske tilsynsmyndighed udarbejdede en omformuleret version af en del af det krav, der er indeholdt i bilaget. Den tjekkiske tilsynsmyndighed udelod dog [hvor det er relevant] en henvisning til "konsekvenserne for kunden skal også vurderes". Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed tilføjer den manglende del af det ovenfor nævnte krav.

19. Endvidere fastsætter underafsnit 3.2.1.2.1.2.13 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav forpligtelsen til at "indeholde en forpligtelse for ansøgeren om at underrette certificeringsorganet om alle ændringer, der kan påvirke det certificerede objekts opfyldelse af certificeringskriterierne". Databeskyttelsesrådet finder denne formulering for generisk og anbefaler, at den tjekkiske tilsynsmyndighed ændrer udkastet til krav med henblik på at medtage "alle ændringer i vedkommendes faktiske eller retlige stilling samt processer og tjenesteydelser, der er berørt af certificeringen".

20. Hvad angår anvendelse af databeskyttelsesmærkninger og -mærker (afsnit 3.2.1.2.1.3 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav), bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til krav fastsætter, at certificeringsaftalen skal indeholde "regler for anvendelse af certifikater, mærkninger og mærker, hvis de er fastsat af ejeren af certificeringsordningen". Samme formulering findes i underafsnit 3.2.1.2.1.2.14. Databeskyttelsesrådet mener, at denne forpligtelse allerede er omfattet af punkt 4.1.2.2., litra I), i ISO 17065, og at den derfor bør være indeholdt i enhver certificeringsordning (se også punkt 4.1.3 i ISO 17065). Af hensyn til klarheden anbefaler Databeskyttelsesrådet således, at den tjekkiske tilsynsmyndighed sletter de nævnte afsnit.

21. Med hensyn til kravene vedrørende forvaltningen af uvildighed er afsnit 4.2.1.b) og 4.2.2 i bilaget, ifølge den tjekkiske tilsynsmyndigheds oplysninger i skabelonen, tilstrækkeligt omfattet af punkt 4.2 i ISO 17065. Databeskyttelsesrådet mener imidlertid, at disse krav udtrykkeligt skal indgå i de udkast til akkrediteringskrav, der udarbejdes af tilsynsmyndighederne i overensstemmelse med bilaget. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed medtager de manglende krav vedrørende den forvaltning af uvildighed, der er fastsat i bilaget.

22. Med hensyn til kravet om erstatningsansvar og finansiering (afsnit 3.2.1.2.3.1 i den tjekkiske tilsynsmyndigheds udkast til krav) opfordrer Databeskyttelsesrådet den tjekkiske tilsynsmyndighed til at præcisere, at det skal sikres regelmæssigt.

2.2.4 RESSOURCEKRAV

23. Hvad angår certificeringsorganets personale (afsnit 3.2.1.2.8.1.6 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav), bemærker Databeskyttelsesrådet, at kravene til personale med ansvar for evalueringer (underafsnit 3.2.1.2.8.1.6.3) omfatter "*5 års erfaring med mindst 10 foretagne revisioner udført inden for certificeringsaktivitet på det samme eller et lignende område [...] eller 5 års erfaring inden for certificering af genstandene for certificeringsorganets fokus*". På samme måde omfatter kravene til personale med ansvar for beslutningstagning (underafsnit 3.2.1.2.8.1.6.4) "*mindst 5 års erfaring med mindst 10 foretagne revisioner udført inden for certificeringsaktivitet på det samme eller et lignende område*". Databeskyttelsesrådet mener, at kravene til ekspertise for evalueringspersonale og beslutningstagere bør skræddersys under hensyntagen til de forskellige opgaver, som de udfører. I denne henseende er Databeskyttelsesrådet af den opfattelse, 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 den tjekkiske tilsynsmyndighed til at omformulere dette underafsnit under hensyntagen til de forskellige krav til den faktiske viden og/eller erfaring, som er relevant for evalueringspersonale og beslutningstagere.

24. Desuden bemærker Databeskyttelsesrådet, at det fremgår af punkt 3.2.1.2.9.1 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav, at outsourcing ikke er tilladt i forbindelse med certificeringsaktiviteter. Det følgende giver dog mulighed for brug af eksterne revisorer og eksterne eksperter til evaluering, medmindre det udgør certificeringsaktiviteter. Databeskyttelsesrådet mener, at udkastet til akkrediteringskrav bør specificere, hvornår "det udgør certificeringsaktiviteter", eller præcisere, at certificeringsorganet bibeholder ansvaret for beslutningstagningen, selv når det bruger eksterne eksperter. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed ændrer udkastet i overensstemmelse hermed.

2.2.5 PROCESKRAV

25. Databeskyttelsesrådet bemærker, at afsnit 3.2.1.2.10.1.1 i den tjekkiske tilsynsmyndigheds udkast til supplerende krav henviser til "alle de supplerende krav vedrørende en interessekonflikt (7.1, punkt 1)". Den tjekkiske tilsynsmyndigheds udkast til supplerende krav indeholder imidlertid ikke supplerende krav vedrørende interessekonflikt. Databeskyttelsesrådet opfordrer derfor den tjekkiske tilsynsmyndighed til at ændre udkastet for at undgå forvirring.

26. Med hensyn til anvendelseskravene bemærker Databeskyttelsesrådet, at underafsnit 3.2.1.2.10.2.3 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav synes at indebære, at der i ansøgningen kun skal gives oplysninger om de overførte data, når overførslen er til et tredjeland eller en international organisation. Databeskyttelsesrådet understreger imidlertid, at ansøgeren altid skal indeholde en beskrivelse af de oplysninger, der er overført til andre systemer eller organisationer, uanset deres beliggenhed. Databeskyttelsesrådet opfordrer derfor den tjekkiske tilsynsmyndighed til at ændre ordlyden for at undgå forvirring.

27. Databeskyttelsesrådet bemærker, at forpligtelsen til i certificeringsaftalen at fastsætte de bindende evalueringsmetoder (afsnit 3.2.1.2.1.2.6 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav) ikke indeholder en henvisning til evalueringsmålet, som fastsat i afsnit 7.3, punkt 1, i bilaget til vejledningen. Af hensyn til klarheden opfordrer Databeskyttelsesrådet den tjekkiske tilsynsmyndighed til at medtage en sådan henvisning.

28. Endvidere bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav tager hensyn til den situation, hvori databehandlere plejer at udføre databehandlingsaktiviteter, i overensstemmelse med bilaget til vejledningen (afsnit 3.2.1.2.10.2 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav). Databeskyttelsesrådet opfordrer den tjekkiske tilsynsmyndighed til at overveje, hvorvidt en henvisning til fælles dataansvarlige og deres særlige ordninger også bør nævnes i denne forbindelse.

29. Vedrørende evalueringskravene (afsnit 3.2.1.2.10.4 i den tjekkiske tilsynsmyndigheds udkast til krav) bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds akkrediteringskrav ikke indeholder certificeringsorganets forpligtelse til i sin certificeringsmekanisme i detaljer at redegøre for, hvordan de oplysninger, som punkt 7.4.6 i ISO 17065 indeholder krav om, oplyser ansøgeren om

afvigelser fra en certificeringsmekanisme. Som det fremgår af bilaget (underafsnit 7.4), bør sådanne oplysningers karakter og timing som minimum fastlægges. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed tilføjer den nævnte forpligtelse.

30. Endvidere synes underafsnit 3.2.1.2.10.4.2 i den tjekkiske tilsynsmyndigheds udkast til krav at begrænse evalueringsmetoderne til test, revision eller kontrol. Databeskyttelsesrådet mener, at der også kunne anvendes andre evalueringsmetoder, og opfordrer derfor den tjekkiske tilsynsmyndighed til at ændre udkastet for at gøre det klart, at opregningen ikke er udtømmende.

31. Hvad angår underafsnit 3.2.1.2.10.4.4.1.4 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav, mener Databeskyttelsesrådet, at det klart bør fremgå af kravene, at certificeringsorganet er forpligtet til at kontrollere, at kriterierne overholdes, og opfordrer tilsynsmyndigheden til at ændre udkastet i overensstemmelse hermed.

32. Med hensyn til evalueringskravene (underafsnit 3.2.1.2.10.5 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav) bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav ikke henviser til forpligtelsen til at fastsætte procedurer for tildeling og tilbagekaldelse af certificeringer. Databeskyttelsesrådet anbefaler, at den tjekkiske tilsynsmyndighed ændrer udkastet i overensstemmelse hermed.

33. Hvad angår kravene vedrørende certificeringsdokumentation bemærker Databeskyttelsesrådet, at det fremgår af afsnit 3.1.2.10.7.2 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav, at certificeringsorganet skal præcisere, at overvågning er en betingelse for certificeringers gyldighed, "hvis overvågning kræves i en certificeringsordning [...]". Databeskyttelsesrådet mener, at overvågningsaktiviteterne altid er obligatoriske i forbindelse med certificering i henhold til databeskyttelsesforordningen, og anbefaler derfor, at den tjekkiske tilsynsmyndighed medtager en sådan forpligtelse.

34. Med hensyn til kravene vedrørende registret over certificerede produkter (afsnit 3.2.1.2.10.8 i den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav og 7.8 i bilaget) og navnlig forpligtelsen til at informere den kompetente tilsynsmyndighed om grundlaget for tildeling eller tilbagekaldelse af den ønskede certificering, bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav henviser til afsnit 3.2.1.2.10.4.5. Dette afsnit vedrører imidlertid forpligtelsen til efter anmodning at gøre evalueringsdokumentationen tilgængelig for den tjekkiske tilsynsmyndighed, mens kravet i afsnit 7.8 i bilaget til vejledningen indeholder en forpligtelse til proaktivt at informere tilsynsmyndigheden om grundlaget for tildeling eller tilbagekaldelse af certificeringen. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed ændrer udkastet i overensstemmelse hermed.

35. Vedrørende de ændringer, der påvirker certificeringen, bemærker Databeskyttelsesrådet, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav blandt de procedurer, som der skal indgås aftale om, ikke nævner den godkendelsesproces med den kompetente tilsynsmyndighed, der er omhandlet i bilaget til vejledningen (s. 19). Databeskyttelsesrådet anerkender, at listen i afsnit 7.10 i bilaget ikke er obligatorisk. For at sikre overensstemmelse opfordrer Databeskyttelsesrådet imidlertid den tjekkiske tilsynsmyndighed til at tilføje en henvisning til godkendelsesprocessen med tilsynsmyndigheden.

36. Databeskyttelsesrådet bemærker, at den tjekkiske tilsynsmyndigheds udkast til akkrediteringskrav ikke klart indeholder certificeringsorganets forpligtelse til at acceptere afgørelser og påbud fra den kompetente tilsynsmyndighed om at tilbagetrække eller undlade at udstede certificering til en

ansøger, hvis kravene til certificering ikke længere er opfyldt. Databeskyttelsesrådet anbefaler, at den tjekkiske tilsynsmyndighed klart medtager en sådan forpligtelse i udkastet til akkrediteringskrav. Med hensyn til ophævelse, begrænsning, suspension eller tilbagetrækning af certificering bemærker Databeskyttelsesrådet, at der i afsnit 3.2.1.2.10.10.2 og 3.2.1.2.10.10.3 i udkastet til krav henvises til en "opfordring". Hvis hensigten er at henvise til "afgørelser og påbud" fra tilsynsmyndigheden, som fastsat i artikel 58, stk. 2, litra h), i databeskyttelsesforordningen, opfordrer Databeskyttelsesrådet den tjekkiske tilsynsmyndighed til at anvende den samme terminologi som databeskyttelsesforordningen og henvise til "afgørelser og påbud".

2.2.6 FORVALTNINGSSYSTEM

37. Databeskyttelsesrådet mener, at afsnit 3.2.1.2.11 i den tjekkiske tilsynsmyndigheds udkast til supplerende krav ikke indeholder certificeringsorganets forpligtelse til "permanent og løbende at offentliggøre, hvilke certificeringer der er udført på hvilket grundlag, hvor længe certificeringerne er gyldige inden for hvilke rammer og på hvilke betingelser", som anført i afsnit 8 i bilaget. Databeskyttelsesrådet anbefaler derfor, at den tjekkiske tilsynsmyndighed ændre udkastet til krav ved at medtage ovennævnte henvisning.

3 KONKLUSIONER/ANBEFALINGER

38. Den tjekkiske tilsynsmyndigheds udkast til krav til akkreditering kan føre til en usammenhængende anvendelse af akkrediteringen af certificeringsorganer, og følgende ændringer skal foretages:

39. Vedrørende "generelle krav til akkreditering" anbefaler Databeskyttelsesrådet, at den tjekkiske tilsynsmyndighed:

    1) medtager forpligtelsen til at give tilsynsmyndigheden adgang til "kontraktligt fortrolige spørgsmål" i afsnit 3.2.1.2.1.2

    2) erstatter "oplysninger om udstedelse af en certificering" med "oplysninger, der er nødvendige for at udstede en certificering" i underafsnit 3.2.1.2.1.2.8

    3) præciserer underafsnit 3.2.1.2.1.2.9 i overensstemmelse med artikel 42, stk. 8, i databeskyttelsesforordningen

    4) i underafsnit 3.2.1.2.1.2.12 [hvor det er relevant] tilføjer en henvisning til "konsekvenserne for kunden skal også vurderes"

    5) ændrer underafsnit 3.2.1.2.1.2.13 for at medtage “alle ændringer i vedkommendes faktiske eller retlige stilling samt processer og tjenesteydelser, der er berørt af certificeringen"

    6) sletter afsnit 3.2.1.2.1.3 og underafsnit 3.2.1.2.1.2.14

    7) medtager de manglende krav vedrørende den forvaltning af uvildighed, der er fastsat i bilaget.

40. Vedrørende "ressourcekrav" anbefaler Databeskyttelsesrådet, at den tjekkiske tilsynsmyndighed:

1) ændrer afsnit 3.2.1.2.9.1 for at specificere, hvornår "det udgør certificeringsaktiviteter", eller præcisere, at certificeringsorganet bibeholder ansvaret for beslutningstagningen, selv når det bruger eksterne eksperter.

41. Vedrørende "proceskrav" anbefaler Databeskyttelsesrådet, at den tjekkiske tilsynsmyndighed:

1) i afsnit 3.2.1.2.10.4 medtager certificeringsorganets forpligtelse til i sin certificeringsmekanisme i detaljer at redegøre for, hvordan de oplysninger, som punkt 7.4.6 i ISO 17065 indeholder krav om, oplyser ansøgeren om afvigelser fra en certificeringsmekanisme

2) ændrer afsnit 3.2.1.2.10.5 for at henvise til forpligtelsen til at fastsætte procedurer for tildeling og tilbagekaldelse af certificeringer

3) ændrer afsnit 3.1.2.10.7.2 for at afspejle, at overvågningsaktiviteterne altid er obligatoriske i forbindelse med certificering i henhold til databeskyttelsesforordningen

4) ændrer afsnit 3.2.1.2.10.8 for at afspejle certificeringsorganets forpligtelse til proaktivt at informere tilsynsmyndigheden om grundlaget for tildeling eller tilbagekaldelse af certificeringen

5) medtager certificeringsorganets forpligtelse til at acceptere afgørelser og påbud fra den kompetente tilsynsmyndighed om at tilbagetrække eller undlade at udstede certificering til en ansøger, hvis kravene til certificering ikke længere er opfyldt.

42. Vedrørende "forvaltningssystem" anbefaler Databeskyttelsesrådet, at den tjekkiske tilsynsmyndighed:

1) medtager certificeringsorganets forpligtelse til "permanent og løbende at offentliggøre, hvilke certificeringer der er udført på hvilket grundlag, hvor længe certificeringerne er gyldige inden for hvilke rammer og på hvilke betingelser", som anført i afsnit 8 i bilaget.

4 AFSLUTTENDE BEMÆRKNINGER

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

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

45. Den tjekkiske tilsynsmyndighed meddeler 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)

Vedtaget