Databeskyttelsesrådets udtalelser (artikel 64)

Udtalelse 14/2020 om udkast til afgørelse fra Irlands kompetente tilsynsmyndighed 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

1 Kortfattet fremstilling af de faktiske omstændigheder 4

2 Vurdering 5

2.1 Databeskyttelsesrådets generelle ræsonnement vedrørende det indsendte udkast til afgørelse 5

2.2 De vigtigste fokusområder i vurderingen (artikel 43, stk. 2, i databeskyttelsesforordningen og bilag 1 til Databeskyttelsesrådets retningslinjer) er, at akkrediteringskrav sikrer, at følgende anvendes på en ensartet måde: 6

2.2.1 PRÆFIKS (afsnit 0 i det nationale irske akkrediteringsorgans udkast til yderligere akkrediteringskrav) 7

2.2.2 BEGREBER OG DEFINITIONER 7

2.2.3 GENERELLE BEMÆRKNINGER 7

2.2.4 GENERELLE KRAV TIL AKKREDITERING (afsnit 4 i udkastet til akkrediteringskrav) 7

2.2.5 STRUKTURELLE KRAV (afsnit 5 i udkastet til akkrediteringskrav) 7

2.2.6 KRAV TIL RESSOURCER (afsnit 6 i udkastet til akkrediteringskrav) 8

2.2.7 KRAV TIL RESSOURCER (afsnit 7 i udkastet til akkrediteringskrav) 8

3 Konklusioner/anbefalinger 9

4 Afsluttende bemærkninger 9

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 (retningslinjer 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 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) "Retningslinjer 4/2018 om akkreditering af certificeringsorganer i henhold til artikel 43 i den generelle forordning om databeskyttelse (2016/679)" (i det følgende benævnt "retningslinjer") 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 GDPR. I forhold til forpligtelserne vedrørende nationale akkrediteringsorganers akkreditering af certificeringsorganer, indeholder artikel 43 i GDPR 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), i GDPR. Databeskyttelsesrådet bemærker, at artikel 43, stk. 2, litra a) til e), i GDPR 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 irske tilsynsmyndighed har indsendt sit udkast til akkrediteringskrav til Databeskyttelsesrådet i medfør af artikel 43, stk. 1, litra b). Sagsakterne blev anset for fuldstændige den 13. februar 2020. Det irske nationale akkrediteringsorgan, INAB, udfører akkreditering af certificeringsorganer på baggrund af certificeringskriterierne i databeskyttelsesforordningen. Det betyder, at INAB vil benytte ISO 17065 og de yderligere 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] 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

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

4. Denne vurdering af den irske tilsynsmyndigheds yderligere 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 retningslinjerne om akkreditering af certificeringsorganer er at bistå tilsynsmyndighederne i deres fastlæggelse af akkrediteringskrav. Bilaget til retningslinjerne 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 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 retningslinjerne (herefter benævnt "bilaget"). Hvor denne udtalelse ikke nævner noget om et specifikt afsnit af den irske tilsynsmyndigheds udkast til akkrediteringskrav, skal det læses, som at Databeskyttelsesrådet ikke har nogen bemærkninger, og at den irske tilsynsmyndighed ikke anmodes om at træffe yderligere foranstaltninger.

9. Denne udtalelse omfatter ikke forhold fremlagt af den irske 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 retningslinjer) er, at akkrediteringskrav sikrer, at følgende anvendes på en ensartet måde:

1) idet alle centrale områder, der er fremhævet i bilaget til retningslinjerne, 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 retningslinjerne 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 (afsnit 0 i det nationale irske akkrediteringsorgans udkast til yderligere akkrediteringskrav)

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 henvisningen til retningslinjerne om akkreditering som "WP 261" ikke er blevet opdateret. Databeskyttelsesrådet vedtog retningslinjer 4/2018 om akkreditering af certificeringsorganer i henhold til artikel 43 i den generelle forordning om databeskyttelse (2016/679). Derfor opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed til at ændre ordlyden og henvise til retningslinjer 4/2018.

2.2.3 GENERELLE BEMÆRKNINGER

13. Databeskyttelsesrådet bemærker, den irske tilsynsmyndigheds udkast til krav gentagne gange henviser til "den kompetente tilsynsmyndighed". Eftersom den kompetente tilsynsmyndighed i dette tilfælde er den irske tilsynsmyndighed, opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed til at erstatte henvisningen med "DPC" eller "den irske tilsynsmyndighed" for at undgå forvirring.

14. Databeskyttelsesrådet anerkender, at den irske tilsynsmyndigheds udkast til krav omfatter et afsnit om termer om vilkår og definitioner. Nogle af udtrykkene anvendes imidlertid ikke konsekvent i dokumentet (f.eks. "object of evaluation" og "ToE"). For at undgå forvirring opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed til at anvende konsekvent terminologi i udkastet til krav.

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

15. Med hensyn til paragraf 7 i underafsnit 4.1.2 i den irske tilsynsmyndigheds udkast til akkrediteringskrav mener Databeskyttelsesrådet, at ordlyden er lidt uklar med hensyn til, hvem der skal gives begrundelse for at godkende certificeringen. Desuden er henvisningen til "at lette" registreringen også uklar. Databeskyttelsesrådet opfordrer derfor den irske tilsynsmyndighed til at omformulere dette på en måde, så det bliver mere klart.

2.2.5 STRUKTURELLE KRAV (afsnit 5 i udkastet til akkrediteringskrav)

16. Databeskyttelsesrådet bemærker, at den irske tilsynsmyndigheds udkast til akkrediteringskrav henviser til udnævnelsen af "en person med den relevante anciennitet med ansvar for overvågning af overholdelse af databeskyttelse og forvaltning af oplysninger". Henvisningen til den relevante anciennitet bør præciseres med hensyn til erfaring og omfanget af beføjelser. Desuden synes denne person at udføre samme funktioner som en databeskyttelsesrådgiver. Databeskyttelsesrådet opfordrer den irske tilsynsmyndighed til at anføre denne persons funktioner og specificere relevante erfaringer.

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

17. Med hensyn til certificeringspersonale (underafsnit 6.1) bemærker Databeskyttelsesrådet, at kravene til personale med teknisk ekspertise og ansvar for at træffe beslutninger omfatter mindst 5 års erhvervserfaring i forbindelse med certificeringsemnet, mens personalet med ansvar for evalueringer bør have mindst 2 års erhvervserfaring. Tilsvarende skal personale med juridisk ekspertise, der træffer afgørelser, have mindst 5 års erhvervserfaring, mens personale med ansvar for evalueringer, skal have mindst 2 års erfaring. 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 ansvarlig for evaluering. Databeskyttelsesrådet mener i den henseende, at der bør lægges vægt på de forskellige typer ekspertise frem for antal års erhvervserfaring. Efter Databeskyttelsesrådets opfattelse bør evalueringspersonalet have en mere specialiseret ekspertise og erhvervserfaring inden for tekniske procedurer (f.eks. auditter og certificeringer), hvorimod beslutningstagerne bør have en mere almen og omfattende ekspertise samt faglig erfaring inden for databeskyttelse. I betragtning heraf opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed 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.

2.2.7 KRAV TIL RESSOURCER (afsnit 7 i udkastet til akkrediteringskrav)

18. Med hensyn til underafsnit 7.10 i den irske tilsynsmyndigheds udkast til akkrediteringskrav ("Ændringer, der påvirker certificeringen") bemærker Databeskyttelsesrådet, at der ikke er nogen henvisning til de ændringsprocedurer, der skal aftales i henhold til afsnit 7.10 i bilaget. Databeskyttelsesrådet opfordrer den irske tilsynsmyndighed til at medtage en sådan henvisning og nævne nogle af de procedurer, der kunne iværksættes (f.eks. overgangsperioder, godkendelsesproces hos den kompetente tilsynsmyndighed mv.). Databeskyttelsesrådet mener endvidere, at den tekniske udvikling også er relevant og kan påvirke certificering. Derfor opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed til at medtage denne mulighed i listen over ændringer, der påvirker certificering. Endelig glæder Databeskyttelsesrådet sig over, at der i listen over ændringer, der kan påvirke certificering, er medtaget overtrædelser af GDPR. For at sikre klarhed opfordrer Databeskyttelsesrådet dog den irske tilsynsmyndighed til at præcisere, at der kun skal tages hensyn til brud på datasikkerheden eller overtrædelser af GDPR, for så vidt de vedrører certificeringen.

19. Med hensyn til de ændringer, der påvirker certificering (underafsnit 7.10 i den irske tilsynsmyndigheds udkast til krav), og navnlig det femte punkt, bemærker Databeskyttelsesrådet, at den irske tilsynsmyndighed henviser til "gældende bindende beslutninger truffet af Det Europæiske Databeskyttelsesråd" og også til artikel 39 i Databeskyttelsesrådets forretningsorden, som omfatter "alle endelige dokumenter, der er vedtaget af Databeskyttelsesrådet". For at sikre en klar forståelse af, hvad der menes med "Databeskyttelsesrådets afgørelser", opfordrer Databeskyttelsesrådet den irske tilsynsmyndighed til at præcisere henvisningen. Den kan for eksempel henvise til "dokumenter vedtaget af Databeskyttelsesrådet".

20. Databeskyttelsesrådet bemærker, at underafsnit 7.11 i den irske tilsynsmyndigheds udkast til krav (ophør, begrænsning, suspendering eller tilbagekaldelse af certificering) ikke indeholder certificeringsorganets forpligtelse til at acceptere beslutninger og ordrer fra den irske tilsynsmyndighed om at tilbagekalde eller undlade at udstede certificeringer til en ansøger, hvis

kravene til certificering ikke eller ikke længere er opfyldt. Databeskyttelsesrådet anbefaler derfor, at den irske tilsynsmyndighed medtager en sådan forpligtelse.

3 KONKLUSIONER/ANBEFALINGER

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

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

1) I underafsnit 7.11 medtager certificeringsorganets forpligtelse til at acceptere afgørelser og ordrer fra den irske tilsynsmyndighed om at tilbagekalde eller undlade at udstede certificering til en ansøger, hvis kravene til certificering ikke eller ikke længere er opfyldt.

4 AFSLUTTENDE BEMÆRKNINGER

23. Denne udtalelse er rettet til den irske 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 skal den irske tilsynsmyndighed senest to uger efter modtagelsen af udtalelsen give 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 listen eller, hvis det helt eller delvist ikke agter at følge udtalelsen fra Databeskyttelsesrådet, give en relevant begrundelse herfor.

25. Den irske 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)