Yttrande 15/2020 om utkastet till beslut från Tysklands behöriga tillsynsmyndigheter om godkännande av kraven för ackreditering av ett certifieringsorgan enligt artikel 43.3 (den allmänna dataskyddsförordningen)

Antaget den 25 maj 2020

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

Antaget

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit detta yttrande

med beaktande av artikel 63, artikel 64.1 c och 64.3–64.8 och artikel 43.3 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, i dess ändrade lydelse enligt gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018,[1]

med beaktande av artiklarna 10 och 22 i arbetsordningen av den 25 maj 2018, och

av följande skäl:

(1) Europeiska dataskyddsstyrelsens viktigaste uppgift är att se till att förordning 2016/679 (nedan kallad *den allmänna dataskyddsförordningen*) tillämpas enhetligt i hela Europeiska ekonomiska samarbetsområdet. I enlighet med artikel 64.1 i den allmänna dataskyddsförordningen ska dataskyddsstyrelsen avge ett yttrande när en tillsynsmyndighet avser att godkänna kraven för ackreditering av certifieringsorgan enligt artikel 43. Syftet med detta yttrande är således att skapa ett harmoniserat förhållningssätt när det gäller de krav som en datatillsynsmyndighet eller det nationella ackrediteringsorganet kommer att tillämpa för ackrediteringen av ett certifieringsorgan. I den allmänna dataskyddsförordningen föreskrivs inte en enda uppsättning krav för ackreditering, men enhetlighet förordas. Dataskyddsstyrelsen försöker uppnå detta mål genom sina yttranden, främst genom att uppmana tillsynsmyndigheterna att utforma sina krav för ackreditering enligt den struktur som fastställs i bilaga 1 till dataskyddsstyrelsens riktlinjer 4/2018 om ackreditering av certifieringsorgan, och vidare genom att analysera dem med hjälp av en mall som dataskyddsstyrelsen tillhandahåller, som gör det möjligt att jämföra kraven (med vägledning av ISO 17065 och dataskyddsstyrelsens riktlinjer om ackreditering av certifieringsorgan).

(2) Med hänvisning till artikel 43 i den allmänna dataskyddsförordningen ska de behöriga tillsynsmyndigheterna anta ackrediteringskrav. De ska emellertid tillämpa mekanismen för enhetlighet för att se till att förtroendet för certifieringsmekanismen ökar, särskilt genom att fastställa höga krav.

(3) Även om kraven för ackreditering omfattas av mekanismen för enhetlighet innebär detta inte att kraven ska vara identiska. De behöriga tillsynsmyndigheterna har ett utrymme för skönsmässig bedömning när det gäller de nationella eller regionala förhållandena, och bör ta hänsyn till sin lokala lagstiftning. Syftet med dataskyddsstyrelsens yttrande är inte att uppnå en enda uppsättning av krav inom EU, utan snarare att undvika väsentliga avvikelser som exempelvis skulle kunna påverka förtroendet när det gäller de ackrediterade certifieringsorganens oberoende eller expertis.

(4) Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (2016/679) (nedan kallade *riktlinjerna*) och riktlinjer 1/2018 om certifiering

[1] Hänvisningar till ”unionen” som görs i hela detta yttrande ska förstås som hänvisningar till ”EES”.

och identifiering av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679, kommer att fungera som vägledning med avseende på mekanismen för enhetlighet.

(5) Om en medlemsstat föreskriver att certifieringsorganen ska ackrediteras av tillsynsmyndigheten bör tillsynsmyndigheten fastställa ackrediteringskrav som inbegriper, men inte är begränsade till, de krav som anges i artikel 43.2. I jämförelse med skyldigheterna avseende nationella ackrediteringsorgans ackreditering av certifieringsorgan innehåller artikel 43 färre uppgifter om kraven för ackreditering när tillsynsmyndigheten själv genomför ackrediteringen. För att bidra till ett harmoniserat förhållningssätt till ackreditering bör de ackrediteringskrav som tillämpas av tillsynsmyndigheten vägledas av ISO/IEC 17065, och de bör kompletteras med ytterligare krav som en tillsynsmyndighet fastställer i enlighet med artikel 43.1 b. Europeiska dataskyddsstyrelsen noterar att artikel 43.2 a–e speglar och anger kraven i ISO 17065, vilket kommer att bidra till samstämmighet[2].

(6) Europeiska dataskyddsstyrelsens yttrande ska antas i enlighet med artikel 64.1 c, 64.3 och 64.8 i den allmänna dataskyddsförordningen, jämförd med artikel 10.2 i dataskyddsstyrelsens arbetsordning, inom åtta veckor från den första arbetsdagen efter det att ordföranden och den behöriga tillsynsmyndigheten har beslutat att handlingarna i ärendet är fullständiga. På beslut av ordföranden får denna period förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1 SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. De tyska tillsynsmyndigheterna i förbundsstaten och delstaterna (nedan kallade *de tyska tillsynsmyndigheterna*) har lämnat in sitt utkast till ackrediteringskrav enligt artikel 43.1 b till Europeiska dataskyddsstyrelsen. Handlingarna i ärendet ansågs vara fullständiga den 13 februari 2020. Tysklands nationella ackrediteringsorgan DAkkS kommer att utföra ackrediteringen av certifieringsorgan för att intyga tillämpningen av certifieringskriterier enligt den allmänna dataskyddsförordningen. Detta innebär att det tyska nationella ackrediteringsorganet kommer att tillämpa ISO 17065 och de ytterligare krav som fastställts av de tyska tillsynsmyndigheterna, när dessa har godkänts av myndigheten, efter ett yttrande från dataskyddsstyrelsen om utkastet till krav, för att ackreditera certifieringsorgan.

2. I enlighet med artikel 10.2 i styrelsens arbetsordning beslutade ordföranden, med tanke på komplexiteten i det aktuella ärendet, att förlänga den ursprungliga antagandeperioden på åtta veckor med ytterligare sex veckor.

[2] Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43.39 i allmänna dataskyddsförordningen. Finns tillgängliga på https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_sv

2 BEDÖMNING

2.1 Dataskyddsstyrelsens allmänna resonemang när det gäller det inlämnade utkastet till beslut

3. Syftet med ett yttrande är att utvärdera de ackrediteringskrav som utarbetats av en tillsynsmyndighet, antingen på grundval av ISO 17065 eller en fullständig uppsättning krav, för att göra det möjligt för ett nationellt ackrediteringsorgan eller en tillsynsmyndighet, i enlighet med artikel 43.1 i den allmänna dataskyddsförordningen, att ackreditera ett certifieringsorgan med ansvar för att utfärda och förnya certifieringar enligt artikel 42 i den förordningen. Detta påverkar inte den behöriga tillsynsmyndighetens uppgifter och befogenheter. I det aktuella fallet noterar dataskyddsstyrelsen att de tyska tillsynsmyndigheterna har valt att använda sig av gemensam ackreditering av sitt nationella ackrediteringsorgan, DAkkS, och den behöriga tillsynsmyndigheten för att utfärda ackrediteringar, efter att ha utarbetat ytterligare krav i enlighet med riktlinjerna, som ska användas vid utfärdandet av ackreditering.

4. Denna utvärdering av de tyska tillsynsmyndigheternas ytterligare ackrediteringskrav syftar till att undersöka hur de skiljer sig (tillägg eller strykningar) från riktlinjerna och i synnerhet bilaga 1 till dessa. Europeiska dataskyddsstyrelsens yttrande är även inriktat på alla aspekter som kan komma att inverka på enhetligheten när det gäller ackrediteringen av certifieringsorgan.

5. Det ska påpekas att riktlinjerna om ackreditering av certifieringsorgan ska tjäna som stöd för tillsynsmyndigheterna när de fastställer sina ackrediteringskrav. Bilagan till riktlinjerna utgör inte i sig ackrediteringskrav. Därför krävs det att tillsynsmyndigheterna definierar ackrediteringskraven för certifieringsorgan så att en praktisk och enhetlig tillämpning blir möjlig, mot bakgrund av tillsynsmyndigheternas arbete.

6. Med hänsyn till deras sakkunskap anser dataskyddsstyrelsen att de nationella ackrediteringsorganen och de behöriga tillsynsmyndigheterna, i tillämpliga fall, bör få ett visst handlingsutrymme vid utarbetandet av vissa specifika bestämmelser inom de tillämpliga ackrediteringskraven. Vid utarbetandet av ytterligare krav vill dataskyddsstyrelsen dock betona vikten av att dessa krav fastställs på ett sätt som möjliggör en praktisk och konsekvent tillämpning och granskning efter behov.

7. Dataskyddsstyrelsen konstaterar även att ISO-standarder, och i synnerhet ISO 17065, omfattas av immateriella rättigheter. Därför kommer dataskyddsstyrelsen i sitt yttrande inte att hänvisa till texten i det relaterade dokumentet. Dataskyddsstyrelsen har med anledning av detta beslutat att i förekommande fall hänvisa till specifika avsnitt i ISO-standarden utan att ordagrant återge texten.

8. Slutligen har dataskyddsstyrelsen genomfört sin bedömning i enlighet med den struktur som fastställs i bilaga 1 till riktlinjerna (nedan kallad *bilagan*). Om det inte står något i yttrandet om ett visst avsnitt i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav, ska det tolkas som att dataskyddsstyrelsen inte har några synpunkter i det aktuella fallet och inte begär att de tyska tillsynsmyndigheterna vidtar några ytterligare åtgärder.

9. I detta yttrande beaktas inte de dokument som lämnats in av de tyska tillsynsmyndigheterna och som inte omfattas av artikel 43.2 i den allmänna dataskyddsförordningen, såsom hänvisningar till nationell lagstiftning. Styrelsen konstaterar dock att nationell lagstiftning bör överensstämma med den allmänna dataskyddsförordningen när så krävs.

2.2 De viktigaste punkterna vid bedömningen (artikel 43.2 i den allmänna dataskyddsförordningen och bilaga 1 till dataskyddsstyrelsens riktlinjer) av om ackrediteringskraven innehåller följande så att de kan utvärderas på ett konsekvent sätt:

1) Behandling av alla viktiga områden som framhävs i bilagan till riktlinjerna och beaktande av eventuella avvikelser från bilagan.

2) Certifieringsorganets oberoende.

3) Intressekonflikter för certifieringsorganet.

4) Certifieringsorganets expertis.

5) Lämpliga säkerhetsåtgärder för att säkerställa att certifieringsorganet tillämpar certifieringskraven enligt den allmänna dataskyddsförordningen på ett korrekt sätt.

6) Förfaranden för utfärdande, periodisk översyn och återkallande av en certifiering enligt den allmänna dataskyddsförordningen.

7) Öppen hantering av klagomål om överträdelser av certifieringen.

10. Med beaktande av att det

a. i artikel 43.2 i den allmänna dataskyddsförordningen finns en förteckning över krav på ackrediteringsområden som ett certifieringsorgan måste uppfylla för att ackrediteras,

b. i artikel 43.3 i den allmänna dataskyddsförordningen föreskrivs att kraven för ackreditering av certifieringsorgan ska godkännas av den behöriga tillsynsmyndigheten,

c. i artikel 57.1 p och q i den allmänna dataskyddsförordningen fastställs att en behörig tillsynsmyndighet måste utarbeta och offentliggöra kraven för ackreditering av certifieringsorgan och kan besluta att själv utföra ackrediteringen av certifieringsorgan,

d. i artikel 64.1 c i den allmänna dataskyddsförordningen föreskrivs att dataskyddsstyrelsen ska avge ett yttrande när en tillsynsmyndighet avser att godkänna kraven för ackreditering av ett certifieringsorgan enligt artikel 43.3.

e. Om ackreditering utförs av det nationella ackrediteringsorganet i enlighet med ISO/IEC 17065/2012 måste även ytterligare krav som fastställts av den behöriga tillsynsmyndigheten tillämpas.

f. Bilaga 1 till riktlinjerna om ackreditering av certifieringsorgan innehåller förslag på krav som en datatillsynsmyndighet kan upprätta och som ska tillämpas när det nationella ackrediteringsorganet ackrediterar ett certifieringsorgan.

Styrelsen anser följande:

2.2.1 PREFIX

11. Styrelsen medger att samarbetsvillkoren, som reglerar förhållandet mellan ett nationellt ackrediteringsorgan och dess datatillsynsmyndighet, i sig inte utgör ett krav för ackreditering av

certifieringsorgan. För tydlighetens och öppenhetens skull anser dock dataskyddsstyrelsen att eventuella samarbetsvillkor ska offentliggöras i ett sådant format som tillsynsmyndigheten finner lämpligt.

2.2.2 TERMER OCH DEFINITIONER

12. Styrelsen noterar att man i kapitel 3 (”Definitioner”) i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav fastställer de tillåtna typerna av certifieringssystem, vilka måste uppfylla kraven enligt DIN EN ISO/IEC 17065. Det bör påpekas att man i avsnitt 5.1 och 5.2 i dataskyddsstyrelsens riktlinjer redan tydligt och uttömmande anger vad som kan certifieras enligt den allmänna dataskyddsförordningen. Därför konstaterar styrelsen att de tyska tillsynsmyndigheterna inte avser att begränsa vad som står i riktlinjerna och att uttalandena i kapitel 3 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav ska anses vara tillämpliga inom ramen för dessa ackrediteringskrav.

2.2.3 ALLMÄNNA ANMÄRKNINGAR

13. Styrelsen noterar att avsnittet ”allmänna anmärkningar” i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav hänvisar till dataskyddsstyrelsens ”auktorisering” av certifieringskriterierna ”i enlighet med artiklarna 63 och 64.1 c i den allmänna dataskyddsförordningen”. Styrelsen noterar att den allmänna dataskyddsförordningen inte ger dataskyddsstyrelsen behörighet att ”auktorisera” certifieringskriterier. Men enligt de tidigare nämnda artiklarna kan dock dataskyddsstyrelsen godkänna certifieringskriterier. Styrelsen rekommenderar därför att de tyska tillsynsmyndigheterna tar bort hänvisningen till ”dataskyddsstyrelsens auktorisering”, så att utkastet följer ordalydelsen i den allmänna dataskyddsförordningen.

2.2.4 ALLMÄNNA KRAV FÖR ACKREDITERING (kapitel 4 i utkastet till ackrediteringskrav)

14. Vad gäller kravet på rättsligt ansvar (avsnitt 4.1 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav) noterar styrelsen att de tyska tillsynsmyndigheterna i de styrkande handlingarna förklarar att certifieringsorganet förväntas ha aktualiserade förfaranden, varför inga ytterligare krav behöver läggas till i detta hänseende. Styrelsen anser dock att en förväntan inte binder certifieringsorganen till att ha sådana förfaranden. Såsom fastställs i avsnitt 4.1.1 i tillägget till riktlinjerna ska certifieringsorganen ha aktualiserade förfaranden som tydligt uppfyller de rättsliga krav som fastställs i villkoren för ackreditering. Vidare ska certifieringsorganet kunna uppvisa belägg för förfaranden och åtgärder i enlighet med den allmänna dataskyddsförordningen som specifikt syftar till att kontrollera och hantera kundorganisationens personuppgifter som en del av certifieringsförfarandet. Styrelsen rekommenderar därför att de tyska tillsynsmyndigheterna ändrar utkastet till krav för att anpassa kraven efter riktlinjerna.

15. Vad gäller underavsnitt 4.1.2.2 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”certifieringsavtal”) noterar styrelsen att de tyska tillsynsmyndigheternas utkast till ackrediteringskrav inte innefattar skyldigheten att ge den behöriga tillsynsmyndigheten fullständig insyn i certifieringsförfarandet, inräknat konfidentiella frågor enligt avtal. Det finns heller ingen hänvisning till sökandens skyldighet att ge certifieringsorganet tillgång till sin behandling av personuppgifter. Dataskyddsstyrelsen rekommenderar därför att de tyska tillsynsmyndigheterna inkluderar ovanstående skyldigheter i sitt utkast.

16. Styrelsen lägger märke till att den uttryckliga hänvisningen till den behöriga tillsynsmyndighetens arbetsuppgifter och befogenheter (tredje strecksatsen i avsnitt 4.1.2 i bilagan) inte finns med i

underavsnitt 4.1.2.2 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav. Styrelsen anser att denna hänvisning bör läggas till i utkastet till krav och rekommenderar därför att de tyska tillsynsmyndigheterna ändrar utkastet i enlighet därmed.

17. De tyska tillsynsmyndigheternas utkast till krav avseende certifieringsavtalet innefattar heller inte skyldigheten att tillåta att certifieringsorganet offentliggör all information som behövs för att bevilja certifiering enligt artiklarna 42.8 och 43.5 i den allmänna dataskyddsförordningen (sjunde strecksatsen i avsnitt 4.1.2 i bilagan). Även om skyldigheten ingår i avsnittet om ledningen av förfarandet i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav, anser styrelsen att den bör ingå i certifieringsavtalet för att göra den mer bindande. Dataskyddsstyrelsen rekommenderar därför att de tyska tillsynsmyndigheterna inkluderar den ovannämnda skyldigheten som del av certifieringsavtalet.

18. Enligt bilagan måste sökanden informera certifieringsorganet om avsevärda förändringar av sin faktiska eller rättsliga ställning och av sina produkter, förfaranden och tjänster som berörs av certifieringen (tionde strecksatsen i avsnitt 4.1.2 i bilagan). I de tyska tillsynsmyndigheternas utkast till ackrediteringskrav är det bara sjätte strecksatsen i underavsnitt 4.1.2.2 som innefattar skyldigheten att informera certifieringsorganet om betydande förändringar i faktiska eller rättsliga förhållanden. Produkterna, förfarandena och tjänsterna nämns dock inte uttryckligen. Styrelsen rekommenderar att de tyska tillsynsmyndigheterna inkluderar denna hänvisning i enlighet med bilagan.

19. Vad gäller underavsnitt 4.2.7 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”hantering av opartiskhet”) rekommenderar styrelsen att de tillämpliga kriterierna för certifieringsorgan som tillhör eller kontrolleras av en separat rättslig enhet bör förstärkas. Detta krävs för att kunna beakta att alla typer av ekonomiska förhållanden mellan certifieringsorganet och den rättsliga enheten, beroende på dess funktioner, kan påverka opartiskheten hos dess certifieringsverksamhet.

20. Vad gäller avsnitt 4.6 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”offentligt tillgänglig information”), noterar styrelsen att det saknas en hänvisning till offentliggörandet av samtliga versioner av de godkända kriterierna och certifieringsförfarandena. Därför uppmanar styrelsen de tyska tillsynsmyndigheterna att ändra utkastet till ackrediteringskrav för att tydliggöra att offentliggörandet innefattar samtliga versioner av de godkända kriterierna och certifieringsförfarandena. Dessutom noterar styrelsen att man i andra stycket i avsnitt 4.6 uppger att ”de certifieringssystem som används av certifieringsorganet de godkända kriterierna enligt artikel 42.5 i den allmänna dataskyddsförordningen som anger tillämpningens auktoriserade varaktighet *ska i allmänhet offentliggöras*.” För att undvika alla tvetydigheter uppmanar styrelsen de tyska tillsynsmyndigheterna att ta bort orden ”i allmänhet” och införa ett ”och” mellan ”certifieringsorgan” och ”de godkända kriterierna”.

2.2.5 RESURSKRAV (kapitel 6 i utkastet till ackrediteringskrav)

21. Vad gäller sakkunskapskraven och i synnerhet underavsnitt 6.1.2.1 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”personalkompetens”) noterar styrelsen att man för den efterfrågade kunskapen i de förtecknade områdena inte specificerar att kunskapen ska vara relevant och lämplig. För att säkerställa överensstämmelse med den expertisnivå som krävs i bilagan rekommenderar dataskyddsstyrelsen att de tyska tillsynsmyndigheterna anpassar ordalydelsen efter riktlinjerna, genom att kräva att kunskapen ska vara relevant och lämplig.

22. Vidare noterar styrelsen att man i kraven för tekniskt sakkunnig personal i beslutsfattande ställning inkluderar minst sju års yrkeserfarenhet eller fem års yrkeserfarenhet inom tekniskt dataskydd, beroende på deras utbildningsnivå, medan personal som ansvarar för utvärderingar bör ha fyra års yrkeserfarenhet eller två års yrkeserfarenhet inom tekniskt dataskydd samt erfarenhet av testförfarandet, beroende på deras utbildningsnivå. Likaså måste juridiskt sakkunniga i beslutsfattande ställning ha minst fem års yrkeserfarenhet av dataskyddslagstiftning, medan de som ansvarar för utvärderingar måste ha minst två års erfarenhet av dataskyddslagstiftning och av revisionsförfarandena. Dataskyddsstyrelsen noterar att minimikravet på antalet år av yrkeserfarenhet skiljer sig markant åt mellan personal med ansvar för beslutsfattande och personal med ansvar för utvärdering. I detta sammanhang finner dataskyddsstyrelsen att kompetenskraven för utvärderare och beslutsfattare bör anpassas så att hänsyn tas till deras olika arbetsuppgifter, snarare än antalet år i yrket. Dataskyddsstyrelsen anser att utvärderare bör ha en mer specialiserad expertis och yrkeserfarenhet av tekniska förfaranden (till exempel revision och certifiering), medan beslutsfattare bör ha en mer generell och övergripande expertis och yrkeserfarenhet av dataskydd. Med anledning av detta uppmanar dataskyddsstyrelsen de tyska tillsynsmyndigheterna att lägga mer fokus på den faktiska kunskap och/eller erfarenhet som är relevant för utvärderare och beslutsfattare och att minska skillnaderna i antalet år i yrket som krävs av dessa.

23. Dessutom anser dataskyddsstyrelsen att kunskapen om de förvaltningssystem som är relevanta för certifieringsområdet bör utökas till ISO/IEC 27701:2019 – Säkerhetstekniker – Tillägg till ISO/IEC 27001 och ISO/IEC 27002 för hantering av personuppgifter – Krav och vägledning – samt uppmanar de tyska tillsynsmyndigheterna att inkludera denna hänvisning.

24. Vad gäller utbildningskraven för teknisk personal anser styrelsen slutligen att ämnesförteckningen redan anpassats till den tekniska expertis som efterfrågas i bilagan. Därför uppmanar styrelsen de tyska tillsynsmyndigheterna att ta bort hänvisningen till ”naturvetenskap” från ämnesförteckningen för den tekniska personalens universitetsutbildning.

2.2.6 FÖRFARANDEKRAV (avsnitt 7 i utkastet till ackrediteringskrav)

25. I kapitel 7 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav noterar styrelsen de många hänvisningarna till termen ”dess kriterier” (till exempel i avsnitt 7.4, 7.6, 7.11 och 7.13). För att undvika alla tvetydigheter uppmanar styrelsen de tyska tillsynsmyndigheterna att förtydliga innebörden av denna term, genom att till exempel lägga till en förklaring i bilaga 1 (ordlista).

26. Vad gäller avsnitt 7.1 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”allmän information”) noterar styrelsen att det saknas en uttrycklig hänvisning till certifieringsorganets skyldighet att uppfylla de ytterligare kraven. Även om det går att sluta sig till en sådan skyldighet från texten till utkastet till krav anser styrelsen att en uttrycklig hänvisning till den ovannämnda skyldigheten bör inkluderas. Styrelsen rekommenderar därför att de tyska tillsynsmyndigheterna ändrar utkastet i enlighet därmed.

27. Styrelsen noterar att de tyska tillsynsmyndigheternas utkast till ytterligare krav inte innehåller någon hänvisning till hanteringen av ett godkänt europeiskt sigill för dataskydd, i enlighet med avsnitt 7.1.2 i bilagan. Styrelsen anser att denna hänvisning bör inkluderas, särskilt med tanke på att ett certifieringsorgan som beviljar europeiska sigill för dataskydd kanske måste ackrediteras i alla

medlemsstater där certifieringsorganet finns.[3] Styrelsen rekommenderar därför att de tyska tillsynsmyndigheterna inkluderar den ovannämnda hänvisningen. I utkastet till krav kan till exempel följande anges: *”Den behöriga tillsynsmyndigheten ska underrättas innan ett certifieringsorgan börjar hantera ett godkänt europeiskt sigill för dataskydd i en ny medlemsstat från en satellitbyrå".*

28. Vad gäller avsnitt 7.2 (”tillämpning”) noterar dataskyddsstyrelsen att man i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav förutser situationen där personuppgiftsbiträden används vid behandling av personuppgifter, i enlighet med bilagan till riktlinjerna. Styrelsen noterar dock att tillämpningen vid användning av personuppgiftsbiträden ska omfatta det eller de relevanta avtalet/avtalen mellan den personuppgiftsansvarige och personuppgiftsbiträdet, i enlighet med bilagan. Styrelsen rekommenderar därför att de tyska tillsynsmyndigheterna anpassar ordalydelsen efter riktlinjerna genom att inkludera hänvisningen till avtalet/avtalen mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Vidare uppmanar styrelsen de tyska tillsynsmyndigheterna att överväga huruvida det i detta fall även bör införas en hänvisning till gemensamma personuppgiftsansvariga och deras specifika överenskommelser.

29. Styrelsen noterar att man i avsnitt 7.2 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav har angett att ”den personuppgiftsansvarige och personuppgiftsbiträdet har rätt att ansöka om certifiering”. Personuppgiftsbiträdenas möjlighet att ansöka om certifiering kommer att bero på det specifika certifieringssystemet. För att undvika missförstånd uppmanar styrelsen därför de tyska tillsynsmyndigheterna att ta bort den ovanstående hänvisningen eller att förtydliga att personuppgiftsbiträdenas möjlighet till certifiering kommer att bero på certifieringssystemets tillämpningsområde.

30. Vad gäller avsnitt 7.3 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”utvärderingsansökningar”) noterar styrelsen att man i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav uppger att ”de planerade utvärderingsmetoderna är avtalsreglerade [...]”. För att förtydliga att detta är ett krav uppmanar styrelsen de tyska tillsynsmyndigheterna att omformulera den första punkten, för att förtydliga att utvärderingsmetoderna ska ingå i certifieringsavtalet – dvs. omformulera kravet till att ”de planerade utvärderingsmetoderna ska vara avtalsreglerade [...]”. Dessutom uppmanar styrelsen de tyska tillsynsmyndigheterna att ersätta hänvisningen till avsnitt 7.3.1.b i ISO 17065 med avsnitt 7.3 i ISO 17065, för att anpassa ordalydelsen efter bilagan. Vidare noterar styrelsen att punkt 4 avser lämplig teknisk och rättslig kompetens. Av tydlighetsskäl uppmanar styrelsen de tyska tillsynsmyndigheterna att lägga till ”på dataskyddsområdet”.

31. Styrelsen noterar att avsnitt 7.4 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”utvärderingsmetoder”) inte innefattar certifieringsorganets skyldighet att beskriva tillräckliga utvärderingsmetoder för att bedöma överensstämmelsen mellan behandlingen av personuppgifter och certifieringskriterierna. Styrelsen rekommenderar att de tyska tillsynsmyndigheterna ändrar utkastet till krav så att det innehåller denna hänvisning. Följande skulle till exempel kunna läggas till: *”Certifieringsorganet ska säkerställa att mekanismer som används för att bevilja certifieringen beskriver tillräckliga utvärderingsmetoder för att bedöma överensstämmelsen mellan behandlingen av personuppgifter och certifieringskriterierna*”. Vad gäller det första området som ska ingå i utvärderingsmetoderna anser styrelsen vidare att nödvändigheten och proportionaliteten även bör bedömas i förhållande till de berörda registrerade, i tillämpliga fall. Slutligen noterar styrelsen att det

[3] För ett liknande resonemang, se riktlinjer 1/2018, punkt 44.

saknas en hänvisning till dokumentation av metoder och fynd. Därför uppmanar styrelsen de tyska tillsynsmyndigheterna att ändra utkastet till krav och uttryckligen inkludera dessa hänvisningar.

32. Vad gäller de befintliga certifieringarna (avsnitt 7.4 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav) anser styrelsen att fjärde strecksatsen på sidan 13 är förvirrande, då det är oklart vilket sambandet är mellan giltighetstiderna för en aktuell och en tidigare certifiering, liksom hur de skulle passa ihop. Det verkar heller inte möjligt att ifrågasätta giltigheten av certifiering som tidigare utfärdats av ett annat ackrediterat certifieringsorgan. Sammanfattningsvis skulle punkten behöva lite klarhet i fråga om förhållandet mellan de olika nämnda delarna. Styrelsen rekommenderar att de tyska tillsynsmyndigheterna ändrar utkastet, särskilt genom att förtydliga att giltighetstiden för certifieringen enligt den allmänna dataskyddsförordningen inte får vara beroende av giltigheten för andra typer av certifieringar.

33. Vad gäller avsnitt 7.5 (”värdering”) i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav, uppmanar styrelsen de tyska tillsynsmyndigheterna att ändra avsnittets titel till ”granskning”.

34. Vad gäller de ändringar som påverkar certifieringen (avsnitt 7.10 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav) noterar styrelsen att man i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav fastställer att ”kunden informeras i god tid om ändringar av de rättsliga ramarna som berör honom”. Med tanke på att certifieringsorganets opartiskhet måste bevaras, uppmanar styrelsen de tyska tillsynsmyndigheterna att omformulera meningen för att tydliggöra att kunden, i god tid, förses med allmän information om ändringar som skulle kunna beröra honom. Styrelsen uppmanar dessutom de tyska tillsynsmyndigheterna att klargöra hänvisningen till ”Europeiska dataskyddsstyrelsens beslut” så att det blir tydligt vad som avses. Myndigheten kunde i stället till exempel hänvisa till ”handlingar som antagits av Europeiska dataskyddsstyrelsen”.

35. Dataskyddsstyrelsen noterar att avsnitt 7.11 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (upphörande, begränsning, upphävande eller återkallande av certifiering) inte omfattar certifieringsorganets skyldighet att godta beslut och påbud från de tyska tillsynsmyndigheterna om att återkalla eller inte utfärda certifiering till en sökande om kraven inte uppfyllts eller längre uppfylls. Dataskyddsstyrelsen rekommenderar därför att de tyska tillsynsmyndigheterna inkluderar denna skyldighet. Vidare uppmanar styrelsen de tyska tillsynsmyndigheterna att ersätta ordet ”begränsning” med ”minskning” från avsnittets titel, i enlighet med bilagan till riktlinjerna.

2.2.7 ANDRA YTTERLIGARE KRAV

36. Vad gäller underavsnitt 8.11.3 i de tyska tillsynsmyndigheternas utkast till ackrediteringskrav (”klagomålshantering”) uppmanar styrelsen de tyska tillsynsmyndigheterna att ersätta hänvisningen till ”motiverade klagomål” med ”underbyggda klagomål” för ökad tydlighet.

3 SLUTSATSER OCH REKOMMENDATIONER

37. Utkastet till ackrediteringskrav från de tyska tillsynsmyndigheterna i förbundsstaten och delstaterna kan leda till att ackrediteringen av certifieringsorgan tillämpas inkonsekvent, och följande ändringar behöver göras:

38. Vad gäller ”allmänna anmärkningar” rekommenderar styrelsen att de tyska tillsynsmyndigheterna

1) tar bort hänvisningen till ”dataskyddsstyrelsens auktorisering”, så att utkastet följer ordalydelsen i den allmänna dataskyddsförordningen.

39. Vad gäller ”allmänna krav för ackreditering” rekommenderar styrelsen att de tyska tillsynsmyndigheterna

1) ändrar kraven avseende rättsligt ansvar (underavsnitt 4.1) så att de följer riktlinjerna,

2) ändrar underavsnitt 4.1.2.2 för att i certifieringsavtalet inkludera skyldigheten att ge de tyska tillsynsmyndigheterna fullständig insyn i certifieringsförfarandet och ge certifieringsorganet tillgång till sökandens behandling av personuppgifter,

3) i underavsnitt 4.1.2.2 inkluderar en uttrycklig hänvisning till den behöriga tillsynsmyndighetens arbetsuppgifter och befogenheter, i enlighet med bilagan,

4) i certifieringsavtalets delar inkluderar skyldigheten att tillåta att certifieringsorganet offentliggör all information som behövs för att bevilja certifiering enligt artiklarna 42.8 och 43.5 i den allmänna dataskyddsförordningen,

5) inkluderar en uttrycklig hänvisning till ”produkter, förfaranden och tjänster som berörs av certifieringen” i sjätte strecksatsen till underavsnitt 4.1.2.2,

6) i underavsnitt 4.2.7 stärker de tillämpliga kriterierna för certifieringsorgan som tillhör eller kontrolleras av en separat rättslig enhet, för att kunna beakta att alla typer av ekonomiska förhållanden mellan certifieringsorganet och den rättsliga enheten, beroende på dess funktioner, kan påverka opartiskheten hos dess certifieringsverksamhet.

40. Vad gäller ”resurskraven” rekommenderar styrelsen att de tyska tillsynsmyndigheterna

1) anpassar ordalydelsen i underavsnitt 6.1.2.1 till riktlinjerna genom att kräva att kunskapen är relevant och lämplig.

41. Vad gäller ”förfarandekraven” rekommenderar dataskyddsstyrelsen att de tyska tillsynsmyndigheterna

1) ändrar i avsnitt 7.1 så att det innehåller en uttrycklig hänvisning till certifieringsorganets skyldighet att uppfylla de ytterligare kraven,

2) inkluderar en hänvisning till hanteringen av ett godkänt europeiskt sigill för dataskydd,

3) anpassar ordalydelsen i avsnitt 7.2 till riktlinjerna genom att inkludera hänvisningen till avtalet/avtalen mellan den personuppgiftsansvarige och personuppgiftsbiträdet,

4) i avsnitt 7.4 inkluderar certifieringsorganets skyldighet att beskriva tillräckliga utvärderingsmetoder för att bedöma överensstämmelsen mellan behandlingen av personuppgifter och certifieringskriterierna,

5) i avsnitt 7.4 förtydligar att giltighetstiden för certifieringen enligt den allmänna dataskyddsförordningen inte får vara beroende av giltigheten för andra typer av certifieringar,

6) i avsnitt 7.11 inkluderar certifieringsorganets skyldighet att godta beslut och påbud från de tyska tillsynsmyndigheterna om att återkalla eller inte utfärda certifiering till en sökande om kraven för certifiering inte längre uppfylls.

4 AVSLUTANDE ANMÄRKNINGAR

42. Detta yttrande riktas till de tyska tillsynsmyndigheterna i förbundsstaten och delstaterna och kommer att offentliggöras i enlighet med artikel 64.5 b i den allmänna dataskyddsförordningen.

43. Enligt artikel 64.7 och 64.8 i den allmänna dataskyddsförordningen ska de tyska tillsynsmyndigheterna, inom två veckor efter att yttrandet inkommit, i elektroniskt format meddela ordföranden om huruvida de kommer att hålla fast vid eller ändra sitt utkast till beslut. Inom samma period ska de tillhandahålla det ändrade utkastet till beslut eller, om de inte avser att följa styrelsens yttrande, tillhandahålla en relevant motivering till varför de inte avser att följa detta yttrande, helt eller delvis.

44. De tyska tillsynsmyndigheterna ska meddela dataskyddsstyrelsen om det slutliga beslutet för att det ska införas i registret över beslut som hanteras inom mekanismen för enhetlighet, i enlighet med artikel 70.1 y i den allmänna dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)