Yttrande från styrelsen (art. 64)

Yttrande 14/2020 om utkastet till beslut från Irlands behöriga tillsynsmyndighet om godkännande av kraven för ackreditering av ett certifieringsorgan enligt artikel 43.3 (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 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 dataskyddsförordningen) tillämpas enhetligt i hela Europeiska ekonomiska samarbetsområdet. I enlighet med artikel 64.1 i 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 tillsynsmyndighet för dataskydd eller det nationella ackrediteringsorganet kommer att tillämpa för ackrediteringen av ett certifieringsorgan. I 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 från ISO 17065 och dataskyddsstyrelsens riktlinjer om ackreditering av certifieringsorgan).

2) Med hänvisning till artikel 43 i 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 dataskyddsförordningen (2016/679) (nedan kallade riktlinjerna) och riktlinjer 1/2018 om certifiering 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.

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

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 man i artikel 43.2 a–e återspeglar 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 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. Den irländska tillsynsmyndigheten 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. Irlands nationella ackrediteringsorgan INAB kommer att genomföra ackrediteringar av certifieringsorgan för att intyga att dessa tillämpar certifieringskriterier i enlighet med dataskyddsförordningen. Detta innebär att det irländska nationella ackrediteringsorganet kommer att tillämpa ISO 17065 och de ytterligare krav som fastställts av irländska tillsynsmyndigheten, 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 dataskyddsstyrelsens 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. Tillgänglig 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 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 den irländska tillsynsmyndigheten har valt att använda sig av det nationella ackrediteringsorganet för att utfärda ackrediteringar, efter att ha utarbetat ytterligare krav i enlighet med riktlinjerna som ackrediteringsorganet ska använda när det utfärdar en ackreditering.

4. Denna utvärdering av den irländska tillsynsmyndighetens ytterligare ackrediteringskrav syftar till att undersöka hur de skiljer sig från riktlinjerna och i synnerhet bilaga 1 (i fråga om tillägg eller strykningar). 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 tillsynsmyndigheten definierar ackrediteringskraven för certifieringsorgan så att en praktisk och enhetlig tillämpning blir möjlig, mot bakgrund av tillsynsmyndighetens arbete.

6. Med hänsyn till deras sakkunskap anser dataskyddsstyrelsen att det är viktigt att de nationella ackrediteringsorganen får ett visst handlingsutrymme vid utarbetandet av vissa specifika bestämmelser inom ramen för 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 utkastet till ackrediteringskrav innebär detta att dataskyddsstyrelsen inte har några synpunkter i det aktuella fallet och att den irländska tillsynsmyndigheten inte behöver vidta några ytterligare åtgärder.

9. I detta yttrande beaktas inte de dokument som lämnats in av den irländska tillsynsmyndigheten som inte omfattas av artikel 43.2 i dataskyddsförordningen, t.ex. hänvisningar till nationell lagstiftning. Dataskyddsstyrelsen konstaterar dock att den nationella lagstiftningen bör överensstämma med 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 dataskyddsförordningen på ett korrekt sätt.

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

7) Öppen hantering av klagomål om överträdelser av certifieringen.

10. Med beaktande av att det

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

b. i artikel 43.3 i dataskyddsförordningen föreskrivs att kraven för ackreditering av certifieringsorgan ska godkännas av den tillsynsmyndighet som är behörig,

c. i artikel 57.1 p och q i 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 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 tillsynsmyndighet kan upprätta och som ska tillämpas när det nationella ackrediteringsorganet ackrediterar ett certifieringsorgan.

anser dataskyddsstyrelsen följande:

2.2.1 INLEDNING (avsnitt 0 i irländska tillsynsmyndighetens utkast till ackrediteringskrav)

11. Dataskyddstyrelsen medger att samarbetsvillkor, som reglerar förhållandet mellan ett nationellt ackrediteringsorgan och tillsynsmyndigheten för dataskydd, 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. Dataskyddsstyrelsen noterar att hänvisningen till riktlinjerna om ackreditering som ”WP 261” inte är uppdaterad. Europeiska dataskyddsstyrelsen antog riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i dataskyddsförordningen (2016/679). Därför uppmanar dataskyddsstyrelsen den irländska tillsynsmyndigheten att ändra ordalydelsen och hänvisa till riktlinjer 4/2018.

2.2.3 ALLMÄNNA KOMMENTARER

13. Dataskyddsstyrelsen noterar att den irländska tillsynsmyndigheten i sitt utkast till krav flera gånger hänvisar till den ”behöriga tillsynsmyndigheten”. Eftersom den behöriga tillsynsmyndigheten i det här fallet är den irländska tillsynsmyndigheten uppmanar dataskyddsstyrelsen denna att ersätta hänvisningen med ”the DPC” (uppgiftsskyddssamordnaren) eller ”the IE SA” (den irländska tillsynsmyndigheten) för att undvika förvirring.

14. Dataskyddsstyrelsen konstaterar att den irländska tillsynsmyndighetens utkast till krav innehåller ett avsnitt om termer och definitioner. Några av termerna används dock inte konsekvent i dokumentet, t.ex. ”object of evaluation” (utvärderingsobjekt) och ”ToE” (evalueringsobjekt). För att undvika förvirring uppmanar dataskyddsstyrelsen den irländska tillsynsmyndigheten att använda enhetlig terminologi i utkasten till krav.

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

15. När det gäller punkt 7 i underavsnitt 4.1.2 i den irländska tillsynsmyndighetens utkast till ackrediteringskrav anser dataskyddsstyrelsen att ordalydelsen är en aning otydlig med avseende på vem skälen för att godkänna certifiering är riktade till. Vidare är även hänvisningen till att ”underlätta” registret otydlig. Därför uppmanar dataskyddsstyrelsen den irländska tillsynsmyndigheten att omformulera utkastet så att det blir tydligare.

2.2.5 STRUKTURELLA KRAV (avsnitt 5 i utkastet till ackrediteringskrav)

16. Dataskyddsstyrelsen konstaterar att det i den irländska tillsynsmyndighetens utkast till ackrediteringskrav hänvisas till utnämningen av ”en person med relevant erfarenhet som är ansvarig för tillsynen av uppgiftsskydd och informationsstyrning”. Hänvisningen till relevant erfarenhet bör förtydligas vad gäller erfarenhet och maktbefogenhetens omfattning. Vidare tycks den här personens roll vara lik dataskyddsombudets. Dataskyddsstyrelsen uppmanar den irländska tillsynsmyndigheten att tydligt klargöra den här personens roll samt att specificera vad som utgör relevant erfarenhet.

2.2.6 RESURSKRAV (avsnitt 6 i utkastet till ackrediteringskrav)

17. När det gäller certifieringsorganspersonal (underavsnitt 6.1) noterar dataskyddsstyrelsen att kraven på personal med teknisk expertis och ansvar för att fatta beslut inbegriper minst fem års professionell erfarenhet relaterad till föremålet för certifieringen, medan personal med ansvar för utvärdering bör ha minst två års professionell erfarenhet. Likaså måste personal med juridisk expertis och ansvar för att fatta beslut ha minst fem års professionell erfarenhet, medan de som ansvarar för utvärderingar måste ha minst två års erfarenhet. Dataskyddsstyrelsen noterar att minimikravet på antalet år av professionell erfarenhet skiljer sig markant mellan personal med ansvar för beslutsfattande och personal med ansvar för utvärdering. I detta avseende anser dataskyddsstyrelsen att fokus bör ligga på typen av expertis snarare än på antalet år av professionell erfarenhet. Enligt dataskyddsstyrelsen bör utvärderare ha en mer specialiserad expertis och professionell erfarenhet av tekniska förfaranden (t.ex. granskning och certifiering), medan beslutsfattare bör ha en mer generell och övergripande expertis och professionell erfarenhet av dataskydd. Med anledning av detta uppmanar dataskyddsstyrelsen den irländska tillsynsmyndigheten att lägga mer fokus på den faktiska kunskap och/eller erfarenhet som är relevant för utvärderare respektive beslutsfattare samt att minska skillnaden i antalet år av erfarenhet som krävs från dessa.

2.2.7 RESURSKRAV (avsnitt 7 i utkastet till ackrediteringskrav)

18. När det gäller underavsnitt 7.10, ”Changes affecting certification” (Förändringar som påverkar certifiering), i den irländska tillsynsmyndighetens utkast till ackrediteringskrav noterar dataskyddsstyrelsen att det inte hänvisas till de ändringsförfaranden som ska fastställas enligt avsnitt 7.10 i bilagan. Dataskyddsstyrelsen uppmuntrar den irländska tillsynsmyndigheten att inkludera en sådan hänvisning samt att nämna några av de förfaranden som skulle kunna införas (t.ex. övergångsperioder, godkännandeförfaranden hos den relevanta tillsynsmyndigheten...). Vidare anser dataskyddsstyrelsen att förändringar i utvecklingen också är relevanta och kan påverka certifiering. Därför uppmuntrar dataskyddsstyrelsen den irländska tillsynsmyndigheten att föra in denna möjlighet i förteckningen över förändringar som påverkar certifiering. Slutligen välkomnar dataskyddsstyrelsen inkluderingen av personuppgiftsbrott och brott mot dataskyddsförordningen på förteckningen över förändringar som kan påverka certifiering. I syfte att garantera tydlighet uppmuntrar emellertid dataskyddsstyrelsen den irländska tillsynsmyndigheten att specificera att uppgiftsbrott eller brott mot dataskyddsförordningen ska tas i beaktande endast såtillvida de är relaterade till certifiering.

19. När det gäller förändringar som påverkar certifiering (underavsnitt 7.10 i den irländska tillsynsmyndighetens utkast till krav), och i synnerhet den femte punktsatsen, noterar dataskyddsstyrelsen att den irländska tillsynsmyndigheten hänvisar till ”Europeiska dataskyddsstyrelsen tillämpliga och bindande beslut” samt till artikel 39 i Europeiska dataskyddsstyrelsen arbetsordning, som omfattar ”alla slutliga dokument som antagits av Europeiska dataskyddsstyrelsen”. Dataskyddsstyrelsen uppmuntrar den irländska tillsynsmyndigheten att klargöra hänvisningen till ”Europeiska dataskyddsstyrelsens beslut” så att det blir tydligt vad som avses. Myndigheten kunde t.ex. i stället hänvisa till ”handlingar som antagits av Europeiska dataskyddsstyrelsen”.

20. Dataskyddsstyrelsen noterar att underavsnitt 7.11 i den irländska tillsynsmyndighetens utkast till krav (upphörande, begränsning, upphävande eller återkallande av certifiering) inte omfattar certifieringsorganets skyldighet att godta beslut och påbud från den irländska tillsynsmyndigheten om att återkalla eller inte utfärda certifiering till en sökande om kraven inte uppfyllts eller längre uppfylls.

Dataskyddsstyrelsen rekommenderar därför den irländska tillsynsmyndigheten att inkludera denna skyldighet.

3 SLUTSATSER OCH REKOMMENDATIONER

21. Den irländska tillsynsmyndighetens utkast till krav för ackreditering kan leda till inkonsekvent tillämpning av ackrediteringen av certifieringsorgan, och följande ändringar behöver göras:

22. När det gäller ”processkraven” rekommenderar dataskyddsstyrelsen att den irländska tillsynsmyndigheten

1) i underavsnitt 7.11 inkluderar certifieringsorganets skyldighet att godta beslut och påbud från den irländska tillsynsmyndigheten om att återkalla eller inte utfärda certifiering till en sökande om kraven för certifiering inte uppfyllts eller längre uppfylls.

4 AVSLUTANDE ANMÄRKNINGAR

23. Detta yttrande riktas till den irländska tillsynsmyndigheten och kommer att offentliggöras i enlighet med artikel 64.5 b i den allmänna dataskyddsförordningen.

24. Enligt artikel 64.7 och 64.8 i dataskyddsförordningen ska den irländska tillsynsmyndigheten, inom två veckor efter att yttrandet inkommit, i elektroniskt format meddela ordföranden om huruvida den kommer att hålla fast vid eller ändra utkastet till förteckning. Inom samma period ska den tillhandahålla det ändrade utkastet till förteckning eller, om den inte avser följa dataskyddsstyrelsens yttrande, tillhandahålla en relevant motivering till varför den inte avser följa detta yttrande, helt eller delvis.

25. Den irländska tillsynsmyndigheten 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 dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordföranden

(Andrea Jelinek)