Yttrande 10/2024 om utkastet till beslut från Sveriges behöriga tillsynsmyndighet om godkännande av kraven för ackreditering av ett certifieringsorgan enligt artikel 43.3 (dataskyddsförordningen)

Antaget den 23 maj 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande yttrande

med beaktande av artiklarna 63, 64.1 c, 64.3–64.8 och 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 (*dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

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

av följande skäl:

1. Dataskyddsstyrelsens viktigaste uppgift är att se till att förordning (EU) 2016/679 tillämpas på ett enhetligt sätt i hela Europeiska ekonomiska samarbetsområdet (EES). I enlighet med artikel 64.1 i dataskyddsförordningen ska dataskyddsstyrelsen avge ett yttrande om en tillsynsmyndighet avser att godkänna kraven för ackreditering av certifieringsorgan enligt artikel 43. Syftet med detta yttrande är därför att skapa en harmoniserad utformning av de krav som en tillsynsmyndighet för dataskydd eller det nationella ackrediteringsorganet ska tillämpa vid ackreditering av certifieringsorgan. Även om dataskyddsförordningen inte fastställer några särskilda ackrediteringskrav förespråkar den enhetlighet. Dataskyddsstyrelsen strävar efter att uppnå detta mål i sina yttranden, för det första genom att uppmana tillsynsmyndigheterna att utforma sina ackrediteringskrav i enlighet med strukturen i bilagan till dataskyddsstyrelsens riktlinjer för ackreditering av certifieringsorgan, och för det andra genom att analysera dem med hjälp av en mall som tillhandahålls av dataskyddsstyrelsen och som gör det möjligt att jämföra kraven (enligt ISO 17065 och dataskyddsstyrelsens riktlinjer för ackreditering av certifieringsorgan).

2. Med hänvisning till artikel 43 i dataskyddsförordningen ska de behöriga tillsynsmyndigheterna anta ackrediteringskrav. De ska dock tillämpa mekanismen för enhetlighet för att göra det möjligt att skapa förtroende för certifieringsmekanismen, särskilt genom att fastställa höga krav.

3. Även om ackrediteringskraven omfattas av mekanismen för enhetlighet bör de inte vara identiska. De behöriga tillsynsmyndigheterna har ett visst utrymme för egna bedömningar när det gäller det nationella eller regionala sammanhanget och de bör ta hänsyn till sin lokala lagstiftning. Syftet med dataskyddsstyrelsens yttrande är inte att skapa en enda uppsättning EU-krav, utan snarare att undvika större inkonsekvenser som bland annat kan påverka förtroendet för de ackrediterade certifieringsorganens oberoende eller expertis.

4. Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (2016/679) (*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 i samband med mekanismen för enhetlighet.

[1] Hänvisningar till ”unionen” i detta yttrande bör förstås som hänvisningar till ”EES”.

5. Om en medlemsstat föreskriver att certifieringsorganen ska ackrediteras av tillsynsmyndigheten bör tillsynsmyndigheten fastställa ackrediteringskrav, inbegripet, men inte begränsat till, de krav som anges i artikel 43.2. I jämförelse med skyldigheterna i samband med ackrediteringen av certifieringsorgan som utförs av nationella ackrediteringsorgan innehåller artikel 43 mindre information om kraven för ackreditering i de fall tillsynsmyndigheten själv genomför ackrediteringen. För att de ackrediteringskrav som tillämpas av tillsynsmyndigheten ska kunna bidra till en harmoniserad ackrediteringsstrategi bör de bygga på ISO/IEC 17065 och kompletteras med de ytterligare krav som en tillsynsmyndighet fastställer i enlighet med artikel 43.1 b. Dataskyddsstyrelsen noterar att kraven i ISO 17065 tas upp och specificeras i artikel 43.2 a–e, vilket kommer att bidra till enhetlighet[2].

6. Dataskyddsstyrelsens yttrande ska i enlighet med artiklarna 64.1 c, 64.3 och 64.8 i förordningen jämförda med artikel 10.2 i dataskyddsstyrelsens arbetsordning antas inom åtta veckor från den första arbetsdag då ordföranden och den behöriga tillsynsmyndigheten har beslutat att handlingarna är fullständiga. Ordföranden får besluta att förlänga denna period med ytterligare sex veckor med hänsyn till ämnets komplexitet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 SAMMANFATTNING AV SAKFÖRHÅLLANDENA

1. Den svenska tillsynsmyndigheten har lämnat in sitt utkast till ackrediteringskrav i enlighet med artikel 43.1 b till dataskyddsstyrelsen. Handlingarna bedömdes vara fullständiga den 11 mars 2024. Sveriges nationella ackrediteringsorgan kommer att ackreditera certifieringsorgan för certifiering enligt kriterierna i dataskyddsförordningen. Det innebär att det nationella ackrediteringsorganet kommer att använda ISO 17065 och de ytterligare krav som fastställts av den svenska tillsynsmyndigheten, när de har godkänts av den svenska tillsynsmyndigheten, efter att dataskyddsstyrelsen har yttrat sig om utkastet till krav, för att ackreditera certifieringsorgan.

2. På grund av ämnets komplexitet beslutade ordföranden att förlänga den inledande åttaveckorsperioden för antagande med ytterligare sex veckor, i enlighet med artikel 10.2 i dataskyddsstyrelsens arbetsordning.

2 BEDÖMNING

2.1 Dataskyddsstyrelsens övergripande resonemang angående det inlämnade utkastet till beslut

3. Syftet med detta yttrande är att bedöma de ackrediteringskrav som utarbetats av en tillsynsmyndighet, i förhållande till ISO 17065 eller en fullständig uppsättning krav, för att, i enlighet med artikel 43.1 i dataskyddsförordningen, göra det möjligt för ett nationellt ackrediteringsorgan eller

[2] Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen, punkt 39. Finns på https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_sv.

en tillsynsmyndighet att ackreditera certifieringsorgan som ansvarar för att utfärda och förnya certifiering i enlighet med artikel 42 i dataskyddsförordningen. Detta påverkar inte den behöriga tillsynsmyndighetens uppgifter och befogenheter. I detta fall noterar dataskyddsstyrelsen att den svenska lagstiftningen [3] ger det nationella ackrediteringsorganet i uppdrag att ackreditera certifieringsorgan enligt artikel 43 i dataskyddsförordningen genom att fastställa ytterligare krav som överensstämmer med riktlinjerna, vilka bör användas av det nationella ackrediteringsorganet vid ackreditering.

4. Denna bedömning av den svenska tillsynsmyndighetens ytterligare ackrediteringskrav syftar till att undersöka avvikelser (tillägg eller strykningar) från riktlinjerna, särskilt från bilaga 1. Dataskyddsstyrelsens yttrande tar också upp alla aspekter som kan påverka en konsekvent ackreditering av certifieringsorgan.

5. Det bör noteras att syftet med riktlinjerna för ackreditering av certifieringsorgan är att göra det lättare för tillsynsmyndigheterna att fastställa ackrediteringskrav. Bilagan till riktlinjerna utgör inte ackrediteringskrav i sig. Ackrediteringskraven för certifieringsorgan måste därför definieras av tillsynsmyndigheten på ett sätt som möjliggör en praktisk och konsekvent tillämpning i enlighet med tillsynsmyndighetens krav.

6. Dataskyddsstyrelsen medger att de nationella ackrediteringsorganen, med tanke på deras expertis, bör ges handlingsfrihet att fastställa vissa särskilda bestämmelser inom ramen för de tillämpliga ackrediteringskraven. Dataskyddsstyrelsen betonar emellertid att eventuella ytterligare krav bör definieras på ett sätt som möjliggör en praktisk och konsekvent tillämpning och översyn av dem efter behov.

7. Dataskyddsstyrelsen påpekar att ISO-standarder, särskilt ISO 17065, omfattas av immateriella rättigheter och hänvisar därför inte till texten i det aktuella dokumentet i detta yttrande. På grund av detta beslutade dataskyddsstyrelsen att i de fall det är relevant peka på särskilda delar av ISO-standarden, dock utan att återge texten.

8. Slutligen har dataskyddsstyrelsen genomfört sin bedömning i enlighet med den struktur som beskrivs i bilaga 1 till riktlinjerna (*bilagan*). Om ett visst avsnitt i den svenska tillsynsmyndighetens utkast till ackrediteringskrav inte nämns i yttrandet bör det tolkas som att dataskyddsstyrelsen inte har några kommentarer och inte ber den svenska tillsynsmyndigheten att vidta ytterligare åtgärder.

9. I detta yttrande beaktas inte punkter i den svenska tillsynsmyndighetens utkast som ligger utanför tillämpningsområdet för artikel 43.2 i dataskyddsförordningen, såsom hänvisningar till nationell lagstiftning. Icke desto mindre noterar dataskyddsstyrelsen att nationell lagstiftning bör vara förenlig med dataskyddsförordningen, när så krävs.

10. Dataskyddsstyrelsens yttrande beaktar eller kommenterar inte den vägledning som den svenska tillsynsmyndigheten har införlivat i utkastet till ackrediteringskrav.

[3] Punkt 4 i förordning 2018:219 med kompletterande bestämmelser till EU:s dataskyddsförordning.

2.2 Bedömningen fokuserar främst på att ackrediteringskraven möjliggör en konsekvent bedömning av följande (artikel 43.2 i dataskyddsförordningen och bilaga 1 till dataskyddsstyrelsens riktlinjer):

a. Att alla viktiga områden som betonas i bilagan till riktlinjerna, samt eventuella avvikelser från bilagan, tas upp.

b. Certifieringsorganets oberoende.

c. Certifieringsorganets intressekonflikter.

d. Certifieringsorganets expertis.

e. Lämpliga säkerhetsåtgärder för att säkerställa att dataskyddsförordningens certifieringskriterier tillämpas på lämpligt sätt av certifieringsorganet.

f. Förfaranden för utfärdande, periodisk översyn och återkallande av certifiering enligt dataskyddsförordningen.

g. Transparent hantering av klagomål om överträdelser av certifieringen.

11. Med beaktande av att

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

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

c. artikel 57.1 p och q i dataskyddsförordningen anger att en behörig tillsynsmyndighet ska utarbeta och offentliggöra kraven för ackreditering av certifieringsorgan och kan besluta att själv ackreditera certifieringsorgan,

d. artikel 64.1 c i dataskyddsförordningen anger att dataskyddsstyrelsen ska avge ett yttrande om en tillsynsmyndighet avser att godkänna ackrediteringskraven för ett certifieringsorgan i enlighet med artikel 43.3,

e. även de ytterligare krav som fastställts av den behöriga tillsynsmyndigheten ska tillämpas om ackrediteringen utförs av det nationella ackrediteringsorganet i enlighet med ISO/IEC 17065/2012,

f. bilaga 1 till riktlinjerna för ackreditering av certifieringsorgan föreslår krav som en tillsynsmyndighet för dataskydd ska utarbeta och som det nationella ackrediteringsorganet ska tillämpa vid ackreditering av certifieringsorgan,

är dataskyddsstyrelsen av följande åsikt:

2.2.1 PREFIX

12. Dataskyddsstyrelsen medger att samarbetsvillkor som reglerar förhållandet mellan ett nationellt ackrediteringsorgan och dess tillsynsmyndighet för dataskydd inte är ett krav för ackreditering av

certifieringsorgan. För fullständighetens och öppenhetens skull anser dataskyddsstyrelsen dock att sådana samarbetsvillkor, i förekommande fall, ska offentliggöras i ett format som tillsynsmyndigheten anser lämpligt.

2.2.2 ALLMÄNNA KOMMENTARER

13. Dataskyddsstyrelsen noterar att den svenska tillsynsmyndigheten i sitt utkast till ackrediteringskrav betecknar bilagan som ytterligare och kompletterande krav för ackreditering av certifieringsorgan. Dataskyddsstyrelsen uppmanar den svenska tillsynsmyndigheten att tydliggöra skillnaden mellan kompletterande och ytterligare krav i texten för att förbättra läsbarhet.

14. Dataskyddsstyrelsen noterar att det bara finns en definierad term i den svenska tillsynsmyndighetens utkast till ackrediteringskrav (dvs. sökande). För att kraven ska bli lättare att läsa uppmanar dataskyddsstyrelsen den svenska tillsynsmyndigheten att lägga till en förteckning över termer och definitioner som inbegriper följande begrepp:

- Ackreditering.
- Certifiering.
- Ackrediteringsorgan.
- Certifieringsorgan.
- Certifieringskriterier.
- Behörig tillsynsmyndighet.
- Uppdragsgivare.
- Dataskyddsstyrelsens riktlinjer för ackreditering.
- Evalueringsobjekt.

15. Dataskyddsstyrelsen uppmanar också den svenska tillsynsmyndigheten att ersätta termen ”krav” med termen ”certifieringskriterier” i avsnitt 4.6 a i utkastet till ackrediteringskrav och att använda denna term konsekvent i hela dokumentet för bättre noggrannhet.

2.2.3 ALLMÄNNA ACKREDITERINGSKRAV

16. Dataskyddsstyrelsen noterar att den svenska tillsynsmyndigheten i avsnitt 4.1.1.1 om efterlevnad av dataskyddsförordningen i utkastet till ackrediteringskrav hänvisar till certifieringsorganets skyldighet att utföra en riskanalys och, vid behov, en konsekvensbedömning. Det är inte helt klart för dataskyddsstyrelsen vad dessa krav innebär. Av tydlighetsskäl rekommenderar dataskyddsstyrelsen därför att båda termerna förtydligas (t.ex. huruvida riskanalysen gäller fysiska personers rättigheter och friheter och om den nämnda konsekvensbedömningen är den konsekvensbedömning avseende dataskydd som ska utföras enligt dataskyddsförordningen).

17. I avsnitt 4.1.2.2 om certifieringsavtalets innehåll i utkastet till ackrediteringskrav noterar dataskyddsstyrelsen att en del som finns med i riktlinjerna för certifieringsavtalets innehåll saknas i den svenska tillsynsmyndighetens utkast till ackrediteringskrav. Mer specifikt innehåller den svenska tillsynsmyndighetens utkast till ackrediteringskrav inte avsnitt 4.1.2.2 i riktlinjerna som rör kravet att

sökanden ska ge den behöriga tillsynsmyndigheten full insyn i certifieringsförfarandet, inbegripet frågor som enligt avtal är konfidentiella och som rör dataskydd i enlighet med artiklarna 42.7 och 58.1 c i dataskyddsförordningen. Dataskyddsstyrelsen rekommenderar därför den svenska tillsynsmyndigheten att ändra detta krav i enlighet härmed.

18. I avsnitt 4.1.2.2 i utkastet till ackrediteringskrav noterar dataskyddsstyrelsen att certifieringsavtalet ska kräva att sökanden uppfyller certifieringssystemets krav. I utkastet anges dock inte att sökanden också alltid ska uppfylla de kriterier som har godkänts av den behöriga tillsynsmyndigheten eller dataskyddsstyrelsen i enlighet med artiklarna 43.2 b och 42.5 i dataskyddsförordningen enligt avsnitt 4.1.2.1 i dataskyddsstyrelsens riktlinjer. Dataskyddsstyrelsen rekommenderar därför den svenska tillsynsmyndigheten att ändra detta krav i enlighet härmed.

19. Dataskyddsstyrelsen rekommenderar också den svenska tillsynsmyndigheten att i samma avsnitt ange att certifieringsavtalet ska omfatta sökandens skyldighet att informera certifieringsorganet ”i händelse av betydande förändringar i dess faktiska eller rättsliga situation och i de av dess produkter, processer och tjänster som berörs av certifieringen” för att anpassa detta utkast till avsnitt 4.1.2.10 i riktlinjerna.

20. Dataskyddsstyrelsen noterar att den svenska tillsynsmyndigheten i avsnitt 4.1.2.2 e hänvisar till överträdelser av dataskyddsförordningen eller kompletterande lagstiftning till dataskyddsförordningen som kan påverka certifieringens giltighet. Av tydlighetsskäl uppmanar dataskyddsstyrelsen den svenska tillsynsmyndigheten att ersätta ”kompletterande lagstiftning till dataskyddsförordningen” med ”nationell lagstiftning”.

21. När det gäller avsnitt 4.1.2.3 om information till sökanden rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att i detta avsnitt i utkastet till ackrediteringskrav lägga till att den information som ska lämnas till sökanden ska dokumenteras i certifieringsavtalet.

22. I samma avsnitt noterar dataskyddsstyrelsen att utkastet till ackrediteringskrav inte inbegriper avsnitt 4.1.2.3 punkt 3 i riktlinjerna som anger att certifieringsavtalet inte ska minska sökandens ansvar för efterlevnaden av förordning (EU) 2016/679 och inte påverkar de behöriga tillsynsmyndigheternas uppgifter och befogenheter enligt artikel 42.5 i dataskyddsförordningen. Dataskyddsstyrelsen rekommenderar den svenska tillsynsmyndigheten att ändra detta utkast så att det överensstämmer med riktlinjerna.

23. När det gäller avsnitt 4.2.3 i den svenska tillsynsmyndighetens ackrediteringskrav välkomnar dataskyddsstyrelsen den svenska tillsynsmyndighetens beskrivningar av hur certifieringsorganets opartiskhet ska säkerställas. Med tanke på att den svenska tillsynsmyndigheten hänvisar till intressekonflikten i avsnitt 7.1 i utkastet rekommenderar dock dataskyddsstyrelsen den svenska tillsynsmyndigheten att lägga till att certifieringsorganets ”uppgifter och skyldigheter inte medför någon intressekonflikt enligt artikel 43.2 e” i utkastet för att säkerställa överensstämmelse med avsnitt 4.2.1 i riktlinjerna.

24. Dataskyddsstyrelsen välkomnar hänvisningen till att certifieringsorganet inte får vara personuppgiftsansvarig i förhållande till sökanden i avsnitt 4.2.3 b om certifieringsorganets opartiskhet i utkastet till ackrediteringskrav. För fullständighetens skull rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att i detta krav lägga till uppgiften att certifieringsorganet inte heller får vara gemensamt personuppgiftsansvarig i förhållande till sökanden.

25. I avsnitt 4.2.3 i utkastet till ackrediteringskrav anger den svenska tillsynsmyndigheten att certifieringsorganet ska redovisa de förbindelser, inbegripet ekonomiska förbindelser, som det har eller har haft med sökanden, utöver den förbindelse som uppstår genom ansökan om certifiering. Dataskyddsstyrelsen rekommenderar den svenska tillsynsmyndigheten att ändra detta utkast så att det överensstämmer med riktlinjerna genom att lägga till uppgiften att certifieringsorganet ska styrka sitt oberoende i enlighet med artikel 43.2 a i dataskyddsförordningen och att detta gäller bevis som rör certifieringsorganets finansiering i den mån det gäller garantier för opartiskhet.

26. I avsnitt 4.3.1 i utkastet till ackrediteringskrav rekommenderar dataskyddsstyrelsen också den svenska tillsynsmyndigheten, när det gäller certifieringsorganets skyldigheter att kontrollera att det har vidtagit alla åtgärder för att fullgöra sina skyldigheter, att dessa åtgärder ska vara lämpliga och täcka in alla ansvarsområden i de geografiska områden eller behörighetsområden där certifieringsorganet verkar i enlighet med avsnitt 4.3 i riktlinjerna.

2.2.4 RESURSKRAV

27. När det gäller avsnitt 6.1.1.2 v om personal med juridisk kompetens i den svenska tillsynsmyndighetens utkast till ackrediteringskrav noterar dataskyddsstyrelsen att utkastet inte helt överensstämmer med avsnitt 6.1 i riktlinjerna om personalens kunskap och expertis. För att säkerställa överensstämmelse rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att anpassa texten till ordalydelsen i riktlinjerna genom att lägga till att kunskapen och expertisen måste vara relevant och lämplig.

28. I samma avsnitt noterar dataskyddsstyrelsen att den svenska tillsynsmyndighetens utkast till ackrediteringskrav begränsar kravens tillämplighet på certifieringsorganets personal till den personal som ansvarar för utvärderingarna (6.1.2.2 a) och den personal som ansvarar för granskningar och certifieringsbeslut (6.1.2.2 b). Certifieringsorganet ska dock se till att all dess personal har relevant och lämplig kompetens enligt punkt 6.1 i riktlinjerna, inbegripet personal som ansvarar för att granska ansökningarna. Därför rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att anpassa resurskraven för certifieringsorganets personal till avsnitt 6.1 i riktlinjerna.

29. När det gäller punkt iv om personal med teknisk kompetens i samma avsnitt (6.1.1.2) i utkastet till ackrediteringskrav rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att anpassa kravens ordalydelse till riktlinjernas ordalydelse genom att lägga till att arbetserfarenheten ska vara ”betydande” i stället för ”tillräcklig”. Dataskyddsstyrelsen rekommenderar också att samma ändring görs i avsnitt 7.3.1 i kraven.

30. I samma avsnitt (punkt b) i den svenska tillsynsmyndighetens utkast till ackrediteringskrav noterar dataskyddsstyrelsen att en hänvisning görs till personalen som ansvarar för revisioner och personalen som ansvarar för certifieringsbeslut. Dataskyddsstyrelsen rekommenderar den svenska tillsynsmyndigheten att klargöra skillnaden mellan ”revisioner” och ”utvärderingar” och att, om det är lämpligt, överväga att ersätta termen ”revision” med termen ”granskning” för överensstämmelse med de ISO-termer som används i avsnitt 7.5.

31. I avsnitt 6.1.2.1 i den svenska tillsynsmyndighetens utkast till ackrediteringskrav anser dataskyddsstyrelsen också att det krav enligt vilket certifieringsorganet ska beakta kraven i punkt 7.4.10 vid utbildning av personal kan uppfattas som en begränsning av den kontinuerliga fortbildning som fordras enligt avsnitt 6.1 i riktlinjerna. Därför uppmanar dataskyddsstyrelsen den svenska

tillsynsmyndigheten att ta hänsyn till detta och omformulera kravet så att den kontinuerliga fortbildningen inte begränsas till utbildningar.

32. I avsnitt 6.2.2 i den svenska tillsynsmyndighetens utkast till ackrediteringskrav rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att lägga till uppgiften att certifieringsorganet behåller beslutsansvaret om underleverantörer används.

2.2.5 PROCESSKRAV

33. I avsnitt 7.4.6 i utkastet anger den svenska tillsynsmyndigheten att certifieringsorganet, utöver kraven i punkt 7.4.6 i ISO/IEC 17065:2012 och med beaktande av certifieringssystemets krav, ska ange när och hur sökanden informeras om avvikelser. Enligt riktlinjerna bör åtminstone ”informationens typ och tidpunkten för den anges”. Därför rekommenderar dataskyddsstyrelsen den svenska tillsynsmyndigheten att i kraven förtydliga att begreppet ”hur” inbegriper definitionen av informationens typ.

34. I avsnitt 7.4.9 i den svenska tillsynsmyndighetens utkast till ackrediteringskrav anges att certifieringsorganet, på begäran av IMY eller en annan tillsynsmyndighet, ska tillhandahålla all dokumentation från utvärderingen. Enligt dataskyddsstyrelsens riktlinjer gäller följande: ”Utöver kraven i punkt 7.4.9 i ISO/IEC 17065/2012 bör det krävas att tillsynsmyndigheten för dataskydd på begäran ska få full tillgång till dokumentationen.” Dataskyddsstyrelsen rekommenderar därför den svenska tillsynsmyndigheten att anpassa detta krav till riktlinjerna.

35. I samma avsnitt i den svenska tillsynsmyndighetens utkast till ackrediteringskrav anges också att certifieringsorganet ska tillhandahålla all dokumentation från utvärderingen, undantaget information vars offentliggörande kan leda till ekonomisk skada för sökanden och som inte är nödvändig för utövandet av befogenheter enligt artikel 58 i dataskyddsförordningen. Vidare anges att om certifieringsorganet inte lämnar ut information ska det informera IMY, eller en annan behörig myndighet, så snart som möjligt och motivera sitt beslut. Dataskyddsstyrelsen betonar att det inte är certifieringsorganet som ska avgöra vilken information som ska lämnas till den svenska tillsynsmyndigheten. Dataskyddsstyrelsen rekommenderar därför den svenska tillsynsmyndigheten att ändra detta krav för att klargöra att certifieringsorganet ska skicka all nödvändig information till den svenska tillsynsmyndigheten, även i enlighet med riktlinjerna, som föreskriver att tillsynsmyndigheten, på dennas begäran, får fullständig tillgång till dokumentationen.

36. Dataskyddsstyrelsen påpekar att det i avsnitt 7.6.1 b inte är certifieringsbegreppet ”certifikatets namn” som hänvisar till certifieringssystemets namn. Dataskyddsstyrelsen förstår också att begreppet ”utvärderingens omfattning” motsvarar certifieringens omfattning såsom avses i avsnitt 7.8 a i utkastet till ackrediteringskrav. Dataskyddsstyrelsen uppmanar därför den svenska tillsynsmyndigheten att genomföra dessa ändringar i ackrediteringskraven.

37. I avsnitt 7.7.1 i utkastet till ackrediteringskrav hänvisar den svenska tillsynsmyndigheten till att evalueringsobjektets version ska anges. Enligt riktlinjerna ska certifieringsorganet också ange evalueringsobjektets namn. Dataskyddsstyrelsen rekommenderar därför att detta krav anpassas till riktlinjerna.

38. I samma avsnitt konstaterar dataskyddsstyrelsen att den längsta giltighetstiden inte anges. Dataskyddsstyrelsen rekommenderar att den svenska tillsynsmyndigheten anpassar detta krav till riktlinjerna genom att lägga till att certifieringsorganet ska se till att certifieringarnas giltighetstid inte överstiger tre år.

39. I avsnitt 7.9.5 i den svenska tillsynsmyndighetens utkast till ackrediteringskrav uppmanar dataskyddsstyrelsen den svenska tillsynsmyndigheten att i stället för att endast hänvisa till de relevanta bestämmelserna i ISO-standarderna även hänvisa till artikel 43.2 c i det relevanta avsnittet i riktlinjerna.

40. I avsnitt 7.11.1 i utkastet till ackrediteringskrav noterar dataskyddsstyrelsen att den svenska tillsynsmyndigheten anger att meddelande ska skickas så snart som möjligt efter certifieringsorganets beslut och ska ange vilka åtgärder som kan vidtas för att återfå certifieringen. Dataskyddsstyrelsen anser att meddelande till den behöriga tillsynsmyndigheten ska skickas omedelbart, i stället för så snart som möjligt, och rekommenderar därför den svenska tillsynsmyndigheten att skärpa detta krav genom att omformulera det i enlighet med riktlinjerna.

2.2.6 KRAV PÅ FÖRVALTNINGSSYSTEMET

41. I avsnitt 8.1.2 i utkastet till ackrediteringskrav noterar dataskyddsstyrelsen att kravet på att dokumentation om förvaltningsprincipernas genomförande ska kunna tillhandahållas när som helst, inte bara under ackrediteringsförfarandet, saknas. Dataskyddsstyrelsen uppmanar den svenska tillsynsmyndigheten att klargöra att handlingarna kan tillhandahållas när som helst, även efter det att ackrediteringen har beviljats.

42. Enligt riktlinjerna ska certifieringsorganet permanent och kontinuerligt offentliggöra vilka certifieringar som utförts på vilken grund (eller inom vilka certifieringsmekanismer eller system), hur länge certifieringarna gäller enligt vilka regler och vilka villkor som gäller (skäl 100). Dataskyddsstyrelsen rekommenderar därför att den svenska tillsynsmyndigheten kräver att förvaltningssystemet säkerställer detta, i enlighet med avsnitt 8 i bilagan till riktlinjerna.

43. När det gäller avsnitt 8.1.2 d i den svenska tillsynsmyndighetens utkast till ackrediteringskrav noterar dataskyddsstyrelsen att förvaltningen av förfarandena, i synnerhet det faktum att förfarandena enligt avsnitt 9.3.4 i riktlinjerna ”i händelse av tillfällig eller permanent återkallelse av ackrediteringen ska integreras i certifieringsorganets förvaltningssystem. Detta gäller också meddelanden till kunderna.”, endast delvis omfattas av avsnitt 8.1.2 d i utkastet. Certifieringsorganets skyldighet att fastställa rutiner för införande av lämpliga förfaranden och kommunikationsstrukturer mellan certifieringsorganet och dess kunder finns inte heller med i utkastet. Dataskyddsstyrelsen rekommenderar därför den svenska tillsynsmyndigheten att ändra dessa krav och göra de tillägg som krävs för att anpassa dem till riktlinjerna.

3 SLUTSATSER OCH REKOMMENDATIONER

44. Den svenska tillsynsmyndighetens utkast till ackrediteringskrav kan leda till en inkonsekvent ackreditering av certifieringsorgan och följande ändringar måste göras:

45. När det gäller allmänna ackrediteringskrav rekommenderar dataskyddsstyrelsen att den svenska tillsynsmyndigheten

    1) förtydligar termerna ”riskanalys” och ”konsekvensanalys” i kraven,

    2) ändrar krav 4.1.1.1 genom att lägga till sökandens skyldighet att ge den behöriga tillsynsmyndigheten full insyn i certifieringsförfarandet, inbegripet frågor som enligt avtal är konfidentiella och som rör dataskydd i enlighet med artiklarna 42.7 och 58.1 c,

3) ändrar kriterium 4.1.2.2 så att det anger att sökanden också alltid ska uppfylla de kriterier som har godkänts av den behöriga tillsynsmyndigheten eller dataskyddsstyrelsen i enlighet med artiklarna 43.2 b och 42.5 i dataskyddsförordningen i linje med avsnitt 4.1.2.1 i dataskyddsstyrelsens riktlinjer,

4) i krav 4.1.2.2 lägger till att certifieringsavtalet ska omfatta sökandens skyldighet att informera certifieringsorganet ”i händelse av betydande förändringar i dess faktiska eller rättsliga situation och i de av dess produkter, processer och tjänster som berörs av certifieringen”,

5) i krav 4.1.2.3 lägger till att den information som ska lämnas till sökanden ska dokumenteras i certifieringsavtalet,

6) ändrar krav 4.1.2.3 så att det framgår att certifieringsavtalet inte ska minska sökandens ansvar för efterlevnaden av dataskyddsförordningen och inte påverkar de behöriga tillsynsmyndigheternas uppgifter och befogenheter enligt artikel 42.5 i dataskyddsförordningen,

7) i avsnitt 4.2.3 lägger till att certifieringsorganets skyldigheter och uppgifter inte leder till en intressekonflikt enligt artikel 43.2 e,

8) för fullständighetens skull lägger till i avsnitt 4.2.3 b att certifieringsorganet inte heller får vara gemensamt personuppgiftsansvarig med sökanden,

9) ändrar avsnitt 4.2.3 genom att lägga till certifieringsorganets skyldighet att styrka sitt oberoende i enlighet med artikel 43.2 a i dataskyddsförordningen och att detta gäller bevis som rör certifieringsorganets finansiering i den mån det gäller garantier för opartiskhet,

10) i avsnitt 4.3.1 förtydligar, när det gäller certifieringsorganets skyldigheter att kontrollera att det har vidtagit alla åtgärder för att fullgöra sina skyldigheter, att dessa åtgärder ska vara lämpliga och täcka in alla ansvarsområden i de geografiska områden eller behörighetsområden där certifieringsorganet verkar i enlighet med avsnitt 4.3 i riktlinjerna.

46. När det gäller resurskrav rekommenderar dataskyddsstyrelsen att den svenska tillsynsmyndigheten

1) anpassar avsnitt 6.1.1.2 v om personal med juridisk kompetens till riktlinjerna genom att lägga till att kunskapen och expertisen måste vara relevant och lämplig,

2) anpassar resurskraven för certifieringsorganets personal till avsnitt 6.1 i riktlinjerna,

3) lägger till att arbetserfarenheten ska vara ”betydande” i avsnitt 6.1.1.2 och avsnitt 7.3.1 iv om personal med teknisk kompetens,

4) tydliggör skillnaden mellan ”revisioner” och ”utvärderingar” och, om det är lämpligt, överväger att ersätta termen ”revision” med termen ”granskning” för överensstämmelse med de ISO-termer som används i avsnitt 7.5,

5) i avsnitt 6.2.2 lägger till att certifieringsorganet behåller beslutsansvaret om underleverantörer används.

47. När det gäller processkrav rekommenderar dataskyddsstyrelsen att den svenska tillsynsmyndigheten

1) i avsnitt 7.4.6 tydliggör att, när det anges att certifieringsorganet ska ange ”hur” sökanden får information om avvikelser, begreppet ”hur” inbegriper definitionen av informationens typ,

2) ändrar avsnitt 7.4.9 för att säkerställa att certifieringsorganet endast ger den svenska tillsynsmyndigheten full tillgång till dokumentation, på tillsynsmyndighetens begäran,

3) ändrar avsnitt 7.4.9 för att klargöra att certifieringsorganet ska skicka all nödvändig information till den svenska tillsynsmyndigheten, utan undantag,

4) ändrar avsnitt 7.7.1 genom att lägga till att även evalueringsobjektets namn ska anges av certifieringsorganet,

5) i avsnitt 7.7.1 lägger till att certifieringsorganet ska se till att certifieringarnas giltighetstid inte överstiger tre år,

6) ändrar krav 7.11.1 genom att ange att meddelande till den behöriga tillsynsmyndigheten ska skickas omedelbart i stället för så snart som möjligt.

48. När det gäller krav på förvaltningssystemet rekommenderar dataskyddsstyrelsen att den svenska tillsynsmyndigheten

1) kräver att förvaltningssystemet säkerställer att certifieringsorganet permanent och kontinuerligt måste offentliggöra vilka certifieringar som utförts på vilken grund (eller inom vilka certifieringsmekanismer eller system), hur länge certifieringarna gäller enligt vilka regler och vilka villkor som gäller (skäl 100).

4 AVSLUTANDE KOMMENTARER

49. Detta yttrande riktar sig till den svenska tillsynsmyndigheten och kommer att offentliggöras i enlighet med artikel 64.5 b i dataskyddsförordningen.

50. I enlighet med artikel 64.7 och 64.8 i dataskyddsförordningen ska den svenska tillsynsmyndigheten inom två veckor efter mottagandet av yttrandet på elektronisk väg meddela dataskyddsstyrelsens ordförande om huruvida den kommer att hålla fast vid eller ändra sitt utkast till förteckning. Inom samma tidsfrist ska tillsynsmyndigheten också översända det ändrade utkastet till förteckning. Om myndigheten inte avser att följa dataskyddsstyrelsens yttrande, helt eller delvis, ska den även tillhandahålla en relevant motivering.

51. Den svenska tillsynsmyndigheten ska meddela dataskyddsstyrelsen sitt slutliga beslut så att det kan införas i registret över beslut som omfattas av mekanismen för enhetlighet i enlighet med artikel 70.1 y i dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

(Anu Talus)

Antaget