Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (2016/679)

Version 3.0

Den 4 juni 2019

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Antagna

Versionshistorik

Version 3.0	Den 4 juni 2019	Bifogad finns bilaga 1 (version 2.0 av bilaga 1 antagen den 4 juni 2019 efter offentligt samråd)
Version 2.0	Den 4 december 2018	Antagande av riktlinjerna efter det offentliga samrådet – Samma dag som bilaga 1 (version 1.0) antogs för offentligt samråd
Version 1.0	Den 6 februari 2018	Artikel 29-gruppens antagande av riktlinjerna (version avsedd för offentligt samråd). Föreliggande version godkändes av Europeiska dataskyddsstyrelsen den 25 maj 2018

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e 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, och

med beaktande av resultaten av det offentliga samråd om riktlinjerna som ägde rum i februari 2018 och bilagan från det möte som ägde rum mellan den 14 december 2018 och den 1 februari 2019 i enlighet med artikel 70.4 i allmänna dataskyddsförordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING

1. Allmänna dataskyddsförordningen (förordning (EU) 2016/679) (nedan kallad *dataskyddsförordningen*), som trädde i kraft den 25 maj 2018, tillhandahåller ett moderniserat regelverk för dataskydd i Europa med inriktning på efterlevnad av redovisningsskyldighet och grundläggande rättigheter. En rad åtgärder som ska underlätta efterlevnaden av bestämmelserna i dataskyddsförordningen är centrala i detta nya regelverk. Åtgärderna omfattar obligatoriska krav under särskilda omständigheter (bland annat utnämning av dataskyddsombud och genomförande av konsekvensbedömning avseende dataskydd) och frivilliga åtgärder som t.ex. uppförandekoder och certifieringsmekanismer.

2. Som ett led i inrättandet av certifieringsmekanismer samt sigill och märkningar för dataskydd ska medlemsstaterna enligt artikel 43.1 i dataskyddsförordningen säkerställa att certifieringsorgan som utfärdar intyg enligt artikel 42.1 är ackrediterade av antingen den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet eller av båda två. Om ackrediteringen utförs av det nationella ackrediteringsorganet i enlighet med ISO/IEC 17065/2012, ska även de ytterligare krav som fastställts av den behöriga tillsynsmyndigheten tillämpas.

3. Begripliga certifieringsmekanismer kan förbättra efterlevnaden av dataskyddsförordningen och insynen för den registrerade, t.ex. mellan personuppgiftsansvariga och personuppgiftsbiträden i affärsrelationer mellan företag (B2B). Personuppgiftsansvariga och personuppgiftsbiträden kommer att kunna åberopa ett intyg från en oberoende tredje part för att visa att deras uppgiftsbehandling är förenlig med bestämmelserna[1].

4. I detta sammanhang har Europeiska dataskyddsstyrelsen beslutat att tillhandahålla riktlinjer för ackreditering. Det särskilda värdet och syftet med ackrediteringen ligger i att den officiellt bekräftar certifieringsorganens behörighet, vilket gör det möjligt att skapa förtroende för certifieringsmekanismen.

[1]Enligt skäl 100 i dataskyddsförordningen kan införandet av certifieringsmekanismer förbättra öppenheten och efterlevnaden av förordningen samt ge den registrerade möjlighet att bedöma nivån på relevanta produkters och tjänsters dataskydd.

5. Syftet med riktlinjerna är att ge vägledning om hur bestämmelserna i artikel 43 i dataskyddsförordningen ska tolkas och genomföras. De ska hjälpa medlemsstater, tillsynsmyndigheter och nationella ackrediteringsorgan att skapa en konsekvent och harmoniserad grund för ackreditering av certifieringsorgan som utfärdar intyg i enlighet med dataskyddsförordningen.

2 RIKTLINJERNAS TILLÄMPNINGSOMRÅDE

6. I riktlinjerna

- fastställs syftet med ackrediteringen i samband med dataskyddsförordningen,
- förklaras på vilka sätt certifieringsorgan kan ackrediteras i enlighet med artikel 43.1, varvid vissa nyckelfrågor som ska beaktas lyfts fram,
- finns en ram för fastställande av ytterligare ackrediteringskrav när ackrediteringen handläggs av det nationella ackrediteringsorganet, och
- finns en ram för fastställande av ytterligare ackrediteringskrav i de fall där ackrediteringen handläggs av tillsynsmyndigheten.

7. Riktlinjerna är inte en regelbok för ackreditering av certifieringsorgan enligt dataskyddsförordningen. De innebär inte någon ny teknisk standard för ackreditering av certifieringsorgan enligt dataskyddsförordningen.

8. Riktlinjerna riktar sig till:

- Medlemsstaterna, som ska se till att certifieringsorganen är ackrediterade av tillsynsmyndigheten och/eller det nationella ackrediteringsorganet.
- De nationella ackrediteringsorgan som utför ackrediteringen av certifieringsorgan enligt artikel 43.1 b.
- Den behöriga tillsynsmyndighet som anger ”ytterligare krav” utöver kraven i ISO/IEC 17065/2012[2] när ackrediteringen utförs av det nationella ackrediteringsorganet enligt artikel 43.1 b.
- Europeiska dataskyddsstyrelsen när denna utfärdar ett yttrande om och godkännande av de behöriga tillsynsmyndigheternas ackrediteringskrav enligt artiklarna 43.3, 70.1 p och 64.1 c.
- Den behöriga tillsynsmyndighet som specificerar ackrediteringskraven när ackreditering utförs av tillsynsmyndigheten enligt artikel 43.1 a.
- Andra berörda parter, t.ex. eventuella certifieringsorgan eller ägare av certifieringssystem som tillhandahåller certifieringskriterier och certifieringsförfaranden[3].

[2]Internationella standardiseringsorganisationen: Bedömning av överensstämmelse – Krav på organ som certifierar produkter, processer och tjänster.

[3] Systemägare innebär en identifierbar organisation som har fastställt certifieringskriterierna och de krav som ska uppfyllas vid bedömningen av överensstämmelse. Ackrediteringen görs av den organisation som gör bedömningar (artikel 43.4) enligt certifieringssystemets krav och utfärdar certifikaten (dvs. av certifieringsorganet, även kallat organ för bedömning av överensstämmelse). Den organisation som gör bedömningarna kan vara samma organisation som utvecklat och äger systemet, men det kan finnas arrangemang där en organisation äger systemet och en annan (eller flera andra) genomför bedömningarna.

9. Definitioner

10. Syftet med följande definitioner är att främja en gemensam förståelse av de grundläggande inslagen i ackrediteringsprocessen. De bör betraktas som referenspunkter och ska inte betraktas som ofelbara. Definitionerna bygger på befintliga regelverk och standarder, inte minst på relevanta bestämmelser i dataskyddsförordningen och ISO/IEC 17065/2012.

11. I föreliggande riktlinjer gäller följande definitioner:

12. *ackreditering* av certifieringsorgan: se avsnitt 3 om tolkningen av ackreditering i den mening som avses i artikel 43 i dataskyddsförordningen.

13. *ytterligare krav*: krav fastställda av behörig tillsynsmyndighet och enligt vilka en ackreditering utförs[4]

14. *certifiering*: bedömning och intygande från opartisk tredje part[5] om att uppfyllandet av certifieringskriterierna har påvisats.

15. *certifieringsorgan*: organ[6] som driver en certifieringsmekanism[7] och som utför tredjepartsbedömning av överensstämmelse[8]

16. *certifieringssystem*: ett certifieringssystem relaterat till specificerade produkter, processer och tjänster som omfattas av samma specificerade krav, specifika regler och förfaranden[9]

17. *kriterier* eller certifieringskriterier: de kriterier enligt vilka en certifiering (bedömning av överensstämmelse) utförs[10].

18. *nationellt ackrediteringsorgan*: det enda organet i en medlemsstat utsett i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 som utför ackreditering med behörighet från den staten[11].

3 TOLKNING AV ”ACKREDITERING” ENLIGT ARTIKEL 43 I DATASKYDDSFÖRORDNINGEN

19. Dataskyddsförordningen innehåller ingen definition av *ackreditering*. I förordning (EG) nr 765/2008 artikel 2.10, som innehåller allmänna ackrediteringskrav, definieras *ackreditering* som

---

[4] Artikel 43.1, 43.3 och 43.6.

[5] Observera att enligt ISO 17000 är ett intyg från tredje part (certifiering) ”tillämpligt på alla föremål för bedömning av överensstämmelse” (5.5) ”utom på de organ som genomför bedömningen av överensstämmelse, för vilka ackreditering är tillämplig” (5.6).

[6] Se ISO 17000, 2.5: ”organ som utför tjänster för bedömning av överensstämmelse”. ISO 17011: ”organ som utför bedömning av överensstämmelse och som kan bli föremål för ackreditering”. ISO/IEC 17065:3,12.

[7] Artikel 42.1 och 42.5 i dataskyddförordningen.

[8] Tredjepartsbedömning av överensstämmelse utförs av en organisation som är oberoende av den person eller organisation som tillhandahåller föremålet, och som inte har användarintressen i föremålet, se ISO 17000, 2.4.

[9] Se 3.9 jämförd med bilaga B till ISO 17065.

[10] Se artikel 42.5.

[11] Se artikel 2.11 i direktiv 765/2008/EG.

20. ”en förklaring från ett nationellt ackrediteringsorgan om att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, eventuella ytterligare krav, bland annat de som fastställs i sektorsspecifika program, för att utföra specifika bedömningar av överensstämmelse.”

21. Enligt ISO/IEC 17011 är

22. ”ackreditering ett intyg från tredje part rörande ett organ för bedömning av överensstämmelse som utgör ett formellt bevis för att organet är behörigt att utföra specifika bedömningar av överensstämmelse.”

23. I artikel 43.1 föreskrivs följande:

24. ”Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering. Medlemsstat ska säkerställa att dessa certifieringsorgan är ackrediterade av en eller båda av följande:

    (a) Den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.
    (b) Det nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 i enlighet med ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.”

25. I dataskyddsförordningen styrs ackrediteringskraven av följande:

- ISO/IEC 17065/2012 och de ”ytterligare krav” som fastställts av den tillsynsmyndighet som är behörig enligt artikel 43.1 b, när ackrediteringen utförs av det nationella ackrediteringsorganet och av tillsynsmyndigheten när den själv utför ackrediteringen.

26. I båda fallen ska de konsoliderade kraven omfatta de krav som anges i artikel 43.2.

27. Europeiska dataskyddsstyrelsen är medveten om att syftet med ackreditering är att ge en officiell förklaring om ett organs behörighet att utföra certifiering (bedömning av överensstämmelse)[12]. Ackreditering enligt dataskyddsförordningen ska innebära följande:

28. Ett intyg[13] från ett nationellt ackrediteringsorgan och/eller en tillsynsmyndighet som visar att ett certifieringsorgan[14] är kvalificerat att utföra certifiering i enlighet med artiklarna 42 och 43 i dataskyddsförordningen, med beaktande av ISO/IEC 17065/2012 och de ytterligare krav som fastställts av tillsynsmyndigheten och/eller av styrelsen.

[12] Se skäl 15 i 765/2008/EG.
[13] Se artikel 2.10 i Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter.
[14] Se definitionen av begreppet ”ackreditering” enligt ISO 17011.

4 ACKREDITERING ENLIGT ARTIKEL 43.1 I DATASKYDDSFÖRORDNINGEN

29. Enligt artikel 43.1 kan certifieringsorgan ackrediteras på flera olika sätt. Enligt dataskyddsförordningen ska tillsynsmyndigheterna och medlemsstaterna definiera förfarandet för ackreditering av certifieringsorgan. I detta avsnitt anges de olika ackrediteringssätt som avses i artikel 43.

4.1 Medlemsstaternas roll

30. Enligt artikel 43.1 ska medlemsstaterna *säkerställa* att certifieringsorganen är ackrediterade, men däri medges också att varje medlemsstat fastställer vem som ska vara ansvarig för att genomföra den bedömning som leder till ackreditering. På grundval av artikel 43.1 finns det tre tillgängliga alternativ: Ackreditering utförs,

(1) enbart av tillsynsmyndigheten, på grundval av dess egna krav,
(2) enbart av det nationella ackrediteringsorgan som anges i enlighet med förordning (EG) nr 765/2008 och på grundval av ISO/IEC 17065/2012 och med ytterligare krav som fastställts av den behöriga tillsynsmyndigheten, eller
(3) både av tillsynsmyndigheten och det nationella ackrediteringsorganet (och i enlighet med samtliga krav i punkt 2 ovan).

31. Det är den enskilda medlemsstaten som beslutar om det nationella ackrediteringsorganet eller tillsynsmyndigheten, eller båda tillsammans, ska genomföra ackrediteringarna, men den bör i alla händelser se till att tillräckliga resurser tillhandahålls[15].

4.2 Samverkan med förordning (EG) nr 765/2008

32. Europeiska dataskyddsstyrelsen noterar att artikel 2.11 i förordning (EG) nr 765/2008 definierar ett nationellt ackrediteringsorgan som ”det *enda* organet i en medlemsstat som har statligt bemyndigande att genomföra ackrediteringar”.

33. Artikel 2.11 kan anses oförenlig med artikel 43.1 i dataskyddsförordningen, vari medges att ackreditering utförs av ett annat organ än det nationella ackrediteringsorganet i medlemsstaten. Europeiska dataskyddsstyrelsen anser att syftet med EU-lagstiftningen är att frångå den allmänna principen att ackrediteringen uteslutande ska utföras av den nationella ackrediteringsmyndigheten. Därför ges tillsynsmyndigheterna samma befogenheter i fråga om ackreditering av certifieringsorgan. Artikel 43.1 är därför ett fall av *lex specialis* i förhållande till artikel 2.11 i förordning (EG) nr 765/2008.

4.3 Det nationella ackrediteringsorganets roll

34. Enligt artikel 43.1 b ska det nationella ackrediteringsorganet ackreditera certifieringsorgan i enlighet med ISO/IEC 17065/2012 och de ytterligare krav som fastställs av den behöriga tillsynsmyndigheten.

35. Av tydlighetsskäl noterar Europeiska dataskyddsstyrelsen att den särskilda hänvisningen till ”artikel 43.3 b första stycket ska tolkas som att ’dessa krav’ avser de ’ytterligare krav’ som fastställts av den behöriga tillsynsmyndigheten enligt artikel 43.1 b och kraven i artikel 43.2.

[15]Se artikel 4.9 i förordning (EG) nr 765/2008.

36. I samband med ackrediteringen ska de nationella ackrediteringsorganen tillämpa de ytterligare krav som tillhandahålls av tillsynsmyndigheterna.

37. Om ett certifieringsorgan med befintlig ackreditering på grundval av ISO/IEC 17065/2012 för certifieringssystem utan koppling till dataskyddsförordningen vill utvidga omfattningen av sin ackreditering till att täcka certifiering utfärdad enligt dataskyddsförordningen, ska det, om ackrediteringen handläggs av det nationella certifieringsorganet, uppfylla de ytterligare krav som fastställs av tillsynsmyndigheten. Om ackreditering för certifiering enligt dataskyddsförordningen erbjuds enbart av den behöriga tillsynsmyndigheten, ska ett certifieringsorgan som ansöker om ackreditering uppfylla de krav som fastställts av respektive tillsynsmyndighet.

4.4 Tillsynsmyndighetens roll

38. Europeiska dataskyddsstyrelsen noterar att tillsynsmyndigheten enligt artikel 57.1 q *ska* utföra ackrediteringen av ett certifieringsorgan enligt artikel 43 som en ”uppgift för tillsynsmyndigheten” enligt artikel 57, och enligt artikel 58.3 e har tillsynsmyndigheten befogenhet och rådgivande befogenhet att ackreditera certifieringsorgan i enlighet med artikel 43. Formuleringen i artikel 43.1 medger viss flexibilitet och tillsynsmyndighetens ackrediteringsfunktion bör betraktas som en uppgift enbart när så är lämpligt. Medlemsstaternas lagstiftning får utnyttjas för att lämna klargöranden på denna punkt. Vid ackreditering som utförs av ett nationellt ackrediteringsorgan krävs dock enligt artikel 43.2 a att certifieringsorganet påvisar oberoende och expertis i förhållande till syftet med certifieringsmekanismen på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande[16].

39. 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 ger artikel 43 mindre ledning med avseende på kraven för ackreditering i de fall där tillsynsmyndigheten själv genomför ackrediteringen. För att de ackrediteringskriterier som tillämpas av tillsynsmyndigheten ska kunna bidra till en harmoniserad strategi för ackreditering bör de bygga på ISO/IEC 17065 och kompletteras med de ytterligare krav som en tillsynsmyndighet fastställer i enlighet med artikel 43.1 b. Europeiska dataskyddsstyrelsen noterar att kraven i ISO 17065 tas upp och specificeras i artikel 43.2 a–e, vilket kommer att bidra till enhetlighet.

40. Om en medlemsstat föreskriver att certifieringsorganen ska ackrediteras av de nationella ackrediteringsorganen, bör tillsynsmyndigheten fastställa ytterligare krav som kompletterar de befintliga ackrediteringskonventioner som avses i förordning (EG) nr 765/2008 (artiklarna 3–14 däri berör hur ackreditering av organ för bedömning av överensstämmelse organiseras och hur de arbetar) och de tekniska föreskrifter som beskriver certifieringsorganens metoder och förfaranden. Förordning (EG) nr 765/2008 innehåller ytterligare vägledning om detta: I artikel 2.10 definieras ackreditering och det hänvisas till ”harmoniserade standarder” och ”eventuella ytterligare krav, bland annat de som fastställs i sektorsspecifika system”. Detta innebär att de ytterligare krav som fastställs av tillsynsmyndigheten bör omfatta särskilda

[16] De ytterligare krav som fastställs av tillsynsmyndigheten enligt artikel 43.1 b bör innehålla krav med avseende på oberoende och expertis. Se även bilaga 1 till riktlinjerna.

krav och vara inriktade på att underlätta bland annat bedömningen av certifieringsorganens oberoende och nivå av expertis i fråga om dataskydd, till exempel deras förmåga att utvärdera och certifiera personuppgiftsbehandling hos personuppgiftsansvariga och personuppgiftsbiträden i enlighet med artikel 42.1. Detta inbegriper nödvändig behörighet för sektoriella system och skyddet av fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter[17]. Bilagan till föreliggande riktlinjer kan förse behöriga tillsynsmyndigheter med upplysningar i samband med fastställandet av ”ytterligare krav” i enlighet med artiklarna 43.1 b och 43.3.

41. I artikel 43.6 anges att ”de krav som avses i punkt 3 i den här artikeln och de kriterier som avses i artikel 42.5 ska offentliggöras av tillsynsmyndigheten i ett lättillgängligt format.” För att säkerställa öppenhet ska därför alla kriterier och krav som godkänts av en tillsynsmyndighet offentliggöras. I fråga om kvalitet och förtroende för certifieringsorganen är det önskvärt att alla ackrediteringskrav är lätt tillgängliga för allmänheten.

4.5 Tillsynsmyndighet agerande som certifieringsorgan

42. Enligt artikel 42.5 får en tillsynsmyndighet utfärda certifieringar, men i dataskyddsförordningen finns inget krav på att denna ska vara ackrediterad för att uppfylla kraven i förordning (EG) nr 765/2008. Europeiska dataskyddsstyrelsen noterar att artikel 43.1 a, och särskilt artikel 58.2 h, samt 3 a, e–f, ger tillsynsmyndigheter befogenhet att utföra både ackreditering och certifiering och samtidigt ge råd och, i tillämpliga fall, återkalla certifieringar eller ålägga certifieringsorgan att inte utfärda certifieringar.

43. Det kan förekomma situationer där det är lämpligt eller påkallat att skilja mellan ackrediterings- och certifieringsrollerna och -uppgifterna, t.ex. om en tillsynsmyndighet och andra certifieringsorgan samexisterar i en medlemsstat och båda utfärdar samma typer av certifieringar. Tillsynsmyndigheterna bör därför vidta tillräckliga organisatoriska åtgärder för att separera uppgifterna enligt dataskyddsförordningen och därigenom förankra och underlätta användningen av certifieringsmekanismer, samtidigt som försiktighetsåtgärder vidtas för att undvika eventuella intressekonflikter till följd av dessa uppgifter. Dessutom bör medlemsstaterna och tillsynsmyndigheterna påminna sig om den harmoniserade europeiska nivån vid utarbetandet av nationell lagstiftning och nationella förfaranden för ackreditering och certifiering i enlighet med dataskyddsförordningen.

4.6 Ackrediteringskrav

44. Bilagan till dessa riktlinjer innehåller vägledning om hur ytterligare ackrediteringskrav identifieras. Däri fastställs de relevanta bestämmelserna i dataskyddsförordningen och föreslås krav som tillsynsmyndigheter och nationella ackrediteringsorgan bör överväga för att säkerställa överensstämmelse med dataskyddsförordningen.

45. Om certifieringsorgan är ackrediterade av det nationella ackrediteringsorganet enligt förordning (EG) nr 765/2008 ska ISO/IEC 17065/2012, med stöd i ovanstående, vara den relevanta ackrediteringsstandarden, kompletterad med de ytterligare krav som fastställts av tillsynsmyndigheten. Artikel 43.2 tar upp de allmänna bestämmelserna i ISO/IEC 17065/2012 mot bakgrund av skyddet av grundläggande rättigheter enligt dataskyddsförordningen. Regelverket i bilagan bygger på artikel 43.2 och ISO/IEC 17065/2012 för fastställande av krav och ytterligare kriterier för bedömningen av certifieringsorganens expertis i fråga om

[17]Artikel 1.2 i dataskyddförordningen.

dataskydd och deras förmåga att respektera fysiska personers rättigheter och friheter med avseende på behandling av personuppgifter enligt dataskyddsförordningen. Europeiska dataskyddsstyrelsen noterar att den är särskilt inriktad på att se till att certifieringsorganen har tillräcklig expertis i fråga om dataskydd i enlighet med artikel 43.1.

46. De ytterligare ackrediteringskrav som fastställs av tillsynsmyndigheten kommer att gälla samtliga certifieringsorgan som ansöker om ackreditering. Ackrediteringsorganet kommer att utvärdera huruvida certifieringsorganet är behörigt att utföra certifieringen i enlighet med de ytterligare kraven och syftet med certifieringen. Det ska finnas referenser till specifika sektorer eller områden för vilka certifieringsorganet är ackrediterat.

47. Europeiska dataskyddsstyrelsen noterar också att den särskilda expertisen i fråga om dataskydd också är nödvändig utöver kraven i ISO/IEC 17065/2012, i de fall där andra, externa, organ – t.ex. laboratorier eller revisorer – utför delar av eller inslag i certifieringen på uppdrag av ett ackrediterat certifieringsorgan. I dessa fall är det inte möjligt att ackreditera dessa externa organ enligt själva dataskyddsförordningen. För att säkerställa att dessa organ är lämpliga för sina uppgifter på de ackrediterade certifieringsorganens vägnar måste det ackrediterade certifieringsorganet dock se till att den expertis i fråga om dataskydd som krävs för det ackrediterade organet också finns och påvisas för det externa organet när det gäller de uppgifter som ska utföras.

48. Ramen för fastställande av ytterligare ackrediteringskrav, såsom den beskrivs i bilagan till dessa riktlinjer, är inte en regelbok för den ackrediteringsprocess som utförs av det nationella ackrediteringsorganet eller tillsynsmyndigheten. Den ger dock vägledning om strukturer och metoder och är därmed en verktygslåda som kan användas av tillsynsmyndigheterna för att fastställa ytterligare ackrediteringskrav.

BILAGA 1

Bilaga 1 innehåller vägledning för specifikationen av ”ytterligare” ackrediteringskrav enligt ISO/IEC 17065/2012 och i enlighet med artiklarna 43.1 b och 43.3 i dataskyddsförordningen.

I denna bilaga anges krav som en tillsynsmyndighet för dataskydd förslagsvis ska utarbeta och som gäller vid en ackreditering av ett certifieringsorgan som utförs av det nationella ackrediteringsorganet eller av den behöriga tillsynsmyndigheten[18]. Dessa ytterligare krav ska meddelas Europeiska dataskyddsstyrelsen innan de godkänns enligt artikel 64.1 c.

Denna bilaga ska samläsas med ISO/IEC 17065/2012. De avsnittsnummer som används här motsvarar dem som används i ISO/IEC 17065/2012. Om tillsynsmyndigheterna utför ackrediteringar i enlighet med artikel 43.1 a, är det lämpligt att så långt möjligt följa detta tillvägagångssätt. Det bidrar till en harmoniserad EU-ackreditering.

Utan att det påverkar tillämpningen av följande riktlinjer eller avsaknad av riktlinjer för någon punkt i ISO/IEC 17065/2012 får den behöriga tillsynsmyndigheten fastställa ytterligare krav avseende dessa punkter om detta sker i enlighet med nationell lagstiftning.

0 PREFIX

[Detta avsnitt avser överenskomna samarbetsvillkor mellan det nationella ackrediteringsorganet och tillsynsmyndigheten för dataskydd, t.ex. vem som ska ansvara för att ta emot ansökningar eller hur erkännandet av godkända kriterier ska organiseras som ett inslag i ackrediteringsprocessen.]

1 TILLÄMPNINGSOMRÅDE[19]

Tillämpningsområdet för ISO/IEC 17065/2012 ska definieras enligt dataskyddsförordningen. Riktlinjerna för ackreditering och certifiering innehåller närmare upplysningar om detta. Tillämpningsområdet för en certifieringsmekanism (t.ex. certifiering av behandling av molntjänster) bör beaktas i det nationella ackrediteringsorganets och den behöriga tillsynsmyndighetens bedömning under ackrediteringsförfarandet, särskilt när det gäller kriterier, expertis och utvärderingsmetod. Det breda tillämpningsområdet för ISO/IEC 17065/2012, som omfattar produkter, processer och tjänster, bör inte få innebära att kraven i dataskyddsförordningen sänks eller åsidosätts, t.ex. kan en styrningsmekanism inte vara den enda faktorn i en certifieringsmekanism eftersom certifieringen måste omfatta behandling av personuppgifter, dvs. behandlingsmoment. Enligt artikel 42.1 är certifiering med stöd i dataskyddsförordningen tillämplig endast på behandling av personuppgiftsansvariga och personuppgiftsbiträden.

2 REFERENSER

Dataskyddsförordningen har företräde framför ISO/IEC 17065/2012. Om det i de ytterligare kraven eller genom certifieringsmekanismen hänvisas till andra ISO-standarder, ska dessa tolkas i enlighet med kraven i dataskyddsförordningen.

---

[18] För närmare upplysningar om godkännandeförfarandet för certifieringskriterier, se avsnitt 4 i riktlinjerna för certifiering.

[19] Numrering hänvisar till ISO/IEC 17065/2012.

3 TERMER OCH DEFINITIONER

Med avseende på denna bilaga ska termerna och definitionerna i riktlinjerna för ackreditering (WP 261) och certifiering (EDPB 1/2018) gälla och ha företräde framför ISO-definitionerna.

4 ALLMÄNNA ACKREDITERINGSKRAV

4.1 Rättsliga och avtalsrelaterade frågor

4.1.1 Rättsligt ansvar

Ett certifieringsorgan bör (alltid) för det nationella ackrediteringsorganet eller den behöriga tillsynsmyndigheten kunna påvisa att de tillämpar uppdaterade förfaranden som överensstämmer med det rättsliga ansvar som anges i villkoren för ackreditering, också ytterligare krav i samband med tillämpningen av förordning 2016/679/EG. Observera att eftersom certifieringsorganet är en personuppgiftsansvarig/ett personuppgiftsbiträde, ska det kunna uppvisa belägg för att det finns förfaranden och åtgärder som är förenliga med förordning 2016/679/EG, särskilt för kontrollerna och hanteringen av kundorganisationens personuppgifter som en del av certifieringsprocessen.

Tillsynsmyndigheten kan besluta att lägga till ytterligare krav och förfaranden för att inför ackrediteringen kontrollera om certifieringsorganen uppfyller dataskyddsförordningens krav.

4.1.2 Certifieringsavtal

Minimikraven för ett certifieringsavtal ska kompletteras med följande punkter:

Certifieringsorganet ska, utöver kraven i ISO/IEC 17065/2012, påvisa att dess certifieringsavtal omfattar följande:

1. Krav på att sökanden alltid uppfyller både de allmänna certifieringskraven i den mening som avses i 4.1.2.2 a i ISO/IEC 17065/2012 och de kriterier som godkänts av den behöriga tillsynsmyndigheten eller Europeiska dataskyddsstyrelsen i enlighet med artikel 43.2 b och artikel 42.5.
2. Krav på att sökanden ger den behöriga tillsynsmyndigheten full insyn i certifieringsförfarandet, inbegripet frågor som är konfidentiella enligt avtal om efterlevnaden av bestämmelserna om dataskydd i enlighet med artiklarna 42.7 och 58.1 c.
3. Oförändrat ansvar för den sökande med avseende på överensstämmelsen med förordning 2016/679/EG. Behöriga tillsynsmyndigheters uppgifter och befogenheter i enlighet med artikel 42.5 påverkas ej.
4. Krav på att den sökande förser certifieringsorganet med all information och medger tillgång till sina behandlingsuppgifter, vilka är nödvändiga för att genomföra certifieringsförfarandet i enlighet med artikel 42.6.
5. Krav på att sökanden efterlever tillämpliga tidsfrister och förfaranden. I certifieringsavtalet ska anges att tidsfrister och förfaranden som till exempel uppstår till följd av certifieringsprogrammet eller andra föreskrifter måste iakttas och följas.
6. I fråga om punkt 4.1.2.2 c nr 1 i ISO/IEC 17065/2012 fastställs reglerna för giltighet, förnyelse och återkallelse i enlighet med artiklarna 42.7 och 43.4, inbegripet regler om lämpliga intervall för omprövning eller granskning (regelbundenhet) i enlighet med artikel 42.7.

7. Certifieringsorganet ska tillåtas lämna ut all information som är nödvändig för att utfärda en certifiering i enlighet med artiklarna 42.8 och 43.5,
8. Regler om nödvändiga försiktighetsåtgärder för utredning av klagomål i den mening som avses i 4.1.2.2 c nr 2 ska inbegripas, och dessutom ska, enligt led j, även uttryckliga förklaringar inbegripas om hur klagomål hanteras i enlighet med artikel 43.2 d.
9. Utöver minimikraven i punkt 4.1.2.2 i ISO/IEC 17065/2012 bör konsekvenserna för kunden också beaktas om en återkallelse eller ett tillfälligt upphävande av ackrediteringen för certifieringsorganet påverkar kunden.
10. Krav på att sökanden underrättar 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.

4.1.3 Användning av sigill och märkningar för dataskydd

Certifikat, sigill och märkningar får användas enbart i enlighet med artikel 42 och 43 och riktlinjerna för ackreditering och certifiering.

4.2 Opartisk förvaltning

Ackrediteringsorganet ska utöver kravet i punkt 4.2 i ISO/IEC 17065/2012 säkerställa följande:

1. Certifieringsorganet uppfyller den behöriga tillsynsmyndighetens ytterligare krav (i enlighet med artikel 43.1 b) på att
    a. i enlighet med artikel 43.2 a uppvisa separata belägg för sitt oberoende. Detta gäller särskilt belägg för finansieringen av certifieringsorganet, i den mån det berör försäkran om opartiskhet.
    b. med avseende på att dess uppgifter och skyldigheter inte medför någon intressekonflikt enligt artikel 43.2 e.
2. Certifieringsorganet har ingen relevant koppling till den kund som det bedömer.

4.3 Ansvarighet och finansiering

Ackrediteringsorganet ska, utöver kravet i 4.3.1 i ISO/IEC 17065/2012, regelbundet se till att certifieringsorganet kan vidta lämpliga åtgärder (t.ex. försäkring eller reserver) för att fullgöra sina skyldigheter i de geografiska regioner där det verkar.

4.4 Icke-diskriminerande villkor

Ytterligare krav får formuleras av tillsynsmyndigheten, om de överensstämmer med nationell lagstiftning.

4.5 Konfidentialitet

Ytterligare krav får formuleras av tillsynsmyndigheten, om de överensstämmer med nationell lagstiftning.

4.6 Offentligt tillgänglig information

Ackrediteringsorganet ska utöver kravet i 4.6 i ISO/IEC 17065/2012 av certifieringsorganet åtminstone kräva att

1. alla versioner (nuvarande och tidigare) av de godkända kriterier som använts i den mening som avses i artikel 42.5 offentliggörs och är lätt tillgängliga för allmänheten, liksom alla certifieringsförfaranden, varvid respektive giltighetsperiod ska anges,
2. information om förfaranden för hantering av klagomål och överklaganden offentliggörs i enlighet med artikel 43.2 d.

5 STRUKTURELLA KRAV, ARTIKEL 43.4 [”KORREKT” BEDÖMNING]

5.1 Organisationsstruktur och högsta ledning

Ytterligare krav får formuleras av tillsynsmyndigheten.

5.2 Mekanismer för säkerställande av opartiskhet

Ytterligare krav får formuleras av tillsynsmyndigheten.

6 RESURSKRAV

6.1 Certifiering av personal vid organet

Ackrediteringsorganet ska utöver kravet i avsnitt 6 i ISO/IEC 17065/2012 för varje certifieringsorgan se till att dess personal

1. har uppvisat lämplig och varaktig expertis (kunskap och erfarenhet) i fråga om dataskydd enligt artikel 43.1,
2. har oberoende och aktuell expertis i fråga om certifieringsobjektet enligt artikel 43.2 a och inte befinner sig i någon intressekonflikt enligt artikel 43.2 e,
3. åtar sig att iaktta de kriterier som avses i artikel 42.5 enligt artikel 43.2 b,
4. har relevant och ändamålsenlig kunskap om och erfarenhet av att tillämpa dataskyddslagstiftning,
5. har relevant och lämplig kunskap om och erfarenhet av tekniska och organisatoriska dataskyddsåtgärder (beroende på vad som är tillämpligt),
6. kan påvisa erfarenhet på de områden som anges i tilläggskraven 6.1.1, 6.1.4 och 6.1.5, särskilt avseende

Personal med teknisk expertis:

- Sådan personal ska ha erhållit en kvalifikation inom ett relevant tekniskt expertområde som åtminstone ska ligga på nivå 6 (t.ex. civilingenjör) inom den europeiska referensramen för kvalifikationer[20] inom det berörda reglerade yrket eller ha betydande yrkeserfarenhet.
- *Personal med ansvar för certifieringsbeslut* ska ha betydande professionell erfarenhet av att identifiera och genomföra dataskyddsåtgärder.
- *Personal med ansvar för utvärderingar* ska ha professionell erfarenhet av tekniskt dataskydd och kunskap om och erfarenhet av jämförbara arbetsuppgifter (t.ex. certifiering eller revision) och registreras på lämpligt sätt.

Personalen ska genom kontinuerlig fortbildning kunna påvisa att den upprätthåller domänspecifik teknisk och revisionsrelaterad kunskap.

Personal med juridisk expertis:

- Juridikstudier vid ett universitet godkänt av EU eller staten i EU i minst åtta terminer samt akademisk masterexamen (LL.M.) eller motsvarande, eller betydande yrkeserfarenhet.

[20] Se jämförelseverktyget för yrkeskvalifikationer: https://ec.europa.eu/ploteus/en/compare?

- *Personal med ansvar för certifieringsbeslut* ska kunna påvisa betydande professionell erfarenhet av lagstiftning om dataskydd och ska registreras på det sätt som medlemsstaten kräver.
- *Personal med ansvar för utvärderingar* ska kunna påvisa minst två års professionell erfarenhet av lagstiftning om dataskydd samt kunskap om och erfarenhet av jämförbara förfaranden (t.ex. certifiering eller revision) och registreras när så krävs av medlemsstaten.
    - Personalen ska genom kontinuerlig fortbildning kunna påvisa att den upprätthåller domänspecifik teknisk och revisionsrelaterad kunskap.

6.2 Utvärderingsresurser

Ytterligare krav får formuleras av tillsynsmyndigheten, om de överensstämmer med nationell lagstiftning.

7 KRAV MED AVSEENDE PÅ FÖRFARANDET ENLIGT ARTIKEL 43.2 C OCH D

7.1 Allmänt

Ackrediteringsorganet ska utöver kravet i avsnitt 7.1 i ISO/IEC 17065/2012 vara skyldigt att säkerställa följande:

1. Certifieringsorganen uppfyller den behöriga tillsynsmyndighetens ytterligare krav (enligt artikel 43.1 b) när de lämnar in ansökan för att se till att uppgifter och skyldigheter inte ger upphov till intressekonflikter enligt artikel 43.2 b.
2. Meddela de relevanta övervakningsorganen innan ett certifieringsorgan vid ett satellitkontor börjar använda ett godkänt europeiskt sigill för dataskydd i en ny medlemsstat.

7.2 Tillämpning

Utöver kraven i punkt 7.2 i ISO/IEC 17065/2012 bör det också föreligga ett krav på följande:

1. Certifieringsobjektet (evalueringsobjektet) ska ingående beskrivas i ansökan. Detta omfattar även en beskrivning av gränssnitt och överföringar till andra system och organisationer, protokoll och andra garantier.
2. I ansökan ska anges huruvida personuppgiftsbiträden används, och om personuppgiftsbiträdet är den sökande ska deras ansvarsområden och uppgifter beskrivas och ansökan ska innehålla relevanta avtal med personuppgiftsansvariga eller personuppgiftsbiträden.

7.3 Granskning av ansökan

Utöver kraven i punkt 7.3 i ISO/IEC 17065/2012 bör det också föreligga ett krav på följande:

1. Bindande utvärderingsmetoder i fråga om evalueringsobjektet ska fastställas i certifieringsavtalet.
2. Vid bedömningen i 7.3 e av huruvida det finns tillräcklig expertis tas i lämplig mån hänsyn till både den tekniska och juridiska expertisen i fråga om dataskydd.

7.4 Utvärdering

Utöver kraven i punkt 7.4 i ISO/IEC 17065/2012 ska certifieringsmekanismen beskriva tillräckligt omfattande utvärderingsmetoder för att möjliggöra en bedömning av behandlingens efterlevnad med certifieringskriterierna, vilket i tillämpliga fall kan omfatta

1. en metod för bedömning av behandlingarnas nödvändighet och proportionalitet i förhållande till deras syfte och de berörda registrerade personerna,
2. en metod för utvärdering av den personuppgiftsansvariges och personuppgiftsbiträdets täckning, sammansättning och bedömning med avseende på de rättsliga påföljderna enligt artiklarna 30, 32 och 35 och 36 i dataskyddsförordningen, och med beaktande av definitionen av tekniska och organisatoriska åtgärder enligt artiklarna 24, 25 och 32 i dataskyddsförordningen, i den mån ovannämnda artiklar är tillämpliga på certifieringsobjektet, och
3. en metod för bedömning av lösningarna, inbegripet garantier, skyddsåtgärder och förfaranden för säkerställande av skyddet av personuppgifter i samband med den behandling certifieringsobjektet får och visa att de rättsliga kraven i kriterierna är uppfyllda, och
4. dokumentation av metoder och resultat.

Certifieringsorganet bör åläggas att se till att dessa utvärderingsmetoder är standardiserade och allmänt tillämpliga. Detta innebär att jämförbara utvärderingsmetoder används för jämförbara evalueringsobjekt. Varje avvikelse från detta förfarande ska motiveras av certifieringsorganet.

Utöver kraven i punkt 7.4.2 i ISO/IEC 17065/2012 bör det tillåtas att utvärderingen genomförs av experter som erkänts av certifieringsorganet.

Utöver kraven i punkt 7.4.5 i ISO/IEC 17065/2012 bör det krävas att dataskyddscertifiering i enlighet med artiklarna 42 och 43 i dataskyddsförordningen, som till viss del redan omfattar certifieringsobjektet, får inbegripas i en befintlig certifiering. Det kommer dock inte att vara tillräckligt för att helt ersätta (partiella) utvärderingar. Certifieringsorganet ska kontrollera att kriterierna är uppfyllda. I och med erkännandet ska det alltid finnas en fullständig utvärderingsrapport eller information som gör det möjligt att utvärdera den tidigare certifieringsverksamheten och dess resultat. En certifieringsförklaring eller liknande certifieringsintyg bör inte anses räcka till för att kunna ersätta en rapport.

Utöver kraven i punkt 7.4.6 i ISO/IEC 17065/2012 bör det krävas att certifieringsorganet i sin certifieringsmekanism ska ange på vilket sätt den information som efterfrågas i punkt 7.4.6 upplyser kunden (den som ansöker om certifiering) om avvikelser från en certifieringsmekanism. I detta sammanhang bör åtminstone informationens typ och tidpunkten för den anges.

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.

7.5 Översyn

Utöver kraven i punkt 7.5 i ISO/IEC 17065/2012 krävs också förfaranden som garanterar periodisk översyn och återkallande av respektive certifieringar enligt artiklarna 43.2 och 43.3 i dataskyddsförordningen.

7.6 Certifieringsbeslut

Utöver punkt 7.6.1 i ISO/IEC 17065/2012 bör certifieringsorganet vara skyldigt att i sina förfaranden ingående ange hur dess oberoende och ansvar i fråga om enskilda certifieringsbeslut säkerställs.

7.7 Certifieringsdokumentation

Utöver kraven i punkt 7.7.1.e i ISO/IEC 17065/2012 och i enlighet med artikel 42.7 i dataskyddsförordningen bör det krävas att certifieringarnas giltighetstid inte är längre än tre år.

Utöver kraven i punkt 7.7.1.e i ISO/IEC 17065/2012 bör det krävas att den avsedda övervakningsperioden i den mening som avses i avsnitt 7.9 också dokumenteras.

Utöver kraven i punkt 7.7.1.f i ISO/IEC 17065/2012 bör certifieringsorganet vara skyldigt att ange certifieringsobjektet i certifieringsdokumentationen (om möjligt med angivande av version eller liknande kännetecken).

7.8 Katalog över certifierade produkter

Utöver kraven i punkt 7.8 i ISO/IEC 17065/2012 bör certifieringsorganet uppmanas att hålla informationen om certifierade produkter, processer och tjänster internt och offentligt tillgängliga. Certifieringsorganet kommer att offentliggöra en sammanfattning av utvärderingsrapporten. Syftet med denna sammanfattning är att bidra till öppenheten om vad som har certifierats och hur bedömningen gjorts. Det rör sig om förklaringar om

(a) certifieringens omfattning och begripliga beskrivningar av certifieringsobjektet (evalueringsobjektet),

(b) de olika certifieringskriterierna (även version eller funktionsstatus),

(c) utvärderingsmetoder, genomförda test och

(d) resultat.

Utöver kraven i punkt 7.8 i ISO/IEC 17065/2012 och i enlighet med artikel 43.5 i dataskyddsförordningen ska certifieringsorganet informera de behöriga tillsynsmyndigheterna om skälen till beviljande eller återkallande av den begärda certifieringen.

7.9 Tillsyn

Utöver punkterna 7.9.1, 7.9.2 och 7.9.3 i ISO/IEC 17065/2012, och i enlighet med artikel 43.2 c i dataskyddsförordningen, bör det krävas obligatoriska regelbundna övervakningsåtgärder för att bibehålla certifieringen under övervakningsperioden.

7.10 Ändringar som påverkar certifieringen

Utöver punkterna 7.10.1 och 7.10.2 i EN ISO/IEC 17065/2012 omfattar de ändringar som påverkar den certifiering som ska bedömas av certifieringsorganet följande: ändringar av lagstiftningen om skydd av personuppgifter, antagande av delegerade akter från Europeiska kommissionen i enlighet med artikel 43.8 och 43.9, Europeiska dataskyddsstyrelsens beslut och domstolsbeslut om dataskydd. De ändringsförfaranden som man kommer överens om här skulle bl.a. kunna omfatta: övergångsperioder, behörig tillsynsmyndighets godkännandeförfarande, förnyad bedömning av certifieringsobjekt och lämpliga åtgärder för att återkalla certifieringen om den certifierade behandlingsåtgärden inte längre är förenlig med de uppdaterade kriterierna.

7.11 Avslutande, begränsning, tillfällig indragning eller återkallelse av certifiering

Utöver kapitel 7.11.1 i ISO/IEC 17065/2012 bör certifieringsorganet i tillämpliga fall vara skyldigt att i tillämpliga fall och alltid skriftligen omedelbart underrätta den behöriga tillsynsmyndigheten och det nationella ackrediteringsorganet om vilka åtgärder som vidtagits och om förlängning, begränsning, tillfälligt upphävande och återkallelse av certifiering.

Enligt artikel 58.2 h ska certifieringsorganet vara skyldigt att godta beslut och anvisningar från den behöriga tillsynsmyndigheten om att återkalla eller inte utfärda certifikat till en kund (sökande), om kravet på certifiering inte (längre) är uppfyllt.

7.12 Uppgiftslagring

Certifieringsorganet bör vara skyldigt att se till att all dokumentation är fullständig, begriplig, uppdaterad och revisionsanpassad.

7.13 Klagomål och överklaganden, artikel 43.2 d

Utöver kraven i punkt 7.13.1 i ISO/IEC 17065/2012 bör certifieringsorganet också uppmanas att ange

(a) vem som kan lämna in klagomål eller invändningar,

(b) vem inom certifieringsorganet som behandlar dem,

(c) vilka kontroller som äger rum i detta sammanhang, och

(d) möjligheter till samråd med berörda parter.

Utöver kraven i punkt 7.13.2 i ISO/IEC 17065/2012 bör certifieringsorganet också uppmanas att ange

(a) hur och vem som ska får en sådan bekräftelse,

(b) gällande tidsfrister, och

(c) vilka processer som därefter kommer att inledas.

Utöver kraven i punkt 7.13.2 i ISO/IEC 17065/2012 måste certifieringsorganet definiera hur åtskillnad garanteras mellan certifieringsverksamhet och handläggningen av överklaganden och klagomål.

8 KRAV PÅ FÖRVALTNINGSSYSTEMET

Ett allmänt krav på förvaltningssystemet enligt kapitel 8 i ISO/IEC 17065/2012 är att genomförandet av alla krav från tidigare kapitel inom ramen för det ackrediterade certifieringsorganets tillämpning av certifieringsmekanismen dokumenteras, utvärderas, kontrolleras och övervakas på ett oberoende sätt.

Den grundläggande principen för förvaltningen är att välja ett system inom vilket målen kan fastställas på ett effektivt och ändamålsenligt sätt, särskilt i fråga om följande: genomförande av certifikattjänster med stöd i lämpliga specifikationer. Detta kräver insyn i och möjlighet till kontroll av certifieringsorganets genomförande av ackrediteringskraven och att det alltid följer reglerna.

Därför måste förvaltningssystemet omfatta en metod för efterlevnad och kontroll i enlighet med bestämmelserna om skydd av personuppgifter och för kontinuerligt kontroll hos det ackrediterade organet.

Dessa förvaltningsprinciper och deras dokumenterade genomförande ska vara transparenta och offentliggöras av det ackrediterade certifieringsorganet i enlighet med ackrediteringsförfarandet och artikel 58, och därefter – på begäran av tillsynsmyndigheten för dataskydd – när som helst under en undersökning i form av dataskyddstillsyn enligt artikel 58.1 b eller en granskning av certifieringar som utfärdats i överensstämmelse med artikel 42.7 enligt artikel 58.1 c.

Det ackrediterade certifieringsorganet ska 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).

8.1 Krav på det allmänna förvaltningssystemet

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att detta överensstämmer med nationell lagstiftning.

8.2 Dokumentation av förvaltningssystemet

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.3 Dokumentstyrning

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.4 Kontroll av redovisande dokument

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.5 Ledningens genomgång.

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.6 Internrevision

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.7 Korrigerande åtgärder

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

8.8 Förebyggande åtgärder

Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att dessa överensstämmer med nationell lagstiftning.

9 YTTERLIGARE KRAV[21]

9.1 Uppdatering av utvärderingsmetoderna

Certifieringsorganet ska fastställa förfaranden för att vägleda uppdateringen av utvärderingsmetoderna för tillämpning i samband med utvärderingen enligt punkt 7.4. Uppdateringen måste ske i samband med ändringar i den rättsliga ramen, de relevanta riskerna och de tekniska och organisatoriska åtgärdernas nivå genomförandekostnaderna för dessa.

9.2 Upprätthållande av expertis

Certifieringsorganen ska fastställa förfaranden som innebär att deras anställda fortbildas och därigenom uppdaterar sina färdigheter, med beaktande av innehållet i punkt 9.1.

9.3 Åligganden och behörigheter

9.3.1 Kommunikation mellan certifieringsorganet och dess kunder

Det ska finnas rutiner för införande av förfaranden och kommunikationsstrukturer mellan certifieringsorganet och dess kund. Detta ska omfatta följande:

1. Dokumentation av uppgifter som utförs av det ackrediterade certifieringsorganet och av organets ansvar med avseende på

[21] Den behöriga tillsynsmyndigheten får ange och lägga till ytterligare krav, förutsatt att detta överensstämmer med nationell lagstiftning.

a. begäranden om information eller
b. för att möjliggöra kontakt vid klagomål om certifiering.

2. Upprätthållande av en ansökningsprocess med avseende på följande:
    a. Information om en ansökans status.
    b. Den behöriga tillsynsmyndighetens utvärderingar med avseende på följande:
        i. Återkoppling
        ii. Beslut av den behöriga tillsynsmyndigheten.

9.3.2 Dokumentation av utvärderingen

Ytterligare krav får formuleras av tillsynsmyndigheten.

9.3.3 Förvaltning av klagomålshantering

Klagomålshantering ska inrättas som en integrerad del av förvaltningssystemet, som särskilt ska uppfylla kraven i punkterna 4.1.2.2 c, 4.1.2.2 j, 4.6 d och 7.13 i ISO/IEC 17065/2012 .

Relevanta klagomål och invändningar ska delges den behöriga tillsynsmyndigheten.

9.3.4 Förvaltning av återkallelse

Förfarandena i händelse av tillfällig eller permanent återkallelse av ackrediteringen ska integreras i certifieringsorganets förvaltningssystem. Detta gäller också meddelanden till kunderna.