Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen

Version 3.0

den 4 juni 2019

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

Antaget

Versionshistorik

Version 3.0	den 4 juni 2019	Införande av bilaga 2 (version 2.0 av bilaga 2 antagen den 4 juni 2019 efter offentligt samråd)
Version 2.1	den 9 april 2019	Antagande av en rättelse till riktlinjerna (punkt 45)
Version 2.0	den 23 januari 2019	Antagande av riktlinjerna efter offentligt samråd – samma dag som bilaga 2 (version 1.0) antogs inför offentligt samråd
Version 1.0	den 25 maj 2018	Antagande av riktlinjerna inför offentligt samråd

Innehållsförteckning

Europeiska dataskyddsstyrelsen har

med beaktande av artikel 70.1e 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 (allmän dataskyddsförordning),

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

med beaktande av artiklarna 12 och 22 i dess arbetsordning av den 25 maj 2018, och

med beaktande av resultaten av det offentliga samråd om riktlinjerna som ägde rum mellan den 30 maj 2018 och den 12 juli 2018, och för bilaga 2 som ägde rum mellan den 15 februari 2019 och den 29 mars 2019 i enlighet med artikel 70.4 i dataskyddsförordningen

ANTAGIT FÖLJANDE RIKTLINJER:

1 INLEDNING

1. Den allmänna dataskyddsförordningen (nedan kallad *förordning 2016/279*, *dataskyddsförordningen* eller *förordningen*) tillhandahåller ett moderniserat ramverk för ansvar och efterlevnad av grundläggande rättigheter vad gäller dataskydd inom Europa. En rad åtgärder som underlättar efterlevnaden av bestämmelserna i dataskyddsförordningen är centrala för detta nya ramverk. Dessa 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. Innan den allmänna dataskyddsförordningen antogs, fastställde artikel 29-gruppen att certifiering skulle kunna spela en viktig roll inom ramverket för ansvarsskyldighet i fråga om dataskydd.1 För att certifieringen ska kunna bli ett tillförlitligt bevis på efterlevnad av dataskyddet, bör det fastställas tydliga regler om certifieringskraven.2 I Artikel 42 i dataskyddsförordningen fastställs den rättsliga grunden för utarbetandet av sådana regler.

3. I artikel 42.1 i dataskyddsförordningen anges följande:

   ”Medlemsstaterna, tillsynsmyndigheterna, [Europeiska dataskydds]styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna

[1] Artikel 29-gruppen, Yttrande 3/2010 om principen om ansvarsskyldighet, WP 173, Bryssel, 13 juli 2010, punkterna 69–71.
[2] Artikel 29-gruppen, Yttrande 3/2010 om principen om ansvarsskyldighet, WP 173, punkt 69.

förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas."

4. Certifieringsmekanismer3 kan förbättra insynen för de registrerade, men också förbättra den mellan företag, t.ex. mellan personuppgiftsansvariga och personuppgiftsbiträden. I skäl 100 i dataskyddsförordningen anges att införandet av certifieringsmekanismer kan förbättra öppenheten och efterlevnaden av förordningen samt tillåta registrerade att bedöma nivån på relevanta produkters och tjänsters dataskydd.4

5. Genom dataskyddsförordningen införs inte någon certifieringsrätt eller certifieringsskyldighet för personuppgiftsansvariga och personuppgiftsbiträden. Enligt artikel 42.3 är certifiering en frivillig process för att påvisa efterlevnad av dataskyddsförordningen. Medlemsstater och tillsynsmyndigheter uppmanas att uppmuntra inrättandet av certifieringsmekanismer och kommer att avgöra de berörda aktörernas deltagande i certifieringsprocessen och livscykeln.

6. Dessutom är tillämpandet av godkända certifieringsmekanismer en faktor som tillsynsmyndigheterna måste beakta som en försvårande eller förmildrande faktor, när de bestämmer om administrativa sanktionsavgifter ska påföras och när de fattar beslut om avgiftens belopp (artikel 83.2 j).5

1.1 Riktlinjernas tillämpningsområde

7. Dessa riktlinjer har ett begränsat tillämpningsområde. De är inte en handbok för certifiering i enlighet med dataskyddsförordningen. Riktlinjernas primära syfte är att fastställa övergripande krav och kriterier som kan vara relevanta för alla typer av certifieringsmekanismer vilka införs i enlighet med artiklarna 42 och 43 i dataskyddsförordningen. Därför kommer riktlinjerna att

   - beskriva skälen till att certifieringen kan fungera som ett ansvarighetsredskap,
   - förklara de centrala begreppen i certifieringsbestämmelserna i artiklarna 42 och 43,
   - förklara omfattningen av vad som kan certifieras i enlighet med artiklarna 42 och 43 och syftet med certifieringen, samt
   - främja att resultatet av certifieringen är meningsfullt, otvetydigt, så reproducerbart som möjligt samt jämförbart oavsett kontrollant (jämförbarhet).

8. Dataskyddsförordningen gör det möjligt för medlemsstater och tillsynsmyndigheter att tillämpa artiklarna 42 och 43 på ett antal olika sätt. Riktlinjerna innehåller råd om tolkning och genomförande av bestämmelserna i artiklarna 42 och 43 som kommer att hjälpa medlemsstater, tillsynsmyndigheter och nationella ackrediteringsorgan att fastställa ett mer

[3] I dessa riktlinjer kallas certifieringsmekanismer och sigill samt märkningar för dataskydd kollektivt *certifieringsmekanismer*, se avsnitt 1.3.2.
[4] I skäl 100 anges att införandet av certifieringsmekanismer bör uppmuntra till att "förbättra öppenheten och efterlevnaden av denna förordning [...] så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd"
[5] Se artikel 29-gruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679 (WP 253).

konsekvent och harmoniserat tillvägagångssätt vad gäller certifieringsmekanismer i enlighet med dataskyddsförordningen.

9. De råd som återfinns i dessa riktlinjer kommer att avse följande:

   - Behöriga tillsynsmyndigheter och Europeiska dataskyddsstyrelsen när de godkänner certifieringskriterier enligt artikel 42.5, artikel 58.3 f samt artikel 70.1 o.
   - Certifieringsorgan, när de utarbetar och reviderar certifieringskriterier innan dessa inlämnas till den behöriga tillsynsmyndigheten för godkännande i enlighet med artikel 42.5.
   - Europeiska dataskyddsstyrelsen, när den godkänner ett europeiskt sigill för dataskydd i enlighet med artiklarna 42.5 och 70.1 o.
   - Tillsynsmyndigheter när de utarbetar sina egna certifieringskriterier.
   - Europeiska kommissionen, som har befogenhet att anta delegerade akter i syfte att specificera de krav som ska beaktas vad gäller certifieringsmekanismer i enlighet med artikel 43.8.
   - Europeiska dataskyddsstyrelsen, när den avger ett yttrande till Europeiska kommissionen om certifieringskraven i enlighet med artikel 70.1 q och artikel 43.8.
   - Nationella ackrediteringsorgan, som kommer att behöva ta hänsyn till certifieringskriterier som syftar till att ackreditera certifieringsorgan i enlighet med EN-ISO/IEC 17065/2012, samt de ytterligare kraven i enlighet med artikel 43.
   - Personuppgiftsansvariga och personuppgiftsbiträden, när de fastställer sin egen strategi för efterlevnad av dataskyddsförordningen och överväger certifiering som ett sätt att påvisa efterlevnad.

10. Europeiska dataskyddsstyrelsen kommer att publicera separata riktlinjer gällande identifiering av kriterier för godkännande av certifieringsmekanismer som överföringsverktyg till tredje länder eller internationella organisationer i enlighet med artikel 42.2.

1.2 Syftet med certifiering i enlighet med dataskyddsförordningen

11. I artikel 42.1 anges att certifieringsmekanismer ska inrättas i syfte ”att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning”.

12. Dataskyddsförordningen ger exempel på sammanhang där godkända certifieringsmekanismer kan användas som en faktor för att påvisa att de personuppgiftsansvariga och personuppgiftsbiträdena fullgör sina skyldigheter vad gäller följande:

   - Genomförandet och påvisandet av lämpliga tekniska och organisatoriska åtgärder i enlighet med artiklarna 24.1, 24.3, 25 samt 32.1 och 32.3.

- Tillräckliga garantier (personuppgiftsbiträden till personuppgiftsansvariga) i enlighet med punkt 1 och (delegerat personuppgiftsbiträde till personuppgiftsbiträde) punkt 4 som det hänvisas till i artikel 28.5.

13. Eftersom certifiering i sig inte bevisar efterlevnad utan snarare bildar ett element som kan användas för att påvisa efterlevnad, bör den utarbetas på ett öppet sätt. Påvisande av efterlevnad kräver styrkande dokumentation, i synnerhet skriftliga rapporter som inte bara upprepar utan faktiskt beskriver hur kriterierna uppfylls och, om de inte inledningsvis uppfyllts, beskriver vilka korrigeringar och åtgärder som genomförts och hur lämpliga dessa är, så att också skälen till att utfärda och upprätthålla certifieringen redovisas. Detta inbegriper utkastet till det enskilda beslutet om utfärdande, förlängning eller återkallande av en certifiering. Detta beslut bör innehålla de skäl, argument och bevis som följer av kriteriernas tillämpning och de bedömningar, slutsatser eller härledningar som följer av fakta eller förutsättningar som konstaterats under certifieringen.

1.3 Nyckelbegrepp

14. I följande avsnitt beskrivs nyckelbegreppen i artiklarna 42 och 43. Genom denna analys skapas en förståelse av grundläggande termer och certifieringens tillämpningsområde enligt dataskyddsförordningen.

1.3.1 Tolkning av termen certifiering

15. Dataskyddsförordningen innehåller ingen definition av termen certifiering. Internationella standardiseringsorganisationen (ISO) tillhandahåller en universell definition av certifiering som en skriftlig försäkran, utfärdad av ett oberoende organ (ett certifikat), om att produkten, tjänsten eller systemet i fråga uppfyller specifika krav. Certifiering kallas också *tredjepartsförfarande för bedömning av överensstämmelse* och certifieringsorgan kan också kallas *CAB* (organ för bedömning av överensstämmelse*).* I ISO/IEC 17000:2004 - Bedömning av överenstämmelse – Terminologi och allmänna principer (som ISO17065 hänvisar till), beskrivs certifiering enligt följande: tredjepartsattestering... kopplad till produkter, processer och tjänster.

16. En attestering är ett utfärdande av ett utlåtande, baserat på ett beslut efter en granskning, som fastställer att specifika krav har uppfyllts (avsnitt 5.2 ISO 17000:2004).

17. Inom ramen för certifiering enligt artiklarna 42 och 43 i dataskyddsförordningen ska certifiering hänvisa till tredjepartsattestering i anslutning till personuppgiftsansvarigas och personuppgiftsbiträdens behandlingsåtgärder.

1.3.2 Certifieringsmekanismer, sigill och märkningar

18. I dataskyddsförordningen definieras inte ”certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd” – och termerna används tillsammans. Ett certifikat är en försäkran

om överensstämmelse. Ett sigill eller en märkning kan användas för att styrka att certifieringsförfarandet har slutförts på ett framgångsrikt sätt. Ett sigill eller en märkning hänvisar vanligtvis till en logotyp eller symbol vars närvaro (utöver certifikatet) visar att certifieringsobjektet har utvärderats individuellt i ett certifieringsförfarande och följer de krav som anges i normgivande dokument, som t.ex. föreskrifter, standarder och tekniska specifikationer. Dessa krav inom ramen för certifiering enligt dataskyddsförordningen fastställs i de ytterligare krav som kompletterar reglerna för ackreditering av certifieringsorgan i ISO/IEC 17065/2012 och de certifieringskriterier som godkänts av den behöriga tillsynsmyndigheten eller styrelsen. Ett certifikat, sigill eller en märkning enligt dataskyddsförordningen kan endast utfärdas efter en oberoende bedömning utförd av ett ackrediterat certifieringsorgan eller en behörig tillsynsmyndighet som fastställer att certifieringskriterierna har uppfyllts.

19. Tabellen visar ett allmänt exempel på ett certifieringsförfarande.

Submission of application by controller or processor	Formal Check by CB	Assessment Pre-Evaluation	Assessment Evaluation of ToE	Assessment Validation of results	Information to CSA	Certification	Monitoring	Renewal of certification
Is the description of the target of evaluation (ToE) anambigous and complete including interfaces?	Can the ToE description be accepted?	What are the applicable criteria?	Does the ToE meet the criteria?	Are all relevant criteria specified reflecting the ToE?	Have the reasons for granting or withdrawing certification been provided?	Can the certificate be awarded?	Does the ToE continue to meet the criteria	Does the processing still meet the certification criteria?
Can access to the ToE processing activities be granted?	Are all documents complete and up -to - date?	What are the applicable evaluation methods?	Is the documentation of the ToE correct?	Has the evaluation been sufficiently documented ?		Are the reports ready for publishing?	Is the certificate/seal/trust mark used correctly?	Have areas of development been satisfactorily addressed?
Art. 42(6)	Art. 43(4)	Art. 43(4)	Art. 42(5), Art. 43(4)	Art. 43(4)	Art. 43(1), 43(5)	Art. 43(1); Art. 42 (7)	Art. 42 (7)	Art. 42 (7)

2 TILLSYNSMYNDIGHETERNAS ROLL

20. I artikel 42.5 anges att certifieringen ska utfärdas av ett ackrediterat certifieringsorgan eller av en behörig tillsynsmyndighet. Utfärdandet av certifiering är enligt dataskyddsförordningen inte en obligatorisk uppgift för tillsynsmyndigheterna. Istället tillåts enligt dataskyddsförordningen ett antal olika modeller. T.ex. kan en tillsynsmyndighet välja ett eller flera av följande alternativ:

- Själv utfärda certifiering med utgångspunkt i sitt eget certifieringssystem.

- Utfärda certifiering med utgångspunkt i sitt eget certifieringssystem, men delegera hela eller delar av bedömningsförfarandet till tredje part.
- Skapa ett eget certifieringssystem och överlåta certifieringsförfarandet till certifieringsorgan som utfärdar certifieringen.
- Uppmuntra marknaden att utveckla certifieringsmekanismer.

21. En tillsynsmyndighet kommer också behöva överväga sin roll mot bakgrund av de beslut som på nationell nivå fattas i fråga om ackrediteringsmekanismer – särskilt om tillsynsmyndigheten själv har befogenhet att ackreditera certifieringsorgan enligt artikel 43.1 i dataskyddsförordningen. Därför måste varje tillsynsmyndighet avgöra vilket tillvägagångssätt som ska användas för att uppfylla det övergripande syftet med certifiering i enlighet med dataskyddsförordningen. Detta kommer att fastställas inte bara med hänsyn till uppgifterna och befogenheterna i artiklarna 57 och 58, utan också med hänsyn till certifiering som en faktor som ska beaktas vid fastställandet av administrativa böter, och mer allmänt som ett sätt att påvisa efterlevnad.

2.1 Tillsynsmyndighet som certifieringsorgan

22. I de fall där en tillsynsmyndighet väljer att genomföra certifiering måste den noggrant utvärdera sin roll med avseende på de uppgifter den tilldelats inom ramen för dataskyddsförordningen. Tillsynsmyndighetens roll bör vara öppen för insyn när den utför sina uppgifter. Den kommer att behöva ta särskild hänsyn till maktdelningen i fråga om utredningar och genomförande för att undvika eventuella intressekonflikter.

23. När en tillsynsmyndighet fungerar som certifieringsorgan måste den säkerställa att en certifieringsmekanism inrättas och utveckla sina egna, eller anta andras, certifieringskriterier. Dessutom har varje tillsynsmyndighet som utfärdar certifieringar i uppgift att regelbundet se över dem (artikel 57.1 o) och befogenhet att återkalla dem i de fall där certifieringskraven inte längre uppfylls (artikel 58.2 h). För att uppfylla dessa krav är det lämpligt att inrätta ett certifieringsförfarande och förfarandekrav och, om inte annat anges t.ex. i nationell lagstiftning, ingå ett rättsligt bindande avtal för tillhandahållande av certifiering med den enskilda sökande organisationen. Det bör säkerställas att sökanden genom detta certifieringsavtal är skyldig att åtminstone uppfylla certifieringskriterierna. Detta inbegriper nödvändiga arrangemang för att genomföra utvärderingen, översynen av kriteriernas efterlevnad och en regelbunden granskning som ska omfatta tillgång till information och/eller lokaler, dokumentation och offentliggörande av rapporter och resultat samt undersökning av klagomål. Vidare förväntas en tillsynsmyndighet, utöver kraven i artikel 43.2, uppfylla kraven i riktlinjerna för ackreditering av certifieringsorgan.

2.2 Tillsynsmyndighetens ytterligare uppgifter avseende certifiering

24. I medlemsstater där certifieringsorgan blir verksamma har tillsynsmyndigheten följande befogenheter och uppgifter oberoende av sin egen verksamhet:

- Att utvärdera certifieringssystemets kriterier och utarbeta ett utkast till beslut (artikel 42.5).

- Att till styrelsen skicka utkastet till beslut när det avser att godkänna certifieringskriterierna (artikel 64.1 c och 64.7) samt ta hänsyn till styrelsens yttrande (artikel 64.1 c och artikel 70.1 t).
- Att godkänna certifieringskriterierna (artikel 58.3 f) innan ackreditering och certifiering kan äga rum (artiklarna 42.5 och 43.2. b)
- Att offentliggöra certifieringskriterierna (artikel 43.6).
- Att verka som behörig myndighet för EU-omfattande certifieringssystem, vilket kan leda till ett europeiskt sigill för dataskydd godkänt av Europeiska dataskyddsstyrelsen (artiklarna 42.5 och artikel 70.1 o).
- Att beordra ett certifieringsorgan att a) inte utfärda certifiering eller b) återkalla certifiering i fall där certifieringskraven (certifieringsförfaranden eller -kriterier) inte uppfylls eller inte längre uppfylls (artikel 58.2 h).

25. Dataskyddsförordningen ålägger tillsynsmyndigheten att godkänna certifieringskriterier, men inte att utveckla certifieringskriterier. En tillsynsmyndighet bör ha en tydlig uppfattning om vad den kan förvänta sig för att kunna godkänna certifieringskriterier i enlighet med artikel 42.5, särskilt i fråga om tillämpningsområde och innehåll för att påvisa efterlevnad av dataskyddsförordningen och med avseende på myndighetens uppgift att övervaka och genomföra tillämpningen av förordningen. Bilagan innehåller vägledning för att säkerställa ett harmoniserat tillvägagångssätt vid bedömningen av kriterier för godkännande.
26. I enlighet med artikel 43.1 ska certifieringsorganen meddela sin tillsynsmyndighet innan de utfärdar eller förnyar certifiering. Detta för att göra det möjligt för den behöriga tillsynsmyndigheten att utöva sina korrigerande befogenheter enligt artikel 58.2 h. Dessutom fastställs det i artikel 43.5 att certifieringsorgan ska informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen. Fastän dataskyddsförordningen ger tillsynsmyndigheterna rätt att avgöra hur de ska ta emot, erkänna, granska och hantera denna information operativt (detta kan t.ex. omfatta tekniska lösningar som möjliggör rapportering från certifieringsorgan), kan dock ett förfarande och kriterier också inrättas för att behandla information och rapporter från certifieringsorganet om varje framgångsrik certifieringsprojekt i enlighet med artikel 43.1. På grundval av denna information kan tillsynsmyndigheten utöva sin befogenhet för att beordra certifieringsorganet att återkalla eller att låta bli att utfärda en certifiering (artikel 58.2 h) och att övervaka och genomföra tillämpningen av kraven och kriterierna för certifiering i enlighet med dataskyddsförordningen (artiklarna 57.1 a och 58.2 h). Detta kommer att främja ett harmoniserat tillvägagångssätt och jämförbarhet vid certifiering av olika certifieringsorgan, samtidigt som tillsynsmyndigheterna fortlöpande underrättas om en organisations certifieringsstatus.

3 ETT CERTIFIERINGSORGANS ROLL

27. Ett certifieringsorgan har till uppgift att utfärda, granska, förnya och återkalla certifiering (artikel 42.5 och artikel 42.7) på grundval av en certifieringsmekanism och godkända kriterier (artikel 43.1). Detta innebär att certifieringsorganet eller en ägare av ett certifieringssystem måste fastställa certifieringskriterier och certifieringsförfaranden, inbegripet förfaranden för övervakning av efterlevnad, granskning, hantering av klagomål och återkallande. Certifieringskriterierna granskas, under efterlevnad av gällande regler och förfaranden, som en del av ackrediteringsförfarandet för utfärdande av certifiering, sigill eller märkningar (artikel 43.2 c).

28. Certifieringsmekanismer och certifieringskriterier är nödvändiga för att certifieringsorganet ska bli ackrediterat i enlighet med artikel 43. Certifieringskriteriernas tillämpningsområde och typ har en betydande inverkan på vad ett certifieringsorgan gör. Certifieringskriteriernas typ och tillämpningsområde påverkar certifieringsförfarandena och vice versa. Specifika kriterier kan exempelvis kräva särskilda utvärderingsmetoder, t.ex. inspektioner på plats och kodgranskning. Dessa förfaranden är obligatoriska för ackreditering och förklaras närmare i riktlinjerna för ackreditering.

29. Certifieringsorganet ska enligt dataskyddsförordningen förse tillsynsmyndigheterna med information, särskilt om enskilda certifieringar, som är nödvändig för att övervaka tillämpningen av certifieringsmekanismen (artiklarna 42.7, 43.5, 58.2 h).

4 GODKÄNNANDE AV CERTIFIERINGSKRITERIER

30. Certifieringskriterierna utgör en integrerad del av alla certifieringsmekanismer. Därför krävs det i dataskyddsförordningen att den behöriga tillsynsmyndigheten godkänner certifieringskriterierna i en certifieringsmekanism (artiklarna 42.5 och 43.2 b). När det gäller ett europeiskt sigill för dataskydd, godkänns certifieringskriterierna däremot av Europeiska dataskyddsstyrelsen (artiklarna 42.5 och 70.1 o). Båda möjligheterna till godkännande av certifieringskriterierna förklaras nedan.

31. Europeiska dataskyddsstyrelsen erkänner följande syften med godkännandet av certifieringskriterier:

    - Att korrekt återspegla de krav och principer för skydd av fysiska personer fastställda i förordning (EU) 2016/679 som gäller för behandling av personuppgifter.
    - Att bidra till en konsekvent tillämpning av dataskyddsförordningen.

32. Ett godkännande medges på grundval av dataskyddsförordningens krav som innebär att personuppgiftsansvariga och personuppgiftsbiträden ska kunna påvisa att certifieringsmekanismen överensstämmer med dataskyddsförordningen. Detta måste till fullo återspeglas i certifieringskriterierna.

4.1 Den behöriga tillsynsmyndighetens godkännande av kriterier

33. Certifieringskriterierna måste godkännas av den behöriga tillsynsmyndigheten före eller under förfarandet för ackreditering av ett certifieringsorgan. Också för uppdaterade eller kompletterande system eller kriterier i enlighet med ISO 17065 avseende samma

certifieringsorgan krävs ett godkännande innan de ändrade certifieringsmekanismerna kan användas (artiklarna 42.5 och 43.2 b). Tillsynsmyndigheterna ska behandla alla ansökningar om godkännande av certifieringskriterier på ett rättvist och icke-diskriminerande sätt i enlighet med ett offentligt tillgängligt förfarande, som innehåller de allmänna villkor som ska uppfyllas och en beskrivning av godkännandeförfarandet.

34. Ett certifieringsorgan kan endast utfärda certifieringar i en viss medlemsstat i enlighet med de kriterier som godkänts av tillsynsmyndigheten i den medlemsstaten. Med andra ord måste certifieringskriterierna godkännas av den behöriga tillsynsmyndigheten i det land där certifieringsorganet avser att erbjuda certifiering och får sin ackreditering. Se avsnittet nedan för europeiska certifieringssystem.

4.2 Europeiska dataskyddsstyrelsens godkännandekriterier för det europeiska sigillet för dataskydd

35. Ett certifieringsorgan kan också utfärda certifiering i enlighet med kriterier för ett europeiskt sigill för dataskydd som godkänts av Europeiska dataskyddstyrelsen. Certifieringskriterier som godkänts av Europeiska dataskyddsstyrelsen enligt artikel 63 kan leda till ett europeiskt sigill för dataskydd (artikel 42.5). Mot bakgrund av befintliga certifierings- och ackrediteringskonventioner bekräftar styrelsen att det är önskvärt att undvika fragmentering av marknaden för dataskyddscertifiering. Styrelsen noterar att medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen i enlighet med artikel 42.1 ska uppmuntra införandet av certifieringsmekanismer, särskilt på unionsnivå.

4.2.1 Ansökan om godkännande

36. Ansökan till styrelsen om godkännande av kriterier i enlighet med artiklarna 42.5 och 70.1 o måste göras genom en behörig tillsynsmyndighet. I ansökan bör ägaren av systemet, kandidaten eller det ackrediterade certifieringsorganet uttrycka sin avsikt att erbjuda kriterierna inom ramen för en certifieringsmekanism som riktar sig till personuppgiftsansvariga och personuppgiftsbiträden i alla medlemsstater. Den behöriga tillsynsmyndigheten kommer att lämna ett utkast till Europeiska dataskyddsstyrelsen när den anser att kriterierna kan godkännas av styrelsen.

37. Var man ska lämna in en ansökan om godkännande av kriterier beror på var ägaren av certifieringssystemet eller certifieringsorganet har sitt huvudkontor.

38. Om ett certifieringsorgan lämnar in en ansökan, är det vanligtvis på väg att i sin medlemsstat ansöka om ackreditering eller har redan ackrediterats av antingen den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet. Om certifieringsorganet redan är ackrediterat för en certifieringsmekanism i enlighet med dataskyddsförordningen kan detta bidra till en effektivisering av godkännandeförfarandet.

4.2.2 Kriterier för det europeiska sigillet för dataskydd

39. Styrelsen kommer att samordna bedömningsprocessen och vid behov godkänna kriterierna för det europeiska sigillet för dataskydd. Bedömningen kommer att inriktas på områden som t.ex. kriteriernas tillämpningsområde och deras tillämplighet för en gemensam certifiering. När kriterierna har godkänts av styrelsen förväntas tillsynsmyndigheten med ansvar för certifieringsorganets huvudkontor inom EU handlägga klagomål om själva mekanismen och informera övriga tillsynsmyndigheter. Denna tillsynsmyndighet är också behörig att vidta åtgärder mot certifieringsorganet. I tillämpliga fall kommer tillsynsmyndigheten att meddela övriga tillsynsmyndigheter och Europeiska dataskyddsstyrelsen.

40. Certifieringskriterierna för en gemensam certifiering är föremål för EU-omfattande krav och bör därför inbegripa en särskild mekanism för hantering av dessa krav. Europeiska certifieringsmekanismer måste vara avsedda att användas i alla medlemsstater. På grundval av artikel 42.5 måste mekanismen för ett europeiskt sigill för dataskydd och dess kriterier kunna anpassas på ett sätt som i tillämpliga fall tar hänsyn till nationella, sektorsspecifika bestämmelser, t.ex. i fråga om databehandling i skolorna, och avse en EU-omfattande tillämpning.

41. Exempel: En internationell skola som erbjuder registrerade inom EU utbildning är baserad i medlemsstat A. Skolan vill certifiera sin webbansökningsprocess med hjälp av ett EU-omfattande certifieringssystem för att erhålla ett europeiskt sigill för dataskydd. Därför avser den att ansöka om certifiering av behandlingsåtgärder erbjudna av ett certifieringsorgan etablerat i medlemsstat B på grundval av ett europeiskt sigill för dataskydd. Kriterierna för sigill som utformats och dokumenterats inom ramen för den relevanta mekanismen måste kunna ta hänsyn till skollagstiftning som är tillämplig i medlemsstat A. Kriterierna bör också innehålla krav på att skolans onlineansökningsprocess tillhandahåller information och uppfyller medlemsstaternas tillämpliga krav på skydd av personuppgifter, vilka kan skilja sig åt från dem i andra medlemsstater. Exempel på detta är personuppgifter som ska lämnas i en ansökan, t.ex. förskolebetyg eller testresultat, olika lagringsperioder, insamling eller behandling av finansiella eller biometriska uppgifter eller andra begränsningar i behandlingen.

    - Allmänna kriterier för godkännande av en mekanism för ett europeiskt sigill för dataskydd omfattar följande:
        - Kriterier som godkänts av styrelsen.
        - Ansökningar i olika behörighetsområden som i tillämpliga fall återspeglar nationella rättsliga krav och sektorsspecifik lagstiftning.
        -
    - Harmoniserade kriterier som kan anpassas så att de återspeglar nationella krav.
        - Beskrivningar av certifieringsmekanismen som specificerar:
        - certifieringsavtalen, med hänsyn till EU-omfattande krav,
        - förfaranden för att säkerställa och tillhandahålla lösningar för nationella variationer och säkerställa att sigillet bidrar till att påvisa efterlevnad av dataskyddsförordningen, och

- språket i rapporterna som riktar sig till alla påverkade tillsynsmyndigheter.

42. Även bilagan innehåller råd om kriterier för det europeiska sigillet för dataskydd.

4.2.3 Ackrediteringens roll

43. Som noterades i 4.2.1 kan certifieringsorgan, när kriterier identifierats som lämpliga för gemensam certifiering och har godkänts av styrelsen i enlighet med artikel 42.5, ackrediteras till att utföra certifiering i enlighet med dessa kriterier på unionsnivå.

44. System som endast är avsedda att erbjudas i vissa medlemsstater kommer inte att kunna tilldelas ett EU-sigill. Ackreditering för ett europeiskt sigill för dataskydd som gäller hela tillämpningsområdet kommer att kräva ackreditering i den medlemsstat som hyser huvudkontoret för certifieringsorganet med ansvar för att tillämpa systemet, dvs. som är ansvarigt för att utfärda certifiering och hantera certifieringsaktiviteterna för sina enheter och dotterbolag i andra medlemsstater. Om andra inrättningar eller kontor hanterar och genomför certifiering på egen hand, kommer var och en av dessa inrättningar eller kontor att behöva separat ackreditering i den medlemsstat där de är baserade. Med andra ord krävs ackreditering enbart i den medlemsstat där certifieringsorganet har sitt huvudkontor när endast huvudkontoret utfärdar certifiering. Om andra inrättningar inom certifieringsorganet däremot också utfärdar certifiering, behöver dessa inrättningar också ackrediteras.

45. Om ett certifieringsorgan inte har ackrediterats för certifiering i enlighet med det europeiska sigillet för dataskydd, kan Europeiska dataskyddsstyrelsens godkända kriterier följaktligen inte användas och sigillet kan inte erbjudas.

5 UTVECKLINGEN AV CERTIFIERINGSKRITERIER

46. I dataskyddsförordningen anges ramverket för utvecklingen av certifieringskriterier. Grundläggande krav för certifieringsförfarandet fastställs i artiklarna 42 och 43, och de artiklarna innehåller också viktiga kriterier för detta förfarande. Grunden för certifieringskriterierna måste dock härledas från principerna och reglerna i dataskyddsförordningen och bidra till att säkerställa att dessa principer och regler uppfylls.

47. Utvecklingen av certifieringskriterierna bör inriktas på kriteriernas verifierbarhet, betydelse och lämplighet för att påvisa efterlevnad av förordningen. Certifieringskriterierna bör formuleras på ett sådant sätt att de är tydliga och lättförståeliga och att de tillåter praktisk tillämpning.

48. Vid utarbetandet av certifieringskriterier ska bl.a. följande aspekter av efterlevnad i samband med bedömningen av behandlingsåtgärder i tillämpliga fall beaktas:

- Behandlingens laglighet i enlighet med artikel 6.

- Principerna för behandling i enlighet med artikel 5.
- De registrerades rättigheter i enlighet med artiklarna 12–23.
- Skyldigheten att meddela om dataskyddsincidenter i enlighet med artikel 33.
- Skyldigheten avseende inbyggt dataskydd och dataskydd som standard, i enlighet med artikel 25.
- Om en konsekvensbedömning avseende dataskydd i enlighet med artikel 35.7 d har utförts i tillämpliga fall.
- De tekniska och organisatoriska åtgärder som vidtagits i enlighet med artikel 32.

49. Beroende på certifieringens tillämpningsområde kan det variera i vilken utsträckning som dessa övervägande återspeglas i kriterierna. Tillämpningsområdet kan omfatta typen av behandlingsåtgärd och området som ska certifieras (t.ex. hälso- och sjukvårdssektorn).

5.1 Vad kan certifieras enligt dataskyddsförordningen?

50. Styrelsen anser att dataskyddsförordningen erbjuder ett omfattande utrymme åt vad som kan certifieras enligt dataskyddsförordningen, så länge som tyngdpunkten ligger på att påvisa att de behandlingsåtgärder som utförts av personuppgiftsansvariga och personuppgiftsbiträden är förenliga med denna förordning (artikel 42.1).

51. Vid bedömningen av en behandlingsåtgärd ska följande tre huvudbeståndsdelar i tillämpliga fall beaktas:

    1. Personuppgifter (dataskyddsförordningens materiella tillämpningsområde).
    2. Tekniska system – den infrastruktur (hårdvara och programvara) som används för att behandla personuppgifterna.
    3. Processer och förfaranden som är anknutna till behandlingsåtgärden.

52. Varje komponent som används i samband med behandlingsåtgärder måste bedömas enligt de fastställda kriterierna. Minst fyra olika viktiga faktorer kan ha betydelse: 1) Den personuppgiftsansvarigas eller personuppgiftsbiträdets organisation och rättsliga struktur. 2) Den avdelning och miljö samt de personer som är inblandade i behandlingsåtgärderna. 3) Den tekniska beskrivningen av de delar som ska bedömas. 4) Den IT-infrastruktur som understödjer behandlingen, till exempel operativsystem, virtuella system, databaser, autentiserings- och auktoriseringssystem, routrar och brandväggar, lagringssystem, kommunikationsinfrastruktur eller internetåtkomst och tillhörande tekniska åtgärder.

53. Alla tre huvudbeståndsdelar är relevanta för utformningen av certifieringsförfaranden och -kriterier. Beroende på certifieringsobjektet kan den utsträckning i vilken hänsyn tas till dem variera. I vissa fall kan man till exempel bortse från vissa beståndsdelar om de inte anses relevanta för certifieringsobjektet.

54. För att ytterligare specificera vad som kan certifieras i enlighet med dataskyddsförordningen innehåller dataskyddsförordningen ytterligare riktlinjer. Det följer av artikel 42.7 att certifiering enligt dataskyddsförordningen endast utfärdas till personuppgiftsansvariga och personuppgiftsbiträden, vilket innebär att t.ex. dataskyddsombud inte kan certifieras. Artikel 43.1 b hänvisar till ISO 17065 som handlar om ackreditering av certifieringsorgan som utvärderar överensstämmelse för produkter, tjänster och förfaranden. En behandlingsåtgärd, eller ett antal behandlingsåtgärder, kan leda till en produkt eller en tjänst i enlighet med terminologin i ISO 17065 och sådana kan vara föremål för certifiering. Exempelvis är behandlingen av anställdas personuppgifter för löneutbetalningar eller ledighetsförvaltning en serie åtgärder i den mening som avses i dataskyddsförordningen och kan leda till en produkt, ett förfarande eller en tjänst i enlighet med den terminologi som används i ISO.

55. På grundval av dessa överväganden anser styrelsen att tillämpningsområdet för certifiering enligt dataskyddsförordningen är inriktat på behandlingsåtgärder eller serier av åtgärder. Dessa kan bestå av styrprocesser i bemärkelsen organisatoriska åtgärder, som alltså är integrerade delar av en behandlingsåtgärd (t.ex. den styrprocess som fastställts för klagomålshantering under behandlingen av anställdas uppgifter för löneutbetalning).

56. För att bedöma huruvida behandlingsåtgärden uppfyller certifieringskriterierna måste ett användningsfall tillhandahållas. Huruvida användningen av en teknisk infrastruktur som utnyttjas under en behandlingsåtgärd uppfyller kriterierna, beror till exempel på de uppgiftskategorier som denna är utformad för att behandla. Organisatoriska åtgärder beror på vilka kategorier och datamängder samt vilken teknisk infrastruktur som används för behandling, med beaktande av behandlingens art, dess tillämpningsområde, innehåll och syfte samt riskerna för de registrerades rättigheter och friheter.

57. Dessutom kan it-applikationer skilja sig mycket åt även om de uppfyller samma behandlingsändamål. Detta måste därför beaktas när man definierar tillämpningsområdet för certifieringsmekanismerna och utarbetar certifieringskriterierna. Certifieringens och kriteriernas omfattning bör inte begränsas så mycket att it-applikationer som utformas på ett annorlunda sätt inte omfattas.

5.2 Bestämma certifieringsobjekt

58. Tillämpningsområdet för en certifieringsmekanism ska särskiljas från objektet – även kallat evalueringsobjektet – i samband med enskilda certifieringsprojekt inom ramen för en certifieringsmekanism. En certifieringsmekanism kan definiera sitt tillämpningsområde antingen generellt eller i förhållande till en viss typ eller visst område av behandlingsåtgärder och kan därför redan identifiera de certifieringsobjekt som omfattas av certifieringsmekanismen (t.ex. säker lagring och skydd av personuppgifter i ett digitalt valv). En tillförlitlig och meningsfull bedömning av efterlevnaden kan endast göras om det enskilda objektet för ett certifieringsprojekt beskrivs exakt. Först ska det tydligt anges vilka behandlingsåtgärder som ingår i certifieringsobjektet och sedan vilka huvudbeståndsdelar, dvs. vilka uppgifter, processer och tekniska infrastrukturer som ska bedömas och vilka som inte ska bedömas. I samband med detta måste gränssnitten till andra processer alltid beaktas och beskrivas. Det är uppenbart att okända företeelser inte kan ingå i bedömningen och därför inte kan certifieras. Det enskilda certifieringsobjektet måste i alla händelser vara meningsfullt

med hänsyn till det budskap eller påstående som görs på/av certifieringen och får inte vilseleda användaren, kunden eller konsumenten.

59. [Exempel 1]

En bank erbjuder sina kunder en webbplats för banktjänster. Inom ramen för denna tjänst finns möjlighet att göra överföringar, köpa aktier, inleda stående betalningsorder och hantera konton. Banken vill certifiera denna enligt en certifieringsmekanism för uppgiftsskydd med ett allmänt tillämpningsområde baserat på allmänna kriterier.

a) Säker inloggning

Säker inloggning är en behandlingsåtgärd som är begriplig för slutanvändaren, och relevant från ett dataskyddsperspektiv, eftersom den utgör en viktig del i att garantera säkerhet för de personuppgifter som berörs. Denna behandlingsåtgärd är därför nödvändig för en säker inloggning och kan alltså utgöra ett meningsfullt evalueringsobjekt, om det tydligt fastställs i certifieringen att enbart inloggningsprocessen är certifierad.

b) Webbgränssnitt

Webbgränssnittet kan vara relevant ur ett dataskyddsperspektiv, men det är inte begriplig för slutanvändaren och kan därför inte vara ett meningsfullt evalueringsobjekt. Dessutom är det oklart för användaren vilka tjänster på webbplatsen och därmed vilka behandlingsåtgärder som omfattas av certifieringen.

c) Nätbaserade banktjänster

Webbgränssnittet tillsammans med det inre systemet är behandlingsåtgärder som tillhandahålls i den nätbaserade banktjänsten och som kan vara meningsfulla för användaren. I detta sammanhang måste de båda ingå i evalueringsobjektet. Däremot kan behandlingsåtgärder som inte är direkt kopplade till tillhandahållandet av nätbaserade banktjänster, till exempel behandlingsåtgärder i syfte att förhindra penningtvätt, utelämnas från evalueringsobjekt.

De nätbaserade banktjänster som banken erbjuder på sin webbplats kan även omfatta andra tjänster som i sin tur kräver egna behandlingsåtgärder. I detta sammanhang kan andra tjänster till exempel omfatta erbjudanden om försäkringsprodukter. Eftersom denna tilläggstjänst inte är direkt kopplad till syftet att tillhandahålla nätbaserade banktjänster, kan den utelämnas från evalueringsobjekt. Om denna tilläggstjänst (försäkringen) utelämnas från evalueringsobjektet, är de av tjänstens gränssnitt som är integrerade på webbplatsen en del av evalueringsobjektet och måste därför beskrivas för att etablera en tydlig åtskillnad mellan tjänsterna. En sådan beskrivning är nödvändig för att identifiera och utvärdera möjliga dataflöden mellan de två tjänsterna.

60. [Exempel 2]

En bank erbjuder sina kunder en tjänst som gör det möjligt att samla information om olika konton och kreditkort från flera banker (kontoaggregering). Banken vill få sina tjänster certifierade enligt dataskyddsförordningen. Den behöriga tillsynsmyndigheten har godkänt en

viss uppsättning certifieringskriterier med inriktning på denna typ av verksamhet. Certifieringsmekanismens tillämpningsområde omfattar endast följande efterlevnadsaspekter:

- Användarautentisering.
- Godkända sätt att få uppgifterna aggregerade från andra banker/tjänster.

Eftersom tillämpningsområdet för denna certifieringsmekanism i sig definierar evalueringsobjektet, är det inte möjligt att på ett meningsfullt sätt begränsa evalueringsobjektet till det föreslagna tillämpningsområdet och endas certifiera särskilda egenskaper eller en enda behandlingsaktivitet. I detta scenario måste ett evalueringsobjekt vara likställt med ett specifikt tillämpningsområde.

5.3 Utvärderingsmetoder och bedömningsgrund

61. Utvärderingsmetoderna och bedömningsgrunden måste identifieras och fastställas om en bedömning av överensstämmelse som bidrar till att påvisa behandlingsåtgärdernas efterlevnad ska utföras. Det gör skillnad om bedömningsinformationen endast hämtas från dokumentation (vilket inte skulle vara tillräckligt i sig) eller om den aktivt samlas in på plats och genom direkt eller indirekt åtkomst. Sättet på vilket information samlas in får konsekvenser för certifieringens betydelse och bör därför definieras och beskrivas.

    Förfaranden för utfärdande och periodisk översyn av certifieringen bör innehålla specifikationer för att fastställa den utvärderingsnivå (omfattning och detaljrikedom) som krävs för att uppfylla certifieringskriterierna, och bör inbegripa tillhandahållandet av följande:

    - Information om och specifikation av de bedömningsmetoder som tillämpats och de resultat som framkommit, t.ex. under granskning på plats eller från dokumentation.
    - Vilka utvärderingsmetoder som används på behandlingsåtgärderna (uppgifter, system, processer) samt syftet med behandlingen.
    - Identifiering av uppgiftskategorier och skyddsbehov samt huruvida personuppgiftsbiträden eller tredje parter är iblandade.
    - Identifiering av roller och förekomsten av en mekanism för åtkomstkontroll som definieras utifrån roller och ansvar.

62. Utvärderingens omfattning påverkar certifieringens betydelse och värde. Om utvärderingens omfattning minskas av pragmatiska skäl eller för att minimera kostnaderna förminskar man betydelsen av en dataskyddscertifiering. Samtidigt kan beslut med utgångspunkt i utvärderingens detaljrikedom överstiga inte bara den sökandes finansiella kapacitet utan också utvärderarnas och granskarnas förmåga. Det kanske inte alltid är nödvändigt att genomföra en väldigt detaljrik analys av de IT-system som används för att påvisa efterlevnad.

5.4 Bedömningsdokumentation

63. Certifieringsdokumentationen bör vara grundlig och omfattande. Brister i dokumentationen innebär att en korrekt bedömning inte kan genomföras. Certifieringsdokumentation är

nödvändig eftersom den ger insyn i utvärderingsprocessen inom ramen för certifieringsmekanismen. Dokumentationen ger svar på frågor vad gäller de lagliga kraven. Certifieringsmekanismerna bör innehålla en standardiserad dokumentationsmetod. Sedan kommer man genom utvärderingen att kunna jämföra certifieringsdokumentationen med det faktiska förhållandet på plats och jämfört med certifieringskriterierna.

64. Omfattande dokumentation om vad som har certifierats och den tillämpade metoden främjar insynen. Enligt artikel 43.2 c ska certifieringsmekanismer omfatta förfaranden som tillåter granskning av certifieringar. Detaljerad dokumentation kan vara det lämpligaste sättet att kommunicera för att möjliggöra tillsynsmyndighetens bedömning av om och i vilken omfattning certifieringen kan bekräftas i formella utredningar. Den dokumentation som sammanställs under utvärderingen bör därför inriktas på följande tre huvudaspekter:

    - Konsekvens och samstämmighet mellan de utvärderingsmetoder som används.
    - Utvärderingsmetoder inriktade på att påvisa att certifieringsobjektet följer certifieringskriterierna och därmed också dataskyddsförordningen.
    - Att utvärderingens resultat har validerats av ett oberoende och opartiskt certifieringsorgan.

5.5 Dokumentation av resultaten

65. I skäl 100 anges information om de mål som eftersträvas genom införandet av certifiering.

”För att förbättra öppenheten och efterlevnaden av denna förordning bör införandet av certifieringsmekanismer och dataskyddsförsegling och dataskyddsmärkning uppmuntras, så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd.”

66. Dokumentationen och rapporteringen av resultat spelar en viktig roll för att öka insynen. Certifieringsorgan som använder certifieringsmekanismer, sigill eller märkning som riktar sig till de registrerade (i deras roll som konsumenter eller kunder) bör tillhandahålla lättillgänglig, förståelig och meningsfull information om de certifierade behandlingsåtgärderna. Den offentliga informationen ska minst omfatta följande:

    - En beskrivning av evalueringsobjekten.
    - Hänvisning till de godkända kriterier som tillämpas på det specifika evalueringsobjektet.
    - Metoder för utvärdering av kriterierna (utvärdering på plats, dokumentation osv.)
    - Certifieringens giltighetstid.
    - Det bör även säkerställas att resultaten är jämförbara för tillsynsmyndigheter och allmänheten.

6 RIKTLINJER FÖR FASTSTÄLLANDE AV CERTIFIERINGSKRITERIER

67. Certifieringskriterier utgör en integrerad del av en certifieringsmekanism. Certifieringsförfarandet omfattar krav på hur, genom vem, i vilken omfattning och med vilken detaljrikedom bedömningen ska ske vad gäller enskilda certifieringsprojekt som rör ett specifikt objekt eller evalueringsobjekt. Certifieringskriterierna innehåller de nominella krav mot vilka de faktiska behandlingsåtgärder som definieras i evalueringsobjektet bedöms. I dessa riktlinjer för fastställandet av certifieringskriterier ges allmänna råd som kommer att underlätta bedömningen av certifieringskriterier som behöver godkännas.

    - De allmänna övervägandena nedan bör beaktas när man godkänner eller definierar certifieringskriterier. Certifieringskriterierna bör uppfylla följande:
    - De bör vara enhetliga och kontrollerbara.
    - De bör kunna granskas för att underlätta utvärderingen av behandlingsåtgärder enligt dataskyddsförordningen, särskilt genom angivande av målen och de tillämpade riktlinjerna för att uppnå dessa mål.
    - De bör vara relevanta med avseende på den avsedda målgruppen (dvs. företag till företag och företag till kund).
    - När detta är tillämpligt bör de vara kompatibla med andra standarder (som t.ex. ISO-standarder eller standarder på nationell nivå).
    - De bör vara flexibla och skalbara för att kunna tillämpas på organisationer av olika typer och storlekar, inklusive mikro-, små och medelstora företag i enlighet med artikel 42.1 och den riskbaserade metoden i enlighet med skäl 77.

68. Ett litet lokalt företag, som en återförsäljare, utför vanligtvis mindre komplicerade behandlingsåtgärder än en stor multinationell återförsäljare. Även om kraven på lagenlighet för behandlingsåtgärderna är desamma, måste behandlingens tillämpningsområde och komplexitet beaktas. Därav följer att det finns ett behov för certifieringsmekanismer och att deras kriterier måste vara skalbara i enlighet vilken behandlingsverksamhet det gäller.

6.1 Befintliga standarder

69. Certifieringsorgan behöver överväga hur specifika kriterier tar hänsyn till befintliga relevanta instrument, som uppförandekoder, tekniska standarder eller nationella reglerande eller rättsliga initiativ. I bästa fall kommer kriterierna att vara kompatibla med befintliga standarder som kan bidra till att en personuppgiftsansvarig eller ett personuppgiftsbiträde kan uppfylla sina skyldigheter enligt dataskyddsförordningen. Medan branschstandarder ofta fokuserar på organisationens skydd och säkerhet, riktar dataskyddsförordningen dock in sig på skyddet av fysiska personers grundläggande rättigheter. Hänsyn måste tas till detta andra perspektiv när man utformar kriterier eller godkänner kriterier och certifieringsmekanismer som bygger på branschstandarder.

6.2 Definition av kriterier

70. Certifieringskriterier måste överensstämma med certifieringsförklaringen (meddelandet eller påståendet) för en certifieringsmekanism och uppfylla de förväntningar som förklaringen ger upphov till. Redan namnet på en certifieringsmekanism kan utpeka tillämpningsområdet och få konsekvenser för fastställandet av kriterier.

71. [Exempel 3]

    En mekanism som kallas HealthPrivacyMark bör begränsa sitt tillämpningsområde till hälso- och sjukvårdssektorn. Sigillets namn ger upphov till förväntningen att dataskyddskrav i samband med hälsouppgifter har granskats. Därför måste mekanismens kriterier vara adekvata för bedömningar av dataskyddskraven inom denna sektor.

72. [Exempel 4]

    För en mekanism som rör certifieringen av behandlingsåtgärder med styrsystem i samband med behandlingen av personuppgifter bör kriterier identifieras som möjliggör bekräftande och utvärdering av styrprocesser och tekniska och organisatoriska åtgärder som stödjer dessa.

73. [Exempel 5]

    Kriterierna för en mekanism som rör molntjänster behöver ta hänsyn till de särskilda tekniska krav som är nödvändiga för användningen av molnbaserade datortjänster. Om servrar till exempel används utanför EU, måste kriterierna ta hänsyn till de villkor som fastställs i kapitel V i dataskyddsförordningen vad gäller villkoren för överföring av personuppgifter till tredjeländer.

74. Kriterier som utformats för att passa olika evalueringsobjekt i olika sektorer och/eller medlemsstater bör uppfylla följande: kunna tillämpas på olika scenarier, möjliggöra identifiering av lämpliga åtgärder som passar i små, medelstora och stora behandlingsåtgärder samt återspegla riskerna av varierande sannolikhetsgrad och svårighet avseende fysiska personers rättigheter och friheter i enlighet med dataskyddsförordningen. Därför måste certifieringsprocessen (för t.ex. dokumentation, tester eller utvärderingsmetoder och omfattning) som kompletterar kriterierna uppfylla dessa behov och tillåta och fastställa regler för att t.ex. tillämpa de relevanta kriterierna på enskilda certifieringsprojekt. Kriterierna måste underlätta en bedömning av om tillräckliga garantier för tillämpningen av lämpliga tekniska och organisatoriska åtgärder har tillhandahållits.

6.3 Certifieringskriteriernas livslängd

75. Även om certifieringskriterierna måste vara tillförlitliga över tid bör de inte vara huggna i sten. De ska revideras exempelvis i följande fall:

    - Om den rättsliga ramen ändras.
    - Om villkor och bestämmelser tolkas genom domar från Europeiska unionens domstol.
    - Om den tekniska nivån har utvecklats.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)

BILAGA 1: TILLSYNSMYNDIGHETERNAS UPPGIFTER OCH BEFOGENHETER I SAMBAND MED CERTIFIERING I ENLIGHET MED DATASKYDDSFÖRORDNINGEN

	Bestämmelser	Krav
Uppgifter	Artikel 43.6	Tillsynsmyndigheten ska offentliggöra de kriterier som avses i artikel 42.5 i ett lättillgängligt format och översända dem till styrelsen.
	Artikel 57.1 n	Tillsynsmyndigheten ska godkänna certifieringskriterier i enlighet med artikel 42.5.
	Artikel 57.1 o	I tillämpliga fall (dvs. när den utfärdar certifiering) ska tillsynsmyndigheten genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7.
	Artikel 64.1 c	Tillsynsmyndigheten ska skicka utkastet till beslut till styrelsen när det syftar till att godkänna de kriterier för certifiering som avses i artikel 42.5.
Befogenheter	Artikel 58.1 c	Tillsynsmyndigheten har befogenhet att utföra översyn av certifiering som utfärdats i enlighet med artikel 42.7.
	Artikel 58.2 h	Tillsynsmyndigheten har befogenhet att återkalla eller beordra certifieringsorganet att återkalla en certifiering eller beordra certifieringsorganet att inte utfärda certifiering.
	Artikel 58.3 e	Tillsynsmyndigheten har befogenhet att ackreditera certifieringsorgan.
	Artikel 58.3 f	Tillsynsmyndigheten har befogenhet att utfärda certifieringar och godkänna kriterier för certifiering.
	Artikel 58.3 e	Tillsynsmyndigheten har befogenhet att ackreditera certifieringsorgan.
	Artikel 58.3 f	Tillsynsmyndigheten har befogenhet att utfärda certifieringar och godkänna kriterier för certifiering.

BILAGA 2

1 INLEDNING

Bilaga 2 innehåller vägledning för granskning och utvärdering av certifieringskriterier enligt artikel 42.5. Bilagan identifierar frågor som en dataskyddstillsynsmyndighet och Europeiska dataskyddsstyrelsen överväger och tillämpar när de ska godkänna certifieringskriterierna för en certifieringsmekanism. Frågorna bör behandlas av certifieringsorgan och systemägare som vill utarbeta kriterier och lämna in dem för godkännande. Förteckningen är inte uttömmande, men innehåller de minimikrav som ska beaktas. Alla frågor kommer inte att vara tillämpliga. De bör dock beaktas när kriterier utarbetas, och en förklaring om varför kriterier inte omfattar vissa områden kan behövas. Vissa frågor upprepas eftersom de ställs utifrån olika perspektiv. Dessa riktlinjer bör beaktas i enlighet med de rättsliga kraven i dataskyddsförordningen och, i tillämpliga fall, i nationell lagstiftning.

2 CERTIFIERINGSMEKANISMENS TILLÄMPNINGSOMRÅDE OCH EVALUERINGSOBJEKT

a. Är certifieringsmekanismens tillämpningsområde (som dataskyddskriterierna ska tillämpas på) tydligt beskrivet?

b. Är certifieringsmekanismens tillämpningsområde relevant för sin målgrupp? Kan det ses som missvisande?

- *Exempel: Ett ”Trusted Company Seal” antyder att ett helt företags behandlingsverksamhet har granskats, även om endast specifika behandlingsåtgärder, dvs. betalningsförfarandet online, är föremål för certifiering. Tillämpningsområdet är därför missvisande.*

c. Återspeglar certifieringsmekanismens tillämpningsområde alla relevanta aspekter av behandlingsåtgärderna?

- *Exempel: Ett ”Privacy Health Mark” måste omfatta alla utvärderingsuppgifter som rör hälsa för att kunna uppfylla kraven i artikel 9.*

d. Möjliggör certifieringsmekanismens tillämpningsområde en meningsfull dataskyddscertifiering som tar de berörda behandlingsåtgärdernas natur, innehåll och risk i åtanke?

- *Exempel: Om certifieringsmekanismens tillämpningsområde enbart är inriktat på specifika aspekter av behandlingsåtgärderna, som insamling av uppgifter, men inte på ytterligare behandlingsåtgärder, som t.ex. behandling för att skapa reklamprofiler eller hantering av den registrerades rättigheter, är det inte meningsfullt för registrerade.*

e. Omfattar certifieringsmekanismens tillämpningsområde behandling av personuppgifter i det relevanta ansökningslandet, eller omfattar det behandling eller överföring över gränserna?

f. Beskriver certifieringskriterierna tillräckligt väl hur evalueringsobjektet borde definieras?

- *Exempel: Ett integritetmärke som erbjuder ett allmänt tillämpningsområde och som enbart kräver ”en specificering av den behandling som är föremål för certifiering” ger inte tillräcklig vägledning om hur man fastställer och beskriver ett evalueringsobjekt.*
- *Exempel: Ett specifikt tillämpningsområde, t.ex. ”Privacy Vault Seal”, som rör säker lagring bör i sina kriterier tydligt beskriva vad som krävs för att uppfylla kraven på detta*

tillämpningsområde, t.ex. en definition av ”vault”, systemkrav och obligatoriska tekniska och organisatoriska åtgärder. I detta fall kan tillämpningsområdet i sig innebära en tydlig definition av evalueringsobjektet.

(1) Krävs det enligt kriterierna att evalueringsobjektet identifierar alla relevanta behandlingsåtgärder, innehåller en illustration av dataflöden och fastställer var evalueringsobjektet ska tillämpas?

- *Exempel: En certifieringsmekanism erbjuder certifiering av personuppgiftsansvarigas behandlingsåtgärder enligt dataskyddsförordningen utan närmare definition av tillämpningsområdet. De kriterier som tillämpas av mekanismen innehåller krav på att den sökande personuppgiftsansvariga fastställer den berörda behandlingsåtgärden (evalueringsobjektet) vad gäller använda datatyper, system och processer.*

(2) Krävs det enligt kriterierna att de sökande klargör var den behandling som är föremål för utvärdering ska börja och sluta? Krävs det enligt kriterierna att evalueringsobjektet ska inkludera gränssnitt där behandlingsåtgärder som är inbördes beroende av varandra inte ingår i evalueringsobjektet? Är detta tillfredsställande motiverat?

- *Exempel: Ett evalueringsobjekt som i tillräcklig detalj beskriver behandlingsåtgärderna för en webbaserad tjänst, dvs. genom att t.ex. omfatta registrering av användare, tillhandahållande av tjänster, fakturering, loggning av IP-adresser, gränssnitt mot användare och tredje parter och undanta serverhotelltjänster (men omfatta avtal om behandling och tekniska och organisatoriska åtgärder).*

g. Säkerställer kriterierna att det (enskilda) evalueringsobjektet är begriplig för sin publik, inbegripet registrerade där detta är relevant?

3 ALLMÄNNA KRAV

a. Har alla termer som används i kriterieförteckningen (dvs. hela listan över kriterier) identifierats, förklarats och beskrivits?

b. Har alla normativa hänvisningar identifierats?

c. Omfattar kriterierna definitionen av de dataskyddsansvar, förfaranden och behandlingsåtgärder som ingår i certifieringsmekanismens tillämpningsområde?

4 BEHANDLINGSÅTGÄRDER, ARTIKEL 42.1

Hanteras i kriterierna alla relevanta delar av behandlingsåtgärderna (uppgifter, system och processer) för certifieringsmekanismens tillämpningsområde (allmänt eller specifikt)?

a. Krävs det enligt kriterierna att den giltiga rättsliga grunden för behandling fastställs för evalueringsobjektet?

b. Erkänns i kriterierna de relevanta behandlingsfaserna och uppgifternas hela livscykel för evalueringsobjektet, inklusive radering eller anonymisering?

c. Krävs det dataportabilitet enligt kriterierna för evalueringsobjektet?

d. Krävs det enligt kriterierna för evalueringsobjektet en möjlighet att identifiera och visa upp särskilda typer av behandlingsåtgärder, t.ex. automatiserat beslutsfattande och profilering?

e. Krävs det enligt kriterierna för evalueringsobjektet en möjlighet att identifiera särskilda uppgiftskategorier?

f. Tillåts och krävs det enligt kriterierna en bedömning av individuella behandlingsåtgärder och skyddsbehovet för de registrerades rättigheter och friheter?

g. Tillåts och krävs det enligt kriterierna tillräcklig hänsyn till risken för de registrerades rättigheter och friheter?

…

5 LAGLIG BEHANDLING AV PERSONUPPGIFTER

a. Krävs det enligt kriterierna en kontroll av hur lagliga enskilda behandlingsåtgärder är i fråga om behandlingens syfte och nödvändighet?

b. Krävs det enligt kriterierna en kontroll av alla krav om en rättslig grund för individuella behandlingsåtgärder?

6 PRINCIPER, ARTIKEL 5

a. Hanteras alla principer för uppgiftsskydd enligt artikel 5 på ett korrekt sätt i kriterierna?

b. Krävs det enligt kriterierna att det individuella evalueringsobjektet ska påvisa uppgiftsminimering?

…

7 ALLMÄNNA SKYLDIGHETER FÖR PERSONUPPGIFTSANSVARIGA OCH -BITRÄDEN

a. Krävs det enligt kriterierna bevis på ett avtal mellan personuppgiftsansvariga och personuppgiftsbiträden?

b. Utvärderas avtalen mellan personuppgiftsansvariga och personuppgiftsbiträden?

c. Framgår den personuppgiftsansvarigas skyldigheter i enlighet med kapitel IV av kriterierna?

d. Krävs det enligt kriterierna bevis för granskning och uppdatering av tekniska och organisatoriska åtgärder som tillämpats av personuppgiftsansvariga i enlighet med artikel 24.1?

e. Kontrolleras det enligt kriterierna om organisationen har bedömt huruvida ett dataskyddsombud bör tillsättas i enlighet med artikel 37? Uppfyller dataskyddsombudet i tillämpliga fall kraven i artiklarna 37–39?

f. Kontrolleras det enligt kriterierna om ett register över behandlingen krävs i enlighet med artikel 30.5 och hanteras kraven i artikel 30 på lämpligt vis?

8 DE REGISTRERADES RÄTTIGHETER

a. Hanteras i tillräcklig utsträckning den registrerades rätt till information i kriterierna och fastställs krav i dem om att respektive åtgärder ska vidtas?

b. Krävs det enligt kriterierna att de registrerade beviljas tillräcklig eller t.o.m. ytterligare åtkomst till och kontroll över sina uppgifter, inbegripet dataportabilitet?

c. Krävs det enligt kriterierna åtgärder som gör det möjligt att ingripa i behandlingsåtgärden för att säkerställa de registrerades rättigheter och tillåta rättelser, radering eller begränsningar?

…

9 RISK FÖR FYSISKA PERSONERS RÄTTIGHETER OCH FRIHETER

a. Tillåts och krävs det enligt kriterierna en bedömning av risken för de registrerades rättigheter och friheter?

b. Anges eller krävs det enligt kriterierna en erkänd metod för riskbedömning? Är den i så fall proportionerlig?

c. Tillåts och krävs det enligt kriterierna en konsekvensbedömning av de tilltänkta behandlingsåtgärderna avseende fysiska personers rättigheter och friheter?

d. Krävs det enligt kriterierna förhandssamråd om de kvarvarande risker som inte kunde minskas med utgångspunkt i konsekvensbedömningens resultat?

10 TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER SOM GARANTERAR SKYDD

a. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder som främjar behandlingsåtgärdernas konfidentialitet?

b. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder som främjar behandlingsåtgärdernas integritet?

c. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder som främjar behandlingsåtgärdernas tillgänglighet?

d. Krävs det enligt kriterierna tillämpning av åtgärder som ger bättre insyn i behandlingsåtgärderna vad gäller följande:

e. Ansvarsskyldighet?

f. De registrerades rättigheter?

g. En utvärdering av individuella behandlingsåtgärder t.ex. i fråga om algoritmisk öppenhet?

h. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder som garanterar registrerades rättigheter, t.ex. möjligheten att tillhandahålla information eller dataportabilitet?

i. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder som gör det möjligt att ingripa i behandlingsåtgärden för att säkerställa de registrerades rättigheter och tillåta rättelser, radering eller begränsningar?

j. Krävs det enligt kriterierna tillämpning av åtgärder som gör det möjligt att ingripa i behandlingsåtgärden för att kunna uppdatera eller kontrollera systemet eller processen?

k. Krävs det enligt kriterierna tillämpning av tekniska och organisatoriska åtgärder för att säkerställa dataminimering, t.ex. genom att avlänka eller separera uppgifter från den registrerade, anonymisering eller pseudonymisering eller isolering av datasystem?

l. Krävs det enligt kriterierna tekniska åtgärder som tillämpar uppgiftsskydd som standard?

m. Krävs det enligt kriterierna tekniska och organisatoriska åtgärder för att införa inbyggt dataskydd, t.ex. ett hanteringssystem för dataskydd som ska visa, informera om, kontrollera och genomföra dataskyddskrav?

n. Krävs det enligt kriterierna tekniska och organisatoriska åtgärder för att tillhandahålla lämplig fortbildning och utbildning för den personal som har permanent eller regelbunden tillgång till personuppgifter?

o. Krävs det granskningsåtgärder enligt kriterierna?

p. Krävs det självutvärdering/intern granskning enligt kriterierna?

q. Krävs det enligt kriterierna åtgärder som säkerställer att rapporteringsplikten för personuppgiftsincidenter genomförs i god tid och rätt omfattning?

r. Krävs det enligt kriterierna att incidenthanteringsförfaranden är införda och verifierade?

s. Krävs det enligt kriterierna övervakning av framväxande integritets- och teknikfrågor och uppdatering av systemet efter behov?

…

11 ANDRA FUNKTIONER SOM FRÄMJAR DATASKYDD

a. Krävs det enligt kriterierna tillämpning av dataskyddsfrämjande teknik? Detta kan omfatta kriterier som fastställer krav på förstärkt dataskydd genom att eliminera eller minska antalet personuppgifter och/eller dataskyddsrisken.

- *Exempel: Kriterier som innehåller krav på ökad olänkbarhet genom användning av användarcentrerad identitetshantering som t.ex. attributbaserad behörighet istället för organisationscentrerad identitetshantering skulle återspegla en teknik för förbättrat dataskydd.*

b. Krävs det enligt kriterierna tillämpning av förbättrade styrmöjligheter för att underlätta självbestämmande och valfrihet för de registrerade?

…

12 KRITERIER SOM SKA VISA ATT DET FÖRELIGGER LÄMPLIGA GARANTIER FÖR ÖVERFÖRING AV PERSONUPPGIFTER

Kriterier kommer att tas upp i de kommande riktlinjerna för artikel 42.2.

13 YTTERLIGARE KRITERIER FÖR ETT EUROPEISKT SIGILL FÖR DATASKYDD

a. Är kriterierna tänkta att omfatta alla medlemsstater?

b. Tas det i kriterierna hänsyn till medlemsstaternas lagstiftning eller scenarion för dataskydd?

c. Krävs det enligt kriterierna en utvärdering av det individuella evalueringsobjektet avseende medlemsstaternas sektorspecifika dataskyddslagar?

d. Krävs det enligt kriterierna att den personuppgiftsansvariga eller personuppgiftsbiträdet ska förse registrerade och berörda parter med information på medlemsstaternas språk vad gäller följande:

e. Behandlingen/evalueringsobjektet?

f. Dokumentation av behandlingen/evalueringsobjektet?

g. Resultatet av utvärderingen?

…

14 ÖVERGRIPANDE UTVÄRDERING AV KRITERIER

a. Omfattar kriterierna till fullo certifieringsmekanismens tillämpningsområde (dvs. heltäckande kriterier) för att ge en garanti om att certifieringen är tillförlitlig?

- *Exempel: Om certifieringsmekanismens tillämpningsområde är inriktat på behandlingsåtgärder rörande hälsa, bör en hög dataskyddsnivå garanteras genom att man fastställer kriterier som säkerställer till exempel en ingående granskning och tillämpningen av inbyggt dataskydd och dataskydd som standard.*

b. Står kriterierna i proportion till omfattningen av de behandlingsåtgärder som omfattas av certifieringsmekanismens tillämpningsområde, informationens känslighet och behandlingens risk?

c. Är det sannolikt att kriterierna förbättrar personuppgiftsansvarigas och personuppgiftsbiträdens efterlevnad av dataskydd?

d. Kommer de registrerade att gynnas av sin rätt till information, t.ex. genom förklaringar om vilka resultat som önskas?