Retningslinjer 1/2018 vedrørende certificering og identifikation af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordningen

Udgave 3.0

4. juni 2019

Vedtaget

Versionshistorik

Udgave 3.0	4. juni 2019	Optagelse af bilag 2 (version 2,0 af bilag 2 vedtaget den 4. juni 2019 efter offentlig høring)
Udgave 2.1	9. april 2019	Vedtagelse af en berigtigelse til retningslinjerne (afsnit 45)
Udgave 2.0	23. januar 2019	Vedtagelse af retningslinjerne efter offentlig høring — Bilag 2 (version 1,0) blev samme dag vedtaget med henblik på offentlig høring
Udgave 1.0	25. maj 2018	Vedtagelse af retningslinjerne med henblik på offentlig høring

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ("databeskyttelsesforordningen"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018,

under henvisning til artikel 12 og 22 i Databeskyttelsesrådets forretningsorden af 25. maj 2018,

under hensyntagen til resultaterne af den offentlige høring om retningslinjerne, der fandt sted mellem den 30. maj 2018 og den 12. juli 2018, og den om bilag 2, som fandt sted mellem den 15. februar og den 29. marts 2019, jf. artikel 70, stk. 4, i databeskyttelsesforordningen —

VEDTAGET FØLGENDE RETNINGSLINJER

1 INDLEDNING

1. Den generelle forordning om databeskyttelse (forordning (EU) 2016/279, "databeskyttelsesforordningen" eller "forordningen") udgør en moderniseret ramme for ansvarlighed og overholdelse af de grundlæggende rettigheder i forbindelse med databeskyttelse i Europa. En række foranstaltninger, der fremmer overholdelse af databeskyttelsesforordningens bestemmelser er afgørende for denne nye ramme. De omfatter obligatoriske krav under specifikke omstændigheder (herunder udnævnelsen af databeskyttelsesrådgivere og udførelse af konsekvensanalyser vedrørende databeskyttelse) og frivillige foranstaltninger som f.eks. adfærdskodekser og certificeringsmekanismer.

2. Inden vedtagelsen af databeskyttelsesforordningen fastslog Artikel 29-Gruppen, at certificering kan udgøre en vigtig del af princippet om ansvarlighed i forbindelse med databeskyttelse[1]. For at certificering kan levere pålideligt bevis for overholdelse af databeskyttelsesreglerne, bør der være klare regler, der fastsætter krav til leveringen af sådan certificering[2]. Databeskyttelsesforordningens artikel 42 udgør retsgrundlaget for udviklingen af sådanne regler.

3. Databeskyttelsesforordningens artikel 42, stk. 1, lyder:

   "Medlemsstaterne, tilsynsmyndighederne, [Det Europæiske Databeskyttelsesråd] og Kommissionen tilskynder navnlig på EU-plan til fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder denne forordning.

[1] Artikel 29-Gruppens udtalelse 3/2010 om princippet om ansvarlighed (WP173), 13.7.2010, afsnit 69-71.
[2] Artikel 29-Gruppens udtalelse 3/2010 om princippet om ansvarlighed (WP173), afsnit 69.

Mikrovirksomheders og små og mellemstore virksomheders særlige behov tages i betragtning".

4. Certificeringsmekanismer[3] kan forbedre gennemsigtigheden for registrerede, men også i business to business-forhold, f.eks. mellem dataansvarlige og databehandlere. I betragtning 100 til databeskyttelsesforordningen anføres det, at fastlæggelsen af certificeringsmekanismer kan forbedre gennemsigtigheden og overholdelsen af forordningen og sætte registrerede i stand til at vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester[4].

5. Der indføres ikke en ret eller pligt til certificering for dataansvarlige og databehandlere med databeskyttelsesforordningen. I henhold til artikel 42, stk. 3, er certificering en frivillig proces, der kan bruges til at påvise, at databeskyttelsesforordningen er overholdt. Medlemsstaterne og tilsynsmyndighederne opfordres til at tilskynde til fastlæggelse af certificeringsmekanismer og træffer afgørelse om inddragelsen af interessenter i certificeringsprocessen og -livscyklussen.

6. Overholdelse af godkendte certificeringsmekanismer er desuden en faktor, som tilsynsmyndighederne skal anse for en skærpende eller en formildende faktor, når de træffer afgørelse om, hvorvidt der skal pålægges en administrativ bøde, og om den administrative bødes størrelse (artikel 83, stk. 2, litra j))[5].

1.1 Retningslinjernes anvendelsesområde

7. Disse retningslinjer har et begrænset anvendelsesområde. De udgør ikke en procedurehåndbog for certificering i overensstemmelse med databeskyttelsesforordningen. Det primære formål med disse retningslinjer er at identificere de overordnede krav og kriterier, som kan være relevante for alle typer certificeringsmekanismer, der udstedes i overensstemmelse med databeskyttelsesforordningens artikel 42 og 43. Retningslinjerne:

    - undersøger rationalet for certificering som et ansvarlighedsværktøj
    - forklarer de centrale begreber i certificeringsbestemmelserne i artikel 42 og 43 og
    - gør rede for anvendelsesområdet for certificering i henhold til artikel 42 og 43, og formålet med certificering
    - bidrager til at sikre, at resultatet af certificering er meningsfuldt, utvetydigt og så reproducerbart som muligt og er sammenligneligt, uanset hvem der har udstedt certifikaterne (sammenlignelighed).

8. I henhold til databeskyttelsesforordningen har medlemsstaterne og tilsynsmyndighederne en række muligheder for at gennemføre artikel 42 og 43. I retningslinjerne gives der gode råd om

[3] I disse retningslinjer benævnes certificeringsmekanismer og databeskyttelsesmærkninger og -mærker under ét "certificeringsmekanismer" (se afsnit 1.3.2).
[4] I betragtning 100 anføres det, at fastlæggelsen af certificeringsmekanismer bør fremmes for "at forbedre gennemsigtigheden og overholdelsen af denne forordning [...], så registrerede hurtigt kan vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester".
[5] Se Artikel 29-Gruppens retningslinjer vedrørende anvendelse og fastsættelse af administrative bøder i overensstemmelse med forordning (EU) 2016/679 (WP 253).

fortolkningen og gennemførelsen af bestemmelserne i artikel 42 og 43, og de kan hjælpe medlemsstaterne, tilsynsmyndighederne og de nationale akkrediteringsorganer med at udvikle en mere ensartet og harmoniseret tilgang til gennemførelsen af certificeringsmekanismer i overensstemmelse med databeskyttelsesforordningen.

9. De gode råd i retningslinjerne er relevante for:

    - de kompetente tilsynsmyndigheder og Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet"), når de godkender certificeringskriterier i henhold til artikel 42, stk. 5, artikel 58, stk. 3, litra f), og artikel 70, stk. 1, litra o)
    - certificeringsorganer, når de udformer og reviderer certificeringskriterier, inden de forelægges den kompetente tilsynsmyndighed til godkendelse i henhold til artikel 42, stk. 5
    - Databeskyttelsesrådet, når det godkender en europæisk databeskyttelsesmærkning i henhold til artikel 42, stk. 5, og artikel 70, stk. 1, litra o)
    - tilsynsmyndighederne, når de udformer deres egne certificeringskriterier
    - Europa-Kommissionen, som har beføjelse til at vedtage delegerede retsakter med henblik på at fastlægge de krav, der skal tages i betragtning vedrørende certificeringsmekanismerne, i henhold til artikel 43, stk. 8
    - Databeskyttelsesrådet, når det afgiver en udtalelse om certificeringskravene i overensstemmelse med artikel 70, stk. 1, litra q), og artikel 43, stk. 8, til Kommissionen
    - nationale akkrediteringsorganer, der skal tage hensyn til certificeringskriterier ved akkrediteringen af certificeringsorganer i overensstemmelse med EN-ISO/IEC 17065/2012 og de yderligere krav i overensstemmelse med artikel 43, og
    - dataansvarlige og databehandlere, når de fastlægger deres egen strategi for overholdelse af databeskyttelsesforordningen og overvejer certificering som et middel til at påvise overholdelse.

10. Databeskyttelsesrådet offentliggør særskilte retningslinjer vedrørende identifikationen af kriterier for godkendelse af certificeringsmekanismer som overførselsværktøjer til tredjelande eller internationale organisationer i henhold til artikel 42, stk. 2.

1.2 Formålet med certificering i henhold til databeskyttelsesforordningen

11. I henhold til artikel 42, stk. 1, skal certificeringsmekanismer fastlægges "med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder denne forordning".

12. I databeskyttelsesforordningen gives der eksempler på den sammenhæng, hvori godkendte certificeringsmekanismer kan anvendes som et element til at påvise, at dataansvarlige og databehandlere overholder deres forpligtelser vedrørende:

    - implementering og påvisning af passende tekniske og organisatoriske foranstaltninger som omhandlet i artikel 24, stk. 1 og 3, artikel 25 og artikel 32, stk. 1 og 3

- de fornødne garantier fra databehandler til dataansvarlig som omhandlet i artikel 28, stk. 1, og fra anden databehandler til databehandler som omhandlet i artikel 28, stk. 4, jf. artikel 28, stk. 5.

13. Eftersom certificering ikke i og af sig selv godtgør overholdelse, men i stedet er et element, der kan bruges til at påvise overholdelse, bør certificering ske på en gennemsigtig måde. Påvisning af overholdelse kræver dokumentation, specifikt skriftlige rapporter, der ikke kun gentager, men beskriver, hvordan kriterierne er opfyldt, og som, hvis kriterierne ikke indledningsvis var opfyldt, beskriver korrektioner og korrigerende tiltag samt deres hensigtsmæssighed, således at der gives en begrundelse for at indrømme og opretholde certificeringen. Dette omfatter en kort beskrivelse af den enkelte afgørelse om indrømmelse, fornyelse eller tilbagetrækning af et certifikat. Heri bør der angives de årsager, argumenter og beviser, der følger af anvendelsen af kriterierne og konklusionerne, vurderingerne eller udledningerne af fakta eller præmisser, der er indsamlet under certificeringen.

1.3 Nøglebegreber

14. I det følgende afsnit gennemgås nøglebegreberne i artikel 42 og 43. I denne analyse udvikles der en forståelse af de grundlæggende udtryk og anvendelsesområdet for certificering i henhold til databeskyttelsesforordningen.

1.3.1 Fortolkning af "certificering"

15. "Certificering" defineres ikke i databeskyttelsesforordningen. Den Internationale Standardiseringsorganisation (ISO) har generelt defineret certificering som "et uafhængigt vurderingsorgans levering af skriftlig dokumentation (et certifikat) for, at produktet, tjenesten eller systemet opfylder specifikke krav". Certificering benævnes også "tredjepartsoverensstemmelsesvurdering", og certificeringsorganer benævnes også "overensstemmelsesvurderingsorganer". I EN-ISO/IEC 17000:2004 — Overensstemmelsesvurdering — Ordliste og generelle principper (hvortil ISO17065 henviser) — defineres certificering som: "tredjepartsattestering … vedrørende produkter, processer og tjenester".

16. Attestering er "udstedelse af en erklæring, der bygger på en beslutning truffet efter en revision, om, at opfyldelsen af de specifikke krav er påvist" (afsnit 5.2, ISO 17000:2004).

17. I forbindelse med certificering i henhold til databeskyttelsesforordningens artikel 42 og 43 henviser certificering til tredjepartsattestering vedrørende dataansvarliges og databehandleres behandlingsaktiviteter.

1.3.2 Certificeringsmekanismer og databeskyttelsesmærkninger og -mærker

18. Databeskyttelsesforordningen definerer ikke "certificeringsmekanismer og databeskyttelsesmærkninger og -mærker" og anvender udtrykkene under ét. Et certifikat er

en overensstemmelseserklæring. En mærkning eller et mærke kan anvendes til at angive den vellykkede gennemførelse af en certificeringsprocedure. En mærkning eller et mærke er almindeligvis et logo eller et symbol, hvis tilstedeværelse (ud over et certifikat) angiver, at genstanden for certificering er blevet uafhængigt vurderet i en certificeringsprocedure og opfylder de fastsatte krav, som er angivet i et normativt dokument som f.eks. regler, standarder eller tekniske specifikationer. I forbindelse med certificering i henhold til databeskyttelsesforordningen er disse krav fastsat i de yderligere krav, der supplerer reglerne for akkreditering af certificeringsorganer i EN-ISO/IEC 17065/2012 og de certificeringskriterier, der er godkendt af den kompetente tilsynsmyndighed eller Databeskyttelsesrådet. Et certifikat, en mærkning eller et mærke som omhandlet i databeskyttelsesforordningen kan kun udstedes efter et akkrediteret certificeringsorgans eller en kompetent tilsynsmyndigheds uafhængige vurdering af dokumentation for, at certificeringskriterierne er blevet opfyldt.

19. I tabellen gives der et generisk eksempel på en certificeringsproces.

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 TILSYNSMYNDIGHEDERNES ROLLE

20. I henhold til artikel 42, stk. 5, skal certificering udstedes af et akkrediteret certificeringsorgan eller af en kompetent tilsynsmyndighed. Udstedelse af certificeringer er ifølge databeskyttelsesforordningen ikke en obligatorisk opgave for tilsynsmyndighederne. Databeskyttelsesforordningen tillader i stedet en række forskellige modeller. En tilsynsmyndighed kan f.eks. vælge en eller flere af følgende muligheder:

    - selv at udstede certificering vedrørende myndighedens egen certificeringsordning

- selv at udstede certificering vedrørende myndighedens egen certificeringsordning, men uddelegere vurderingsprocessen helt eller delvist til tredjeparter
- etablere sin egen certificeringsordning og overlade certificeringsproceduren til de certificeringsorganer, der udsteder certificeringen, og
- tilskynde markedet til at udvikle certificeringsmekanismer.

21. En tilsynsmyndighed skal også vurdere sin rolle i lyset af de afgørelser, der træffes på nationalt plan vedrørende akkrediteringsmekanismer – navnlig hvis tilsynsmyndigheden selv har beføjelse til at akkreditere certificeringsorganer i henhold til databeskyttelsesforordningens artikel 43, stk. 1. Hver tilsynsmyndighed bestemmer derfor, hvilken tilgang den vil benytte for at opfylde det brede formål med certificering i henhold til databeskyttelsesforordningen. Dette bestemmes i forbindelse med opgaverne og beføjelserne i artikel 57 og 58 og under hensyntagen til certificering som en faktor, der skal tages i betragtning ved fastlæggelsen af administrative bøder, og mere generelt som et middel til at påvise overholdelse.

2.1 Tilsynsmyndighed som certificeringsorgan

22. Hvis en tilsynsmyndighed vælger at udføre certificering, skal den nøje overveje sin rolle med hensyn til de opgaver, den er tildelt i medfør af databeskyttelsesforordningen. Myndighedens rolle og myndighedsudøvelse bør være gennemsigtig. Den skal specifikt tage hensyn til magtopdelingen i forbindelse med undersøgelser og håndhævelse med henblik på at undgå potentielle interessekonflikter.

23. Når en tilsynsmyndighed fungerer som certificeringsorgan, skal den sørge for, at der er etableret en certificeringsmekanisme, og udvikle eller vedtage certificeringskriterier. Hver tilsynsmyndighed, som udsteder certificeringer, skal regelmæssigt gennemgå dem (artikel 57, stk. 1, litra o)) og har beføjelse til at trække en certificering tilbage, hvis kravene til certificering ikke er eller ikke længere er opfyldt (artikel 58, stk. 2, litra h)). For at opfylde disse krav kan der etableres en certificeringsprocedure og proceskrav, og der kan, hvis andet ikke er fastsat ved f.eks. national lov, indgås en retligt bindende aftale om leveringen af certificeringsaktiviteter med en enkelte ansøgerorganisation. Det bør sikres, at det i denne certificeringsaftale kræves, at ansøgeren mindst overholder certificeringskriterierne, herunder de nødvendige ordninger for at foretage evalueringen, overvåge opfyldelsen af kriterierne og foretage regelmæssig revision, herunder adgang til oplysninger og/eller lokaler, dokumentation og offentliggørelse af rapporter og resultater, samt undersøgelse af klager. Det forventes yderligere, at en tilsynsmyndighed anvender kravene i retningslinjerne for akkreditering af certificeringsorganer ud over kravene omhandlet i artikel 43, stk. 2.

2.2 Tilsynsmyndighedens yderligere opgaver vedrørende certificering

24. I medlemsstater, hvor certificeringsorganer bliver aktive, har tilsynsmyndigheden, uanset dens egne aktiviteter, beføjelse til og til opgave at:

- vurdere en certificeringsordnings kriterier og udarbejde et udkast til afgørelse (artikel 42, stk. 5)

- meddele Databeskyttelsesrådet udkastet til afgørelse, når den har til hensigt at godkende kriterierne for certificering (artikel 64, stk. 1, litra c) og artikel 64, stk. 7) og tage hensyn til Databeskyttelsesrådets udtalelse (artikel 64, stk. 1, litra c) og artikel 70, stk. 1, litra t))
- godkende kriterierne for certificering (artikel 58, stk. 3, litra f)), inden akkreditering og certificering kan finde sted (artikel 42, stk. 5, og artikel 43, stk. 2, litra b))
- offentliggøre certificeringskriterierne (artikel 43, stk. 6)
- fungere som kompetent myndighed for EU-dækkende certificeringsordninger, som kan føre til en europæisk databeskyttelsesmærkning godkendt af Databeskyttelsesrådet (artikel 42, stk. 5, og artikel 70, stk. 1, litra o)), og
- give et certificeringsorgan påbud om a) ikke at udstede en certificering eller b) at trække certificeringen tilbage, hvis kravene til certificering (certificeringsprocedurer eller -kriterier) ikke er eller ikke længere er opfyldt (artikel 58, stk. 2, litra h)).

25. Ifølge databeskyttelsesforordningen har tilsynsmyndigheden til opgave at godkende certificeringskriterier, ikke at udvikle kriterier. For at godkende certificeringskriterier i henhold til artikel 42, stk. 5, skal en tilsynsmyndighed have en klar forståelse af, hvad der forventes, specifikt med hensyn til anvendelsesområde og indhold, med henblik på at påvise, at databeskyttelsesforordningen overholdes, og med hensyn til dens opgave med at overvåge og håndhæve anvendelsen af forordningen. I bilaget gives der vejledning for at sikre en harmoniseret tilgang til vurderingen af kriterierne med henblik på godkendelse.

26. I henhold til artikel 43, stk. 1, skal certificeringsorganer underrette deres tilsynsmyndighed inden udstedelse eller fornyelse af certificeringer for at gøre det muligt for den at udøve sine korrigerende beføjelser i henhold til artikel 58, stk. 2, litra h). I henhold til artikel 43, stk. 5, skal certificeringsorganer desuden give den kompetente tilsynsmyndighed oplysninger om begrundelsen for at udstede eller tilbagetrække den certificering, der er anmodet om. Selv om databeskyttelsesforordningen gør det muligt for tilsynsmyndighederne at bestemme, hvordan disse oplysninger operationelt skal modtages, anerkendes, revideres og håndteres (dette kan f.eks. omfatte teknologiske løsninger, som understøtter rapportering fra certificeringsorganer), kan der indføres en proces og kriterier for behandling af de oplysninger og rapporter, som certificeringsorganet giver om hvert godkendt certificeringsprojekt i henhold til artikel 43, stk. 1. På grundlag af disse oplysninger kan tilsynsmyndigheden udøve sine beføjelser til at give certificeringsorganet påbud om at tilbagetrække eller ikke at udstede en certificering (artikel 58, stk. 2, litra h)) og til at overvåge og håndhæve anvendelsen af kravene og kriterierne for certificering i henhold til databeskyttelsesforordningen (artikel 57, stk. 1, litra a), og artikel 58, stk. 2, litra h)). Dette vil understøtte en harmoniseret tilgang og sammenlignelighed, når certificering foretages af forskellige certificeringsorganer, og vil sikre, at tilsynsmyndighederne har kendskab til oplysninger om en organisations certificeringsstatus.

3 ET CERTIFICERINGSORGANS ROLLE

27. Et certificeringsorgans rolle er at udstede, revidere, forny og tilbagetrække certificeringer (artikel 42, stk. 5 og 7) på grundlag af en certificeringsmekanisme og godkendte kriterier (artikel 43, stk. 1). Dette kræver, at certificeringsorganet eller ejeren af en certificeringsordning fastlægger og opstiller certificeringskriterier og certificeringsprocedurer, herunder procedurer for overvågning af overholdelse, revision, håndtering af klager og tilbagetrækning. Certificeringskriterierne revideres som led i akkrediteringsprocessen, som omfatter de regler og procedurer, hvorefter certificeringer, mærkninger eller mærker udstedes (artikel 43, stk. 2, litra c)).

28. Certificeringsorganet kan kun opnå akkreditering i henhold til artikel 43, hvis der forefindes en certificeringsmekanisme og certificeringskriterier. Anvendelsesområdet for og typen af certificeringskriterier, som påvirker certificeringsprocedurerne, har stor betydning for, hvad et certificeringsorgan gør, og omvendt. Specifikke kriterier kan f.eks. kræve specifikke evalueringsmetoder så som kontroller på stedet og revision af kodeksen. Disse procedurer er obligatoriske for at opnå akkreditering og er forklaret nærmere i retningslinjerne vedrørende akkreditering.

29. I henhold til databeskyttelsesforordningen skal certificeringsorganet give tilsynsmyndighederne oplysninger, navnlig om individuelle certificeringer, som er nødvendige for at overvåge anvendelsen af certificeringsmekanismen (artikel 42, stk. 7, artikel 43, stk. 5, og artikel 58, stk. 2, litra h)).

4 GODKENDELSEN AF CERTIFICERINGSKRITERIER

30. Certificeringskriterierne udgør en integreret del af alle certificeringsmekanismer. Følgelig skal certificeringskriterierne i en certificeringsmekanisme godkendes af den kompetente tilsynsmyndighed i henhold til databeskyttelsesforordningen (artikel 42, stk. 5, og artikel 43, stk. 2, litra b)). Hvis der er tale om en europæisk databeskyttelsesmærkning, skal certificeringskriterier godkendes af Databeskyttelsesrådet (artikel 42, stk. 2, og artikel 70, stk. 1, litra o)). Begge muligheder for godkendelse af certificeringskriterierne er forklaret nedenfor.

31. Databeskyttelsesrådet anerkender følgende formål med godkendelsen af certificeringskriterier:

    - at afspejle de krav og principper for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger, der er fastlagt i forordning (EU) 2016/679, og
    - at bidrage til den ensartede anvendelse af databeskyttelsesforordningen.

32. Godkendelse indrømmes på grundlag af databeskyttelsesforordningens krav om, at certificeringsmekanismen skal gøre det muligt for dataansvarlige og databehandlere at påvise, at de overholder databeskyttelsesforordningen, i overensstemmelse med certificeringskriterierne.

4.1 Den kompetente tilsynsmyndigheds godkendelse af kriterier

33. Certificeringskriterier skal godkendes af den kompetente tilsynsmyndighed inden eller under processen for akkreditering af et certificeringsorgan. Det samme certificeringsorgan skal også

godkende opdaterede eller yderligere ordninger eller sæt af kriterier efter ISO 17065, inden de ændrede certificeringsmekanismer anvendes (artikel 42, stk. 5, og artikel 43, stk. 2, litra b)). Tilsynsmyndighederne skal behandle alle anmodninger om godkendelse af certificeringskriterier på en rimelig og ikkediskriminerende måde i overensstemmelse med en offentligt tilgængelig procedure, som angiver de generelle betingelser, der skal opfyldes, og en beskrivelse af godkendelsesprocessen.

34. Et certificeringsorgan kan kun udstede certificeringer i en bestemt medlemsstat i overensstemmelse med de kriterier, der er godkendt af tilsynsmyndigheden i den pågældende medlemsstat. Certificeringskriterierne skal med andre ord godkendes af den kompetente tilsynsmyndighed det sted, hvor certificeringsorganet har til hensigt at tilbyde certificering og opnår akkreditering. Se afsnittet nedenfor vedrørende EU-dækkende certificeringsordninger.

4.2 Databeskyttelsesrådets godkendelse af kriterier for den europæiske databeskyttelsesmærkning

35. Et certificeringsorgan kan også udstede certificering i overensstemmelse med kriterier for en europæisk databeskyttelsesmærkning, der er godkendt af Databeskyttelsesrådet. Certificeringskriterier, der er godkendt af Databeskyttelsesrådet i henhold til artikel 63, kan føre til en europæisk databeskyttelsesmærkning (artikel 42, stk. 5). I lyset af eksisterende certificerings- og akkrediteringskonventioner bør det efter Databeskyttelsesrådets opfattelse undgås, at markedet for certificering vedrørende databeskyttelse fragmenteres. Rådet bemærker, at medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen i henhold til artikel 42, stk. 1, skal tilskynde til etableringen af certificeringsmekanismer, navnlig på EU-plan.

4.2.1 Ansøgning om godkendelse

36. Ansøgningen om Databeskyttelsesrådets godkendelse af kriterier i henhold til artikel 42, stk. 5, og artikel 70, stk. 1, litra o), skal indgives via en kompetent tilsynsmyndighed og bør indeholde oplysninger om ordningsejerens, kandidatens eller det akkrediterede certificeringsorgans hensigt om at tilbyde kriterierne i en certificeringsmekanisme, som henvender sig til dataansvarlige og databehandlere i alle medlemsstater. Den kompetente tilsynsmyndighed fremsender et udkast til Databeskyttelsesrådet, når den vurderer, at kriterierne bør godkendes af Databeskyttelsesrådet.

37. Hvor en ansøgning om godkendelse af kriterier skal indgives, afhænger af, hvor ejerne af certificeringsordningen eller certificeringsorganerne har deres hovedkvarter.

38. Hvis et certificeringsorgan indgiver en ansøgning, er det sædvanligvis i gang med at ansøge om akkreditering eller er allerede blevet akkrediteret af den kompetente tilsynsmyndighed eller af det nationale akkrediteringsorgan i dets medlemsstat. Hvis certificeringsorganet allerede er akkrediteret for en certificeringsmekanisme efter databeskyttelsesforordningen, kan dette bidrage til at strømline godkendelsesprocessen.

4.2.2 Kriterier vedrørende den europæiske databeskyttelsesmærkning

39. Databeskyttelsesrådet vil koordinere vurderingsprocessen og godkende kriterierne vedrørende den europæiske databeskyttelsesmærkning, når det er nødvendigt. Denne vurdering omhandler f.eks.: kriteriernes anvendelsesområde og muligheden for, at de kan anvendes som en fælles certificering. Hvis kriterierne er godkendt af Databeskyttelsesrådet, forventes det, at den tilsynsmyndighed, der er kompetent for certificeringsorganets hovedkvarter i Unionen, håndterer klager vedrørende selve mekanismen og underretter de øvrige tilsynsmyndigheder. Denne tilsynsmyndighed er også kompetent til at træffe foranstaltninger over for certificeringsorganet. Den kompetente tilsynsmyndighed underretter de øvrige tilsynsmyndigheder og Databeskyttelsesrådet, for så vidt det er nødvendigt.

40. Certificeringskriterier, der vedrører en fælles certificering, er underlagt EU-dækkende krav og bør omfatte en specifik mekanisme til håndtering af disse krav. Europæiske certificeringsmekanismer skal være udformet til at blive anvendt i alle medlemsstater. På grundlag af artikel 42, stk. 5, skal mekanismen for en europæisk databeskyttelsesmærkning og de tilknyttede kriterier kunne tilpasses, så de tager hensyn til nationale sektorspecifikke bestemmelser, der finder anvendelse, f.eks. vedrørende databehandling i skoler, og skal kunne anvendes i hele EU.

41. Eksempel: En international skole, der tilbyder undervisning til registrerede i Unionen, er etableret i medlemsstat "A". Skolen ønsker at certificere sin onlineansøgningsproces efter en EU-dækkende certificeringsordning for at opnå en europæisk databeskyttelsesmærkning. Skolen ønsker at ansøge om certificering af behandlingsaktiviteter, der tilbydes af et certificeringsorgan, der er etableret i medlemsstat "B", på grundlag af en europæisk databeskyttelsesmærkning. De kriterier for mærkningen, der er udformet og dokumenteret i den relevante mekanisme, skal overholde de bestemmelser for skoler, der finder anvendelse i medlemsstat "A". Kriterierne bør også indeholde krav om, at der i skolens onlineansøgningsproces gives oplysninger om og tages hensyn til de gældende krav til databeskyttelse i medlemsstaten, som kan adskille sig fra kravene i andre medlemsstater. Et eksempel er samlinger af personoplysninger, der skal indgives i forbindelse med ansøgningen, f.eks. førskolekarakterer eller testresultater, forskellige opbevaringsperioder, indsamling eller behandling af finansielle eller biometriske data og yderligere behandlingsbegrænsninger.

    - Højniveaukriterier for godkendelse af en mekanisme for en europæisk databeskyttelsesmærkning omfatter:
        - kriterier godkendt af Databeskyttelsesrådet
        - anvendelse på tværs af jurisdiktioner, der i relevant omfang afspejler de nationale retlige krav og sektorspecifikke regler
        -
    - harmoniserede kriterier, som kan tilpasses, så de afspejler de nationale krav
        - en beskrivelse af certificeringsmekanismen
        - certificeringsaftalerne med anerkendelse af paneuropæiske krav

- procedurer, der kan sikre og tilvejebringe løsninger vedrørende nationale forskelle, og som kan sikre, at mærkningen hjælper med at påvise, at databeskyttelsesforordningen overholdes, og
- sproget i rapporterne til alle berørte tilsynsmyndigheder.

42. Bilaget indeholder også vejledning om kriterier vedrørende den europæiske databeskyttelsesmærkning.

4.2.3 Akkrediteringens rolle

43. Når kriterier anses for egnede til fælles certificering og er blevet godkendt som sådanne af Databeskyttelsesrådet i henhold til artikel 42, stk. 5, kan certificeringsorganer som bemærket i afsnit 4.2.1 akkrediteres til at foretage certificering efter disse kriterier på EU-plan.

44. Ordninger, der kun påtænktes anvendt i en bestemt medlemsstat, kan ikke tildeles EU-mærkning. Akkreditering med henblik på at opnå en europæisk databeskyttelsesmærkning kræver akkreditering i den medlemsstat, hvor hovedkvarteret for det certificeringsorgan, der har til hensigt at anvende ordningen, er beliggende, dvs. det organ, der har ansvaret for at udstede certificeringer og forvalte dets enheders og datterselskabers certificeringsaktiviteter i andre medlemsstater. Hvis andre afdelinger eller kontorer forvalter og udfører certificeringer selvstændigt, skal disse afdelinger eller kontorer have særskilt akkreditering i den medlemsstat, hvor de er etableret. Akkreditering kræves med andre ord kun i den medlemsstat, hvor hovedkvarteret for certificeringsorganet er beliggende, hvis kun hovedkvarteret udsteder certifikater. Hvis andre afdelinger under certificeringsorganet også udsteder certifikater, skal disse afdelinger derimod også akkrediteres.

45. Hvis et certificeringsorgan ikke er blevet akkrediteret til at certificere under den europæiske databeskyttelsesmærkning, kan de kriterier, der er godkendt af Databeskyttelsesrådet, ikke anvendes, og mærkningen kan ikke tilbydes.

5 UDVIKLINGEN AF CERTIFICERINGSKRITERIER

46. Med databeskyttelsesforordningen opstilles der en ramme for udviklingen af certificeringskriterier. De grundlæggende krav vedrørende certificeringsproceduren er omhandlet i artikel 42 og 43, som også omhandler de grundlæggende kriterier for certificeringsprocedurer, men selve certificeringskriterierne udspringer af databeskyttelsesforordningens principper og regler og hjælper med at sikre, at de opfyldes.

47. Udviklingen af certificeringskriterier bør fokusere på certificeringskriteriernes verificerbarhed, betydning og egnethed til at påvise, at forordningen overholdes. Certificeringskriterierne bør formuleres på en sådan måde, at de er klare og forståelige, og at de kan anvendes i praksis.

48. Ved udformningen af certificeringskriterier skal der bl.a. tages hensyn til følgende aspekter vedrørende overholdelse, som understøtter vurderingen af behandlingsaktiviteterne:

    - behandlingens lovlighed i henhold til artikel 6
    - principperne for behandling af personoplysninger i henhold til artikel 5
    - de registreredes rettigheder i henhold til artikel 12-23
    - forpligtelsen til at anmelde brud på persondatasikkerheden i henhold til artikel 33
    - forpligtelsen til databeskyttelse gennem design og standardindstillinger i henhold til artikel 25
    - om der er udført en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35, stk. 7, litra d), hvis det er relevant, og
    - de tekniske og organisatoriske foranstaltninger, der er gennemført i henhold til artikel 32.

49. Det omfang, hvori disse hensyn afspejles i kriterierne, varierer afhængigt af anvendelsesområdet for certificering, som kan omfatte typen af behandlingsaktivitet(er) og certificeringsområdet (f.eks. sundhedssektoren).

5.1 Hvad kan certificeres efter databeskyttelsesforordningen?

50. Databeskyttelsesforordningen opstiller efter Databeskyttelsesrådets opfattelse brede rammer for, hvad der kan certificeres efter databeskyttelsesforordningen, såfremt målet er at hjælpe med at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder denne forordning (artikel 42, stk. 1).

51. Vurderingen af en aktivitet skal omfatte følgende tre centrale komponenter, hvis det er relevant:

    1. personoplysninger (databeskyttelsesforordningens materielle anvendelsesområde)
    2. tekniske systemer — infrastrukturen som f.eks. hardware og software, der anvendes til at behandle personoplysninger, og
    3. processer og procedurer vedrørende behandlingsaktiviteterne.

52. Hver komponent, der anvendes i behandlingsaktiviteter, skal vurderes i forhold til de fastsatte kriterier. Mindst fire forskellige vigtige faktorer kan have betydning: 1) den dataansvarliges eller databehandlerens organisation og juridiske form, 2) den afdeling, det miljø og de personer, der er involveret i behandlingsaktiviteterne, 3) den tekniske beskrivelse af de elementer, der skal vurderes, og endelig 4) den IT-infrastruktur, der understøtter behandlingsaktiviteterne, herunder operativsystemer, virtuelle systemer, databaser, autentificerings- og godkendelsessystemer, routere og firewalls, lagringssystemer, kommunikationsinfrastruktur eller internetadgang og tilknyttede tekniske foranstaltninger.

53. Alle tre centrale komponenter er relevante for udformningen af certificeringsprocedurer og kriterier. Afhængigt af genstanden for certificering varierer det, hvorvidt de tages i betragtning. I nogle tilfælde tages visse komponenter f.eks. ikke i betragtning, hvis de ikke anses for relevante for genstanden for certificering.

54. Med henblik på at specificere, hvad der kan certificeres efter databeskyttelsesforordningen, gives der yderligere vejledning i databeskyttelsesforordningen. Det følger af artikel 42, stk. 7, at certificeringer under databeskyttelsesforordningen kun udstedes til dataansvarlige og databehandlere. Det betyder, at certificering af databeskyttelsesrådgivere ikke er omfattet. I artikel 43, stk. 1, litra b), henvises der til ISO 17065, som omhandler akkrediteringen af certificeringsorganer, der vurderer overensstemmelsen af produkter, tjenester og processer. En behandlingsaktivitet eller en række aktiviteter kan føre til et produkt eller en tjeneste ifølge terminologien i ISO 17065 og kan som sådan være underlagt certificering. Behandlingen af medarbejderdata med henblik på lønudbetaling eller ferieplanlægning er en række aktiviteter som omhandlet i databeskyttelsesforordningen og kan også føre til et produkt eller en tjeneste ifølge ISO's terminologi.

55. Ud fra disse betragtninger finder Databeskyttelsesrådet, at anvendelsesområdet for certificering under databeskyttelsesforordningen er målrettet mod behandlingsaktiviteter eller rækker af aktiviteter. Disse kan omfatte forvaltningsprocesser, dvs. organisatoriske foranstaltninger, som udgør en integreret del af en behandlingsaktivitet (f.eks. den forvaltningsproces, der er fastlagt for at håndtere klager som en del af behandlingen af medarbejderdata med henblik på lønudbetaling).

56. For at vurdere, om behandlingsaktiviteten opfylder certificeringskriterierne, skal der gives et eksempel på anvendelsen. Hvorvidt anvendelsen af en teknisk infrastruktur i forbindelse med en behandlingsaktivitet, opfylder kriterierne, afhænger f.eks. af de kategorier af data, den er udviklet til at behandle. Organisatoriske foranstaltninger afhænger af kategorierne og mængden af data og den tekniske infrastruktur, der anvendes til behandlingen, under hensyntagen til behandlingens karakter, anvendelsesområde, indhold og formål samt risiciene for de registreredes rettigheder og frihedsrettigheder.

57. Det skal endvidere erindres, at der er stor variation mellem IT-applikationer, selv om de tjener de samme behandlingsformål. Dette skal derfor tages i betragtning ved fastlæggelsen af certificeringsmekanismernes anvendelsesområde og udformningen af certificeringskriterierne, dvs. at anvendelsesområdet for certificering og kriterier ikke bør være så snævert, at det udelukker IT-applikationer, der har en anden udformning.

5.2 Fastlæggelse af genstanden for certificering

58. Der skal sondres mellem anvendelsesområdet for en certificeringsmekanisme og genstanden — også kaldet evalueringsmålet — i de enkelte certificeringsprojekter under en certificeringsmekanisme. En certificeringsmekanisme kan definere sit anvendelsesområde enten generelt eller i forhold til en bestemt type eller et bestemt område af behandlingsaktiviteter og kan dermed allerede identificere de genstande for certificering, der falder inden for certificeringsmekanismens anvendelsesområde (f.eks. sikker lagring og beskyttelse af personoplysninger i et digitalt datalager). En pålidelig, meningsfuld vurdering af overensstemmelse kan under alle omstændigheder kun finde sted, hvis den individuelle

genstand for et certificeringsprojekt er klart beskrevet. Det skal klart være beskrevet, hvilke behandlingsaktiviteter der er omfattet af genstanden for certificering, og derefter hvilke centrale komponenter, dvs. data, processer og teknisk infrastruktur, der vurderes, og hvilke der ikke vurderes. På denne måde skal grænsefladerne til andre processer også altid tages i betragtning og beskrives. Det, der ikke er kendt, kan naturligvis ikke medtages i vurderingen og kan derfor ikke certificeres. Den individuelle genstand for certificering skal under alle omstændigheder være meningsfuld, for så vidt angår det budskab eller den påstand, der fremsættes om/af certificeringen, og bør ikke vildlede brugeren, kunden eller forbrugeren.

59. [Eksempel 1]

En bank tilbyder sine kunder et websted med netbankfunktioner. Inden for rammerne af denne tjeneste kan kunderne foretage overførsler, købe aktier, oprette stående ordrer og styre deres konti. Banken ønsker at certificere følgende under en certificeringsmekanisme vedrørende databeskyttelse med et generelt anvendelsesområde på grundlag af generiske kriterier:

a) Sikker login

Sikker login er en behandlingsaktivitet, som er forståelig for slutbrugeren, og som er relevant fra et databeskyttelsesperspektiv, da den er vigtig for at garantere sikkerheden af de berørte personoplysninger. Denne behandlingsaktivitet er derfor nødvendig for sikker login og kan dermed bidrage til et meningsfuldt evalueringsmål, hvis det i certifikatet klart anføres, at kun behandlingsaktiviteten vedrørende login er certificeret.

b) Web-frontend

Mens netbankens web-frontend kan være relevant fra et databeskyttelsesperspektiv, er den ikke forståelig for slutbrugeren og kan derfor ikke være et meningsfuldt evalueringsmål. Det er desuden ikke klart for brugeren, hvilke tjenester på webstedet og dermed hvilke behandlingsaktiviteter der er omfattet af certificeringen.

c) Netbank

Netbankens web-frontend er sammen med dens backend behandlingsaktiviteter, som leveres inden for netbanktjenesten, og som kan være meningsfulde for brugeren. I denne sammenhæng skal de begge medtages i evalueringsmålet. Behandlingsaktiviteter, som ikke direkte har forbindelse til leveringen af netbanktjenesten, f.eks. behandlingsaktiviteter, der har til formål at forhindre hvidvask af penge, kan udelukkes fra evalueringsmålet.

De netbanktjenester, som banken tilbyder via sit websted, kan imidlertid også omfatte andre tjenester, som da kræver deres egne behandlingsaktiviteter. I denne sammenhæng kan andre tjenester omfatte eksempelvis tilbud om forsikringsprodukter. Da denne yderligere tjeneste ikke er direkte forbundet med leveringen af netbanktjenester, kan den udelukkes fra evalueringsmålet. Hvis denne yderligere tjeneste (forsikring) er udelukket fra evalueringsmålet, er de grænseflader til denne tjeneste, der er integreret på webstedet, en del af evalueringsmålet og skal derfor beskrives for klart at skelne mellem tjenesterne. En

sådan beskrivelse er nødvendig for at identificere og evaluere mulige datastrømme mellem de to tjenester.

60. [Eksempel 2]

    En bank tilbyder sine kunder en tjeneste, der sætter dem i stand til at samle oplysninger vedrørende forskellige konti og kreditkort fra flere banker (kontosamling). Banken ønsker at få denne tjeneste certificeret efter databeskyttelsesforordningen. Den kompetente tilsynsmyndighed har godkendt en specifik række af certificeringskriterier, der fokuserer på denne aktivitetstype. Certificeringsmekanismens anvendelsesområde omfatter kun følgende overholdelsesaspekter:

    - brugerautentificering og
    - acceptable metoder til at indhente data, der skal samles, fra andre banker/tjenester.

    Eftersom evalueringsmålet er defineret i denne certificeringsmekanismes anvendelsesområde, kan evalueringsmålet ikke meningsfuldt indsnævres inden for det foreslåede anvendelsesområde, så kun en bestemt funktion eller en enkelt behandlingsaktivitet certificeres. I dette scenarie skal et evalueringsmål være det samme som et bestemt anvendelsesområde.

5.3 Evalueringsmetoder og vurderingsmetodologi

61. En overensstemmelsesvurdering, der skal bidrage til at påvise overensstemmelse for behandlingsaktiviteter, kræver, at evalueringsmetoderne og vurderingsmetodologien identificeres og fastlægges. Det har betydning, om oplysningerne til vurderingen udelukkende indsamles fra dokumentation (som ikke er tilstrækkeligt i sig selv), eller om de aktivt indsamles på stedet og ved direkte eller indirekte adgang. Den måde, hvorpå oplysninger indsamles, har konsekvenser for betydningen af certificering og bør derfor defineres og beskrives.

    Procedurer for udstedelse og regelmæssig revision af certificeringer bør omfatte specifikationer, der fastlægger det relevante evalueringsniveau (dybde og granularitet) for at opfylde certificeringskriterierne, og bør omfatte tilvejebringelse af:

    - oplysninger om og specifikation af de anvendte vurderingsmetoder og indsamlede resultater under f.eks. revisioner på stedet eller fra dokumentation
    - evalueringsmetoder med fokus på behandlingsaktiviteterne (data, systemer og processer) og formålet med behandling
    - identifikation af datakategorierne, behovene for databeskyttelse og eventuel involvering af tredjeparter
    - identifikation af roller og eksistensen af en mekanisme til adgangskontrol defineret med udgangspunkt i roller og ansvarsområder.

62. Evalueringens dybde påvirker certificeringens betydning og værdi. Hvis evalueringens dybde reduceres af praktiske hensyn for at mindske omkostningerne, mindskes betydningen af databeskyttelsescertificering. Beslutninger om evalueringens granularitet kan på den anden side overstige ansøgerens finansielle kapacitet og ofte også evaluatorers og revisorers

kapacitet. Med henblik på at påvise overensstemmelse er en meget detaljeret analyse af de anvendte IT-systemer ikke altid afgørende for, at den er meningsfuld.

5.4 Dokumentation af vurdering

63. Certificeringsdokumentationen bør være grundig og fyldestgørende. Manglende dokumentation bevirker, at der ikke kan foretages en korrekt vurdering. Certificeringsdokumentation har primært til formål at sikre gennemsigtigheden af evalueringsprocessen under certificeringsmekanismen. Dokumentation besvarer spørgsmål vedrørende de lovfastsatte krav. Certificeringsmekanismer bør omfatte en standardiseret dokumentationsmetodologi. Derefter vil evaluering gøre det muligt at sammenligne certificeringsdokumentationen med den faktiske status på stedet og i forhold til certificeringskriterier.

64. Fyldestgørende dokumentation af, hvad der er blevet certificeret, og af den anvendte metode sikrer gennemsigtighed. I henhold til artikel 43, stk. 2, litra c), bør certificeringsmekanismer fastlægge procedurer for revision af certificeringer. For at sætte tilsynsmyndigheden i stand til at vurdere, om og hvorvidt certificeringen kan anerkendes ved formelle undersøgelser, kan detaljeret dokumentation være den mest effektive kommunikationsform. Den dokumentation, der udarbejdes under evalueringer, bør derfor navnlig omhandle tre hovedaspekter:

    - de anvendte evalueringsmetoders konsekvens og sammenhæng
    - evalueringsmetoder, der har til formål at påvise, at genstanden for certificering opfylder certificeringskriterier og dermed overholder forordningen, og
    - at resultaterne af evalueringen er blevet valideret af et uafhængigt og uvildigt certificeringsorgan.

5.5 Dokumentation af resultater

65. Betragtning 100 omhandler de mål, der forfølges med indførelsen af certificering.

"For at forbedre gennemsigtigheden og overholdelsen af denne forordning bør fastlæggelsen af certificeringsmekanismer og databeskyttelsesmærkninger og -mærker fremmes, så registrerede hurtigt kan vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester."

66. For at forbedre gennemsigtigheden spiller dokumentationen og formidlingen af resultater en vigtig rolle. Certificeringsorganer, der anvender certificeringsmekanismer og databeskyttelsesmærkninger og -mærker over for de registrerede (i deres rolle som forbrugere eller kunder), bør give lettilgængelige, letforståelige og meningsfulde oplysninger om de certificerede behandlingsaktiviteter. Disse offentlige oplysninger bør mindst omfatte:

    - en beskrivelse af evalueringsmålet
    - en henvisning til de godkendte kriterier, der finder anvendelse på det specifikke evalueringsmål

- metodologien til evalueringen af kriterierne (evaluering på stedet, dokumentation osv.) og
- gyldighedsperioden for certifikatet og
- bør sætte tilsynsmyndighederne og offentligheden i stand til at sammenligne resultater.

6 RETNINGSLINJER FOR FASTLÆGGELSE AF CERTIFICERINGSKRITERIER

67. Certificeringskriterier er en integreret del af en certificeringsmekanisme. Certificeringsproceduren omfatter kravene med hensyn til hvordan, af hvem, i hvilket omfang vurderingen skal foretages, og granulariteten af vurderingen, der skal finde sted i de enkelte certificeringsprojekter vedrørende en specifik genstand eller et specifikt mål for evalueringen. Certificeringskriterierne fastlægger de nominelle krav, i forhold til hvilke den faktiske behandlingsaktivitet, der er defineret i evalueringsmålet, vurderes. Disse retningslinjer for fastlæggelse af certificeringskriterier udgør en generel vejledning, som vil lette vurderingen af certificeringskriterier med henblik på godkendelse.
    - Der bør tages hensyn til følgende generelle betragtninger, når certificeringskriterier godkendes eller fastlægges. Certificeringskriterier bør:
    - være ensartede og verificerbare
    - kunne revideres med henblik på at lette evalueringen af behandlingsaktiviteter i henhold til databeskyttelsesforordningen ved navnlig at angive målene og retningslinjerne for gennemførelsen af disse mål
    - være relevante for den aktuelle målgruppe (f.eks. B2B og B2C)
    - tage hensyn til og i relevant udstrækning være interoperable med andre standarder (f.eks. ISO-standarder og nationale standarder) og
    - være fleksible og skalerbare med henblik på anvendelse på forskellige typer og størrelser af organisationer, herunder mikrovirksomheder og små og mellemstore virksomheder, i henhold til artikel 42, stk. 1, og den risikobaserede tilgang omhandlet i betragtning 77.
68. En lille lokal virksomhed, f.eks. en forhandler, vil sædvanligvis udføre mindre komplekse behandlingsaktiviteter end en stor multinational forhandler. Mens kravene til behandlingsaktiviteternes lovlighed er de samme, skal omfanget af databehandling og kompleksiteten heraf tages i betragtning. Følgelig skal certificeringsmekanismer og deres kriterier være skalerbare i forhold til den aktuelle behandlingsaktivitet.

6.1 Eksisterende standarder

69. Certificeringsorganer skal overveje, hvordan specifikke kriterier tager hensyn til eksisterende relevante instrumenter, f.eks. adfærdskodekser, tekniske standarder eller nationale forskrifter og lovinitiativer. Ideelt vil kriterier være interoperable med eksisterende standarder, som kan hjælpe dataansvarlige eller databehandlere med at opfylde deres forpligtelser i medfør af databeskyttelsesforordningen. Mens industristandarder ofte fokuserer på organisationens beskyttelse og sikkerhed mod trusler, har databeskyttelsesforordningen imidlertid fokus på beskyttelsen af fysiske personers grundlæggende rettigheder. Dette andet perspektiv skal tages i betragtning, når kriterier udformes, eller når kriterier eller certificeringsmekanismer baseret på industristandarder godkendes.

6.2 Fastlæggelse af kriterier

70. Certificeringskriterier skal svare til en certificeringsmekanismes eller -ordnings certificeringserklæring (budskab eller påstand) og skal matche de forventninger, den giver anledning til. En certificeringsmekanismes navn kan allerede identificere anvendelsesområdet og vil have konsekvenser for fastlæggelsen af kriterier.

71. [Eksempel 3]

    En mekanisme med navnet "PrivatSundhed" bør begrænse sit anvendelsesområde til sundhedssektoren. Mærkningsnavnet giver anledning til en forventning om, at databeskyttelseskrav i forbindelse med sundhedsdata er blevet undersøgt. Følgelig skal kriterierne for denne mekanisme være tilstrækkelige til at vurdere databeskyttelseskravene i denne sektor.

72. [Eksempel 4]

    En mekanisme, som vedrører certificeringen af behandlingsaktiviteter, der omfatter forvaltningssystemer inden for databehandling, bør identificere kriterier, der gør det muligt at genkende og vurdere forvaltningsprocesser og de understøttende tekniske og organisatoriske foranstaltninger.

73. [Eksempel 5]

    Kriterierne for en mekanisme, der vedrører cloudcomputing, skal tage hensyn til de særlige tekniske krav, der gør sig gældende for anvendelse af cloudbaserede tjenester. Hvis servere f.eks. anvendes uden for Unionen, skal kriterierne tage hensyn til de betingelser, der er fastsat i databeskyttelsesforordningens kapitel V vedrørende dataoverførsel til tredjelande.

74. Kriterier, der er udformet til at passe til forskellige evalueringsmål i forskellige sektorer og/eller medlemsstater, bør: muliggøre anvendelse i forskellige scenarier, muliggøre identifikation af hensigtsmæssige foranstaltninger, der passer til små, mellemstore eller store behandlingsaktiviteter, og afspejle risiciene for fysiske personers rettigheder og frihedsrettigheder af varierende sandsynlighed og alvor i overensstemmelse med databeskyttelsesforordningen. Følgelig skal de certificeringsprocedurer (f.eks. vedrørende dokumentation, test eller evalueringsmetode og -dybde), der supplerer kriterierne, imødekomme disse behov, og de skal tillade og indføre regler for f.eks. anvendelsen af de relevante kriterier i individuelle certificeringsprojekter. Kriterier skal lette en vurdering af,

hvorvidt der gives tilstrækkelige garantier for gennemførelsen af relevante tekniske og organisatoriske foranstaltninger.

6.3 Certificeringskriteriers levetid

75. Selv om certificeringskriterier skal være pålidelige over tid, er de ikke mejslet i sten. De skal f.eks. revideres, når:

    - den retlige ramme ændres
    - vilkår og bestemmelser fortolkes i EU-Domstolens praksis, eller
    - den tekniske standard er blevet videreudviklet.

For Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)

BILAG 1: TILSYNSMYNDIGHEDERNES OPGAVER OG BEFØJELSER I FORBINDELSE MED CERTIFICERING I OVERENSSTEMMELSE MED DATABESKYTTELSESFORORDNINGEN

	Bestemmelser	Krav
Opgaver	Artikel 43, stk. 6	Kræver, at tilsynsmyndigheden offentliggør de kriterier, der er omhandlet i artikel 42, stk. 5, i en lettilgængelig form og overfører dem til Databeskyttelsesrådet.
	Artikel 57, stk. 1, litra n)	Kræver, at tilsynsmyndigheden godkender certificeringskriterier i henhold til artikel 42, stk. 5.
	Artikel 57, stk. 1, litra o)	Bestemmer, at tilsynsmyndigheden, når det er relevant (dvs. når den udsteder en certificering), skal foretage en regelmæssig revision af certificeringer udstedt i overensstemmelse med artikel 42, stk. 7.
	Artikel 64, stk. 1, litra c)	Kræver, at tilsynsmyndighed meddeler Databeskyttelsesrådet udkastet til afgørelse, når den har til hensigt at godkende kriterierne for certificering omhandlet i artikel 42, stk. 5.
Beføjelser	Artikel 58, stk. 1, litra c)	Bestemmer, at tilsynsmyndighed har beføjelse til at udføre revisioner i henhold til artikel 42, stk. 7.
	Artikel 58, stk. 2, litra h)	Bestemmer, at tilsynsmyndigheden har beføjelse til at tilbagetrække eller give certificeringsorganet påbud om at tilbagetrække en certificering eller give certificeringsorganet påbud om, ikke at udstede certificeringen.
	Artikel 58, stk. 3), litra e)	Bestemmer, at tilsynsmyndigheden har beføjelse til at akkreditere certificeringsorganer.
	Artikel 58, stk. 3), litra f)	Bestemmer, at tilsynsmyndigheden har beføjelse til at udstede certificeringer og godkende certificeringskriterier.

BILAG 2

1 INDLEDNING

Bilag 2 indeholder retningslinjer for gennemgang og vurdering af certificeringskriterier i henhold til artikel 42, stk. 5. I bilaget udpeges emner, som en tilsynsmyndighed for databeskyttelse og Det Europæiske Databeskyttelsesråd vil tage i betragtning og anvende med henblik på godkendelse af en certificeringsmekanismes certificeringskriterier. Certificeringsorganer og ejere af certificeringsordninger, som ønsker at udarbejde udkast til og fremlægge kriterier til godkendelse, bør tage hensyn til spørgsmålene. Listen er ikke udtømmende, men indeholder de emner, der som minimum skal tages i betragtning. Ikke alle spørgsmål vil være relevante, men de bør dog tages i betragtning i forbindelse med udarbejdelsen af kriterier, og der kan være behov for at argumentere for, hvorfor kriterierne ikke dækker specifikke aspekter. Nogle spørgsmål gentages, fordi de udspringer fra forskellige synsvinkler. Denne vejledning bør tages i betragtning i overensstemmelse med de juridiske krav i databeskyttelsesforordningen og, hvis det er relevant, i national lovgivning.

2 CERTIFICERINGSMEKANISMENS ANVENDELSESOMRÅDE OG EVALUERINGSMÅL

a. Er certificeringsmekanismens anvendelsesområde (som databeskyttelseskriterierne skal anvendes på) klart beskrevet?

b. Giver certificeringsmekanismens anvendelsesområde mening for dens målgruppe, eller er det vildledende?

- *Eksempel: Et "pålideligt virksomhedssegl" indikerer, at forarbejdningsaktiviteterne i en hel virksomhed er blevet auditeret, selv om det kun er specifikke forarbejdningsaktiviteter, f.eks. onlinebetalingsprocessen, der faktisk har været genstand for certificering. Anvendelsesområdet er derfor vildledende.*

c. Afspejler certificeringsmekanismens anvendelsesområde alle relevante aspekter af forarbejdningsaktiviteterne?

- *Eksempel: Et "godkendelsesmærke for databeskyttelse i sundhedsvæsenet" skal omfatte alle evalueringsdata vedrørende sundhed for at opfylde kravene i artikel 9.*

d. Giver certificeringsmekanismens anvendelsesområde mulighed for en meningsfuld certificering af databeskyttelse under hensyntagen til arten, indholdet og risikoen ved de tilknyttede behandlingsaktiviteter?

- *Eksempel: Hvis der i certificeringsmekanismens anvendelsesområde er fokus på bestemte aspekter af behandlingsaktiviteter, såsom indsamling af data, men ikke på de efterfølgende behandlingsaktiviteter, såsom behandling med henblik på at skabe reklameprofiler eller forvaltning af den registreredes rettigheder, så ville det ikke give mening for de registrerede.*

e. Dækker certificeringsmekanismens anvendelsesområde behandling af personlige oplysninger i det land, hvor mekanismen anvendes, eller tager den hånd om grænseoverskridende behandling og/eller overførsler?

f. Beskriver certificeringskriterierne i tilstrækkelig grad, hvordan evalueringsmålet bør fastsættes?

- *Eksempel: Et "databeskyttelsessegl" med et generelt anvendelsesområde, som kun kræver "en specifikation af den behandlingsaktivitet, der skal certificeres", ville ikke give tilstrækkelig tydelig vejledning om, hvordan et evalueringsmål fastsættes og beskrives.*
- *Eksempel: Et (specifikt) anvendelsesområde, seglet for sikker opbevaring af personlige oplysninger i en digital sikkerhedsboks, bør i de tilknyttede kriterier omfatte en detaljeret beskrivelse af kravene til dette anvendelsesområde, dvs. en definition af sikkerhedsboks, systemkrav samt obligatoriske tekniske og organisatoriske foranstaltninger. I dette tilfælde kan evalueringsmålet defineres tydeligt af anvendelsesområdet.*

(1) Kræver kriterierne, at evalueringsmålet omfatter identifikation af alle relevante behandlingsaktiviteter, illustration af datastrømme og fastlæggelse af evalueringsmålets anvendelsesområde?

- *Eksempel: En certificeringsmekanisme tilbyder certificering af behandlingsaktiviteter for registeransvarlige under databeskyttelsesforordningen uden yderligere præcisering af anvendelsesområdet (generelt anvendelsesområde). Mekanismens kriterier kræver, at den ansøgende registeransvarlige fastlægger den målrettede behandlingsaktivitet med hensyn til de anvendte datatyper, systemer og processer.*

(2) Kræver kriterierne, at ansøgeren tydeliggør, hvor den behandling, der skal evalueres, begynder og slutter? Kræver kriterierne, at evalueringsmålet omfatter grænseflader, hvor indbyrdes afhængige behandlingsaktiviteter ikke indgår som en del af evalueringsmålet? Og er dette behørigt begrundet?

- *Eksempel: Et evalueringsmål, der tilstrækkeligt detaljeret beskriver en webbaseret tjenestes behandlingsaktivitet, herunder brugerregistrering, ydelse af tjenester, fakturering, registrering af IP-adresser, grænseflader til brugere og tredjeparter, men ikke server-hosting (men inklusiv aftaler vedrørende behandling og obligatoriske tekniske og organisatoriske foranstaltninger).*

g. Garanterer kriterierne, at hvert enkelt evalueringsmål er forståeligt for modtageren, herunder registrerede personer, hvis det er relevant?

3 GENERELLE KRAV

a. Anvendes alle de relevante termer i kriteriekataloget (dvs. den samlede liste over certificeringskriterier), og identificeres, forklares og beskrives de?

b. Identificeres alle normative referencer?

c. Omfatter kriterierne fastlæggelse af databeskyttelsesrelaterede ansvarsområder, procedurer og behandling, som falder inden for certificeringsmekanismens anvendelsesområde?

4 BEHANDLINGSAKTIVITET, ARTIKEL 42, STK. 1

Adresserer kriterierne alle relevante dele af behandlingsaktiviteterne (data, systemer og processer), for så vidt angår certificeringsmekanismens anvendelsesområde (generelt eller specifikt)?

a. Kræver kriterierne identifikation af de gyldige retsgrundlag for behandlingen for så vidt angår evalueringsmålet?

b. Anerkender evalueringsmålene de relevante faser af behandlingen og hele livscyklussen for data, herunder sletning og/eller anonymisering for så vidt angår evalueringsmålet?

c. Kræver kriterierne dataportabilitet for så vidt angår evalueringsmålet?

d. Giver kriterierne mulighed for at identificere og afspejle særlige former for behandlingsaktiviteter, f.eks. automatisk beslutningstagning og profilering for så vidt angår evalueringsmålet?

e. Giver kriterierne mulighed for at identificere særlige datakategorier for så vidt angår evalueringsmålet?

f. Gør kriterierne det muligt at vurdere de risici, der er forbundet med de enkelte behandlingsaktiviteter og de registreredes beskyttelsesbehov hvad angår rettigheder og friheder, og indeholder de krav herom?

g. Giver kriterierne mulighed for at tage tilstrækkeligt hensyn til risici i forbindelse med fysiske personers rettigheder og friheder, og indeholder de krav herom?

…

5 LOVLIGHEDEN AF BEHANDLINGEN

a. Indeholder kriterierne krav om, at lovligheden af behandlingen i forbindelse med hver enkelt behandlingsaktivitet undersøges med hensyn til behandlingens formål og nødvendighed?

b. Indeholder kriterierne krav om, at alle kravene til et retsgrundlag for hver enkelt behandling undersøges?

6 PRINCIPPER, ARTIKEL 5

a. Adresserer kriterierne i tilstrækkelig grad alle databeskyttelsesprincipper i henhold til artikel 5?

b. Indeholder kriterierne krav om dokumentation for dataminimering i forbindelse med hver enkelt behandlingsaktivitet?

…

7 DATAANSVARLIGES OG DATABEHANDLERES ALMINDELIGE FORPLIGTELSER

a. Indeholder kriterierne krav om dokumentation for kontraktlige aftaler mellem databehandlere og dataansvarlige?

b. Evalueres aftaler mellem dataansvarlige og databehandlere?

c. Afspejler kriterierne den dataansvarliges forpligtelser i henhold til kapitel IV?

d. Indeholder kriterierne krav om dokumentation for gennemgang og ajourføring af tekniske og organisatoriske foranstaltninger, som den dataansvarlige har gennemført i henhold til artikel 24, stk. 1?

e. Opfylder kriterierne kravet om, at organisationen har vurderet, om der bør udpeges en databeskyttelsesrådgiver som krævet i artikel 37? Opfylder databeskyttelsesrådgiveren kravene i artikel 37-39, hvor det er relevant?

f. Opfylder kriterierne kravet om dokumentation for behandlingsaktiviteter i overensstemmelse med artikel 30, stk. 5, og om at kravene i artikel 30 adresseres på passende vis?

8 DE REGISTREREDES RETTIGHEDER

a. Adresserer kriterierne i tilstrækkelig grad de registreredes ret til information, og indeholder de krav om, at der skal gennemføres foranstaltninger med henblik herpå?

b. Indeholder kriterierne krav om, at de registrerede gives passende eller endnu bedre adgang til og kontrol med deres data, herunder dataportabilitet?

c. Indeholder kriterierne krav om, at der gennemføres foranstaltninger, som gør det muligt at gribe ind i behandlingsaktiviteten med henblik på at garantere de registreredes rettigheder og muliggøre rettelser, sletning eller begrænsninger?

…

9 RISICI I FORBINDELSE MED FYSISKE PERSONERS RETTIGHEDER OG FRIHEDER

a. Giver kriterierne mulighed for at vurdere risikoen i forbindelse med fysiske personers rettigheder og friheder, og indeholder de krav herom?

b. Tilvejebringer kriterierne en anerkendt metode til risikovurdering, eller indeholder de krav herom? Er metoden passende, hvis det er relevant?

c. Giver kriterierne mulighed for at vurdere virkningen af de planlagte behandlingsaktiviteter på fysiske personers rettigheder og friheder, og indeholder de krav herom?

d. Indeholder kriterierne krav om forudgående høring om de resterende risici, som ikke kunne afbødes, på grundlag af resultaterne af konsekvensanalysen vedrørende databeskyttelse?

10 TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BESKYTTELSE

a. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger til sikring af fortroligheden i forbindelse med behandlingsaktiviteter?

b. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger til sikring af behandlingsaktiviteters integritet?

c. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger til sikring af behandlingsaktiviteters tilgængelighed?

d. Indeholder kriterierne krav om gennemførelse af foranstaltninger til sikring af gennemsigtighed i behandlingsaktiviteter med hensyn til:

e. Ansvarlighed?

f. De registreredes rettigheder?

g. Vurdering af de enkelte behandlingsaktiviteter, f.eks. men hensyn til gennemsigtighed i algoritmer?

h. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger til sikring af de registreredes rettigheder, f.eks. muligheden for at give oplysninger eller med hensyn til dataportabilitet?

i. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger, som gør det muligt at gribe ind i behandlingsaktiviteten med henblik på at garantere de registreredes rettigheder og muliggøre rettelser, sletning eller begrænsninger?

j. Indeholder kriterierne krav om gennemførelse af foranstaltninger, som gør det muligt at gribe ind i behandlingsaktiviteten med henblik på at lappe eller kontrollere systemet eller processen?

k. Indeholder kriterierne krav om gennemførelse af tekniske og organisatoriske foranstaltninger med henblik på at sikre dataminimering, f.eks. gennem afkobling eller adskillelse af oplysningerne fra den registrerede, anonymisering, pseudonymisering eller isolering af datasystemer?

l. Indeholder kriterierne krav om tekniske foranstaltninger med henblik på gennemførelse af databeskyttelse som standard?

m. Indeholder kriterierne krav om tekniske og organisatoriske foranstaltninger til gennemførelse af databeskyttelse gennem design, f.eks. et system til forvaltning af databeskyttelse, som har til formål at fremvise, oplyse, kontrollere og håndhæve databeskyttelseskravene?

n. Indeholder kriterierne krav om tekniske og organisatoriske foranstaltninger til gennemførelse af passende efteruddannelse og uddannelse af det personale, der har permanent eller regelmæssig adgang til personoplysninger?

o. Indeholder kriterierne krav om revision af foranstaltningerne?

p. Indeholder kriterierne krav om selvevaluering/intern revision?

q. Indeholder kriterierne krav om foranstaltninger, som skal sikre, at meddelelsespligten i forbindelse med brud på persondatasikkerheden udføres i rette tid og på passende vis?

r. Indeholder kriterierne krav om, at procedurer for håndtering af hændelser skal være gennemført og godkendt?

s. Indeholder kriterierne krav om overvågning af, hvordan spørgsmål vedrørende privatlivets fred og teknologi udvikler sig, og om opdatering af ordningen efter behov?

…

11 ANDRE SÆRLIGE DATABESKYTTELSESVENLIGE ELEMENTER

a. Indeholder kriterierne krav om indførelse af teknikker til forbedring af databeskyttelsen? Dette kan omfatte kriterier, som indeholder krav om forbedret databeskyttelse gennem fjernelse eller reduktion af risikoen i forbindelse med personoplysninger og/eller databeskyttelse.

- *Eksempel: Kriterier indeholdende krav om bedre muligheder for afkobling gennem anvendelse af brugercentreret identitetsstyring, såsom egenskabsbaserede brugeroplysninger fremfor organisationscentreret identitetsstyring, kan udgøre en teknik til at forbedre databeskyttelsen.*

b. Indeholder kriterierne krav om indførelse af bedre kontrolmekanismer for de registrerede med henblik på at fremme deres selvbestemmelsesret og valgfrihed?

…

12 KRITERIER, SOM HAR TIL FORMÅL AT PÅVISE, AT DER FINDES TILSTRÆKKELIGE BESKYTTELSESFORANSTALTNINGER I FORBINDELSE MED OVERFØRSEL AF PERSONOPLYSNINGER

Kriterierne vil blive adresseret i de kommende retningslinjer vedrørende artikel 42, stk. 2.

13 YDERLIGERE KRITERIER FOR EN EUROPÆISK DATABESKYTTELSESMÆRKNING

a. Er det meningen, at kriterierne skal dække alle medlemsstater?

b. Tager kriterierne hensyn til medlemsstaternes databeskyttelseslovgivning og databeskyttelsesscenarier?

c. Indeholder kriterierne krav om en evaluering af de enkelte evalueringsmål for så vidt angår medlemsstaternes databeskyttelseslovgivning i bestemte sektorer?

d. Indeholder kriterierne krav om, at den dataansvarlige eller databehandleren leverer oplysninger til de registrerede og interesserede parter på medlemsstaternes sprog vedrørende:

e. behandlingen/evalueringsmålet?

f. dokumentation for behandlingen/evalueringsmålet?

g. evalueringens resultater?

…

14 SAMLET EVALUERING AF KRITERIERNE

a. Dækker kriterierne fuldt ud certificeringsmekanismens anvendelsesområde (dvs. omfattende kriterier) med henblik på at tilvejebringe tilstrækkelige garantier til, at certificeringen kan anses for pålidelig?

- *Eksempel: Hvis der inden for certificeringsmekanismens anvendelsesområde er fokus på behandlingsaktiviteter på sundhedsområdet, bør der garanteres et højt databeskyttelsesniveau ved at fastsætte kriterier, der sikrer eksempelvis en grundig vurdering og anvendelse af principper om privatliv-gennem-design og privatliv-som-standard.*

b. Står kriterierne i et passende forhold til omfanget af de behandlingsaktiviteter, som adresseres af certificeringsmekanismens anvendelsesområde, oplysningernes følsomhed og risikoen ved behandlingen?

c. Er det sandsynligt, at kriterierne forbedrer de dataansvarliges og databehandlernes overholdelse af databeskyttelsesreglerne?

d. Vil der ske forbedringer med hensyn til de registreredes informationsrettigheder, bl.a. ved at forklare ønskede resultater for de registrerede?