Udtalelse 15/2026 om Europrivacy-certificeringskriterierne vedrørende Databeskyttelsesrådets godkendelse heraf som europæisk databeskyttelsesmærkning, der skal anvendes som et redskab til overførsler i henhold til databeskyttelsesforordningens artikel 42 og 46

Vedtaget den 15 april 2026

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

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 63, artikel 64, stk. 2, artikel 42 og artikel 46 i Europa-Parlamentets og Rådets forordning 2016/679/EU 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 aftalen om Det Europæiske Økonomiske Samarbejdsområde ("EØS-aftalen"), særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg 6. juli 2018[1],

under henvisning til artikel 10 og 22 i sin forretningsorden og ud fra følgende betragtninger:

1 Medlemsstaterne, tilsynsmyndighederne, Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") og Kommissionen tilskynder navnlig på EU-plan til fastlæggelse af certificeringsmekanismer for databeskyttelse ("certificeringsmekanismer") samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder databeskyttelsesforordningen under hensyntagen til mikrovirksomheders og små og mellemstore virksomheders særlige behov2. Fastlæggelsen af certificeringsmekanismer kan desuden forbedre gennemsigtigheden og give de registrerede mulighed for at vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester3.

2 Certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger eller -mærker, der er godkendt i henhold til databeskyttelsesforordningens artikel 42, stk. 5, kan – ud over overholdelse af de dataansvarlige eller databehandlere, der er omfattet af denne forordning – fastlægges med det formål at påvise tilstedeværelse af fornødne garantier afgivet af dataansvarlige eller databehandlere, der i henhold til artikel 3 ikke er omfattet af databeskyttelsesforordningen, inden for rammerne af overførsel af personoplysninger til tredjelande eller internationale organisationer ("dataimportører"), jf. databeskyttelsesforordningens artikel 46, stk. 2, litra f)4.

3 Certificering, der skal anvendes som et redskab til overførsler, er en ny overførselsmekanisme, der er indført ved databeskyttelsesforordningens artikel 46 for at sikre, at en dataansvarlig eller databehandler omfattet af databeskyttelsesforordningen ("dataeksportør i EØS"), hvis der ikke foreligger en afgørelse i henhold til databeskyttelsesforordningens artikel 45, stk. 3, kun kan overføre personoplysninger til et tredjeland eller en international organisation, hvis der er givet fornødne garantier, og på betingelse af, at der findes rettigheder, som kan håndhæves, og effektive retsmidler for registrerede. Navnlig kan en certificeringsmekanisme, der er godkendt i henhold til databeskyttelsesforordningens artikel 42, ifølge databeskyttelsesforordningens artikel 46, stk. 2, litra f), udgøre sådanne fornødne garantier, hvis den ledsages af bindende tilsagn, som kan håndhæves, fra dataimportørerne om at anvende de fornødne garantier, herunder vedrørende registreredes rettigheder. Certificeringskriterierne udgør en integreret del af en certificeringsmekanisme. Følgelig kræver databeskyttelsesforordningen, at kriterierne for en national certificeringsmekanisme godkendes af den kompetente tilsynsmyndighed (databeskyttelsesforordningens artikel 42, stk. 5, og artikel 43, stk. 2, litra b), eller, i tilfælde af

[1] Henvisninger til "medlemsstater" i hele denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".
[2] Databeskyttelsesforordningens artikel 42, stk. 1.
[3] Databeskyttelsesforordningens betragtning 100.
[4] Jf. databeskyttelsesforordningens artikel 42, stk. 2.

en europæisk databeskyttelsesmærkning, af Databeskyttelsesrådet (databeskyttelsesforordningens artikel 42, stk. 5, og artikel 70, stk. 1, litra o)).

4 Når en tilsynsmyndighed har til hensigt at foreslå, at Databeskyttelsesrådet godkender en europæisk databeskyttelsesmærkning i henhold til databeskyttelsesforordningens artikel 42, stk. 5, bør tilsynsmyndigheden angive, at den ansvarlige for ordningen har til hensigt at tilbyde certificeringsmekanismen i alle medlemsstater. I dette tilfælde er Databeskyttelsesrådets vigtigste opgave at sikre ensartet anvendelse af databeskyttelsesforordningen gennem sammenhængsmekanismen som omhandlet i databeskyttelsesforordningens artikel 63, 64 og 65. Inden for disse rammer godkender Databeskyttelsesrådet ifølge databeskyttelsesforordningens artikel 64, stk. 2, certificeringskriterierne.

5 Europæisk databeskyttelsesmærkning, der er godkendt i henhold til databeskyttelsesforordningens artikel 42, stk. 5, og fastlagt med det formål at påvise tilstedeværelsen af fornødne garantier afgivet af dataimportører sammen med bindende tilsagn, som kan håndhæves, fungerer som et redskab, som omfatter overførsel af personoplysninger fra alle EØS-medlemsstater til tredjelande eller internationale organisationer[5].

6 Ved vurderingen af en certificeringsmekanisme, der skal anvendes som et redskab til overførsler, foretager Databeskyttelsesrådet sin vurdering på grundlag af "Retningslinjer 1/2018 vedrørende certificering og identifikation af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordningen" ("retningslinjerne") og tillægget hertil med vejledning om vurdering af certificeringskriterier ("tillægget") samt af "Retningslinjer 07/2022 om certificering som et redskab til overførsler" ("retningslinjerne om certificering som et redskab til overførsler").

7 Databeskyttelsesrådet anerkender, at hver certificeringsmekanisme bør behandles individuelt, uden at dette berører vurderingen af andre certificeringsmekanismer.

8 Certificeringsmekanismer, der skal anvendes som et redskab til overførsler, bør gøre det muligt for dataimportører at påvise tilstedeværelsen af fornødne garantier for at sikre, at det beskyttelsesniveau for fysiske personer, som er garanteret ved databeskyttelsesforordningen, ikke undergraves, når overførte personoplysninger behandles uden for EØS[6]. Derfor bør kriterierne på passende vis afspejle de krav og principper vedrørende beskyttelse af personoplysninger, der er fastsat i databeskyttelsesforordningen, for at sikre, at den beskyttelse, databeskyttelsesforordningen giver, følger med personoplysningerne[7].

9 Samtidig bør den ansvarlige for ordningen sikre, at certificeringsmekanismen er tilpasset til og i overensstemmelse med samtlige inddragede eller udnyttede ISO-standarder og certificeringspraksis.

10 Som følge heraf bør certificeringer tilføre dataimportører merværdi ved at bidrage til gennemførelsen af standardiserede og specificerede organisatoriske og tekniske foranstaltninger for at påvise, at der findes fornødne garantier ved behandling af personoplysninger modtaget fra dataeksportører i EØS. I den forbindelse minder Databeskyttelsesrådet om, at genstanden for certificeringen – som falder sammen med

[5] Databeskyttelsesrådets retningslinjer 07/2022 om certificering som et redskab til overførsler, version 2.0, vedtaget den 14. februar 2023, punkt 30.
[6] Databeskyttelsesforordningens artikel 44.
[7] Se meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden (COM(2017) 07 final, s. 4).

certificeringens evalueringsmål – generelt bør være behandlingen af de data, der overføres til dataimportøren i tredjelandet, og selve overførslen, hvis den samme importør er ansvarlig[8].

11 Certificeringer vil også have merværdi for dataeksportøren, som kan beslutte at henholde sig til den certificering, som en dataimportør har opnået, som et redskab til at overføre personoplysninger i henhold til databeskyttelsesforordningens artikel 46, stk. 2, litra f), og som et element til at påvise overholdelse af forpligtelser, f.eks. i henhold til databeskyttelsesforordningens artikel 24, stk. 3, eller artikel 28, stk. 5[9].

12 I den forbindelse minder Databeskyttelsesrådet om, at dataeksportører, som ønsker at anvende en certificering som en fornøden garanti i henhold til databeskyttelsesforordningens artikel 46, stk. 2, litra f), desuden er forpligtet til at kontrollere, om den certificering, de ønsker at henholde sig til, er effektiv i betragtning af den tilsigtede databehandlings karakteristika. Med henblik herpå skal dataeksportøren kontrollere certificeringen for at verificere, at den udstedte certificering er gyldig, at den omfatter den specifikke overførsel, der skal foretages, at selve overførslen af personoplysninger er omfattet af certificeringens anvendelsesområde, og at den indeholder oplysninger om og passende dokumentation for eventuelle videreoverførsler[10].

13 Dataeksportøren skal også kontrollere, at det certificeringsorgan, der udsteder certificeringen, er akkrediteret af et nationalt akkrediteringsorgan eller en kompetent tilsynsmyndighed. Desuden bør dataeksportøren henvise til anvendelsen af certificering som et redskab til overførsel i kontrakten om databehandling i henhold til databeskyttelsesforordningens artikel 28, hvis der er tale om overførsler fra en dataansvarlig til en databehandler, eller i en kontrakt om dataudveksling indgået med dataimportøren, hvis der er tale om overførsler fra en dataansvarlig til en dataansvarlig[11]. Dataeksportøren skal også overholde de særlige forpligtelser, der følger af databeskyttelsesforordningens artikel 13, stk. 1, litra f), navnlig ved at oplyse den registrerede om de anvendte fornødne garantier, dvs. i tilfælde af certificering i henhold til databeskyttelsesforordningens artikel 46, stk. 2, litra f), det certifikat, som importøren har modtaget i henhold til en bestemt certificeringsmekanisme, og om, hvordan der kan fås en kopi af certifikatet samt de garantier, der er indeholdt i certificeringskriterierne, eller hvor de er blevet gjort tilgængelige.

14 Databeskyttelsesrådet glæder sig over den indsats, som de ansvarlige for ordningen har gjort for at udarbejde certificeringsmekanismer, der er praktiske og potentielt omkostningseffektive redskaber til at sikre større overensstemmelse med databeskyttelsesforordningen og fremme de registreredes ret til privatlivets fred og databeskyttelse ved at øge gennemsigtigheden.

15 Databeskyttelsesrådet minder om, at certificeringer er frivillige ansvarlighedsværktøjer, og at overholdelsen af en certificeringsmekanisme ikke hindrer tilsynsmyndighederne i at udøve deres opgaver og beføjelser i henhold til databeskyttelsesforordningen og den relevante nationale lovgivning. Dette gælder i forbindelse med certificeringer, der skal anvendes som et redskab til overførsler, også med særligt hensyn til overholdelsen af de forpligtelser, som dataimportørerne via kontraktlige eller andre retligt bindende instrumenter påtager sig som bindende tilsagn, der kan håndhæves, over for dataeksportørerne, om at anvende de fornødne garantier, som certificeringsmekanismen indeholder, herunder for så vidt angår registreredes rettigheder.

[8] Se Databeskyttelsesrådets retningslinjer 7/2022 om certificering som et redskab til overførsler, version 2.0, vedtaget den 14. februar 2023, punkt 16.
[9] Retningslinjer 7/2022 om certificering som et redskab til overførsler, punkt 5.
[10] Retningslinjer 7/2022 om certificering som et redskab til overførsler, punkt 20.
[11] Ibid.

16 Denne udtalelse har til formål at sikre en ensartet anvendelse af databeskyttelsesforordningen, herunder af tilsynsmyndighederne, dataansvarlige og databehandlere, i lyset af de centrale elementer, som certificeringsmekanismerne skal fastlægge. Denne udtalelse har navnlig til formål at vurdere de certificeringskriterier, som dataimportører agter at anvende som et redskab til overførsler. Derfor behandler Databeskyttelsesrådet her spørgsmål som kriteriernes anvendelsesområde, anvendelighed og relevans, når overførsler finder sted fra alle EØS-medlemsstater og/eller fra dataeksportører, der er omfattet af databeskyttelsesforordningens anvendelsesområde.

17 Denne udtalelse har udelukkende fokus på certificeringskriterierne. Databeskyttelsesrådet kan kræve et højt informationsniveau hvad angår evalueringsmetoder for grundigt at kunne vurdere kriteriernes kontrollerbarhed inden for rammerne af sin udtalelse. Dette omfatter dog ikke nogen form for godkendelse af sådanne evalueringsmetoder.

18 Databeskyttelsesrådets udtalelse vedtages i overensstemmelse med databeskyttelsesforordningens artikel 64, stk. 2, sammenholdt med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden inden for otte uger regnet fra den første arbejdsdag, efter formanden og den kompetente tilsynsmyndighed har konkluderet, at sagsakterne er komplette. Efter formandens afgørelse kan denne frist forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet. Hvis konklusionen på Databeskyttelsesrådets udtalelse er, at kriterierne ikke kan godkendes, kan tilsynsmyndigheden forelægge kriterierne til godkendelse igen, når de betænkeligheder, der er givet udtryk for i den oprindelige udtalelse fra Databeskyttelsesrådet, er blevet afhjulpet–

vedtaget følgende udtalelse:

1 Resumé af de faktiske omstændigheder

19 I overensstemmelse med databeskyttelsesforordningens artikel 42, stk. 2, og artikel 46, stk. 2, litra f), retningslinjer 1/2018 og retningslinjer 7/2022 om certificering som et redskab til overførsler er Europrivacy version 82 ("certificeringskriterierne") udarbejdet af European Center for Certification and Privacy ("den ansvarlige for ordningen").

20 Databeskyttelsesrådet minder om, at det allerede den 10. oktober 2022 i sin udtalelse 28/2022 godkendte Europrivacy-certificeringskriterierne (version 60) som europæisk databeskyttelsesmærkning i henhold til databeskyttelsesforordningens artikel 42, stk. 5, med det formål at påvise overholdelse af databeskyttelsesforordningen i henhold til databeskyttelsesforordningens artikel 42, stk. 1. En sådan ordning var ikke en certificering i henhold til databeskyttelsesforordningens artikel 46, stk. 2, litra f), til brug for overførsel af personoplysninger.

21 Den 29. januar 2026 indsendte Luxembourgs tilsynsmyndighed ("den luxembourgske tilsynsmyndighed") til Databeskyttelsesrådet en ajourført version af de allerede godkendte certificeringskriterier for Europrivacy EU Data Protection Seal med et udvidet anvendelsesområde, der navnlig omfatter ansøgere, som er omfattet af databeskyttelsesforordningens artikel 3, stk. 2, samt andre ændringer af de centrale certificeringskriterier (version 82). Databeskyttelsesrådet har vedtaget udtalelse 14/2026 om denne ajourførte version (version 82) af Europrivacy-certificeringskriterierne, der skal påvise overholdelse af databeskyttelsesforordningens i henhold til artikel 42, stk. 5.

22 Samme dag indsendte den luxembourgske tilsynsmyndighed også til Databeskyttelsesrådet et yderligere sæt certificeringskriterier ("The Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46"), som er bestemt til at blive anvendt som et redskab

til overførsler i henhold til databeskyttelsesforordningens artikel 46, stk. 2, litra f), til godkendelse i henhold til databeskyttelsesforordningens artikel 64, stk. 2.

23 Beslutningen om, at sagsakterne var komplette, blev truffet den 31. marts 2026.

2 Vurdering

24 Databeskyttelsesrådet har foretaget sin vurdering af de certificeringskriterier, som dataimportører skal anvende som et redskab til overførsler, og som er forelagt til godkendelse i henhold til databeskyttelsesforordningens artikel 42, stk. 5, sammenholdt med databeskyttelsesforordningens artikel 46, stk. 2, litra f), i overensstemmelse med den struktur, som er fastlagt i bilag 2 til retningslinjer 1/2018 ("bilaget"), tillægget hertil og retningslinjerne om certificering som et redskab til overførsler[12].

25 Databeskyttelsesrådet fremhæver, at den nuværende ordning i overensstemmelse med betingelserne i databeskyttelsesforordningens artikel 42, stk. 2, og artikel 46, stk. 2, litra f), er bestemt til at blive anvendt som et redskab til overførsler, og at de certificeringer, der udstedes i henhold til ordningen, derfor kan benyttes af dataeksportører som omhandlet i databeskyttelsesforordningens kapitel V (dvs. dataansvarlige eller databehandlere, der er omfattet af databeskyttelsesforordningen for den pågældende behandling[13]) til at overføre personoplysninger til certificerede dataimportører, som ikke er omfattet af databeskyttelsesforordningen i henhold til artikel 3[14]. Det betyder, at overførsel af personoplysninger til dataimportøren i tredjelandet først kan finde sted, når den pågældende importør er blevet certificeret og har underskrevet bindende tilsagn, som kan håndhæves, over for EØS-dataeksportøren, om at anvende de fornødne garantier, der er fastsat i certificeringskriterierne, ved behandling af de overførte personoplysninger inden for den evaluerede mekanismes anvendelsesområde, herunder for så vidt angår registreredes rettigheder.

26 I forbindelse med denne udtalelse og med henblik på at godkende Europrivacy-certificeringskriterierne, som skal anvendes som et redskab til overførsler, har Databeskyttelsesrådet vurderet de indledende kontroller vedrørende ansøgningen og den evaluerede mekanisme for dataimportører (ADI), Europrivacy-kernekriterierne vedrørende databeskyttelsesforordningen for dataimportører (GI) og kontrol af tekniske og organisatoriske foranstaltninger (T).

27 Med hensyn til certificeringsprocessen fremhæver Databeskyttelsesrådet i lyset af den særlige karakter af certificering, der skal anvendes som et redskab til overførsler, behovet for stor gennemsigtighed og glæder sig over de præciseringer, der i denne forbindelse gives i Europrivacy-certificeringsordningen, hvorefter "overførsler ikke kan påbegyndes, før certificeringen er udstedt". I den forbindelse noterer Databeskyttelsesrådet sig, at før overførslen af personoplysninger finder sted, kan "vurderingen foretages med personoplysninger, der ikke er omfattet af databeskyttelsesforordningen, eller med data, der ikke er personoplysninger. Hvor det er nødvendigt, kan der anvendes fiktive data til at vurdere specifikke kriterier", og at "auditøren, når overførslen af personoplysninger er påbegyndt, skal foretage en fornyet vurdering af disse kriterier ved den efterfølgende tilsynskontrol"[15].

[12] Se navnlig afsnit 3 og 4 i retningslinjer 07/2022.
[13] Se retningslinjer 05/2021 om samspillet mellem anvendelsen af artikel 3 og bestemmelserne om internationale overførsler i henhold til kapitel V i GDPR, version 2.0, vedtaget den 14. februar 2023, punkt 9.
[14] Databeskyttelsesforordningens artikel 42, stk. 2.
[15] Se Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR, EP-CS.1.DI, afsnit 6.1.

28 Databeskyttelsesrådet minder om, at det kan være nødvendigt at foretage visse tilpasninger af akkrediteringen af certificeringsorganer for så vidt angår certificering, der anvendes som et redskab til overførsler, i overensstemmelse med retningslinjerne om certificering som et redskab til overførsler16. Denne udtalelse behandler imidlertid ikke dette spørgsmål, da det ikke henhører under Databeskyttelsesrådets kompetence.

29 Databeskyttelsesrådet minder også om, at certificeringskriterierne skal gøres tilgængelige i overensstemmelse med databeskyttelsesforordningens artikel 42, stk. 8, og, navnlig når certificering skal anvendes som et redskab til overførsler, i overensstemmelse med databeskyttelsesforordningens artikel 13, stk. 1, litra f), for de registrerede, hvis personoplysninger vil blive overført på grundlag af den certificering, der er udstedt til dataimportøren.

30 Databeskyttelsesrådet bemærker, således som det er præciseret i ordningens definitioner, at henvisninger til "kompetente databeskyttelsesmyndigheder" i hele ordningen skal forstås som henvisninger til databeskyttelsesmyndigheder i EØS17.

31 Samtidig bemærker Databeskyttelsesrådet, at henvisninger til "gældende lovgivning" og "tredjelandes lovgivning" betyder den lovgivning, der finder anvendelse på ansøgeren og/eller på de personoplysninger, der behandles i den evaluerede mekanisme, for så vidt som denne lovgivning ikke pålægger begrænsninger af databeskyttelsesrettighederne, som går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at beskytte et af de mål, der er anført i databeskyttelsesforordningens artikel 23, stk. 1, står i et rimeligt forhold til det forfulgte mål, respekterer det væsentlige indhold af retten til databeskyttelse og sikrer specifikke foranstaltninger til beskyttelse af de registreredes grundlæggende rettigheder og interesser.

2.1 Certificeringsmekanismens anvendelsesområde og evalueret mekanisme

32 Udvidelsen af Europrivacy-certificeringsordningen for certificering af dataimportører i henhold til artikel 46 er beregnet til at blive anvendt i henhold til databeskyttelsesforordningens artikel 42, stk. 2, og artikel 46, stk. 2, litra f), af dataimportører, der er etableret uden for EØS, og som ikke er omfattet af databeskyttelsesforordningen i henhold til artikel 3, med henblik på at påvise, at der findes fornødne garantier inden for rammerne af overførsel af personoplysninger til tredjelande eller internationale organisationer. Således adskiller dens anvendelsesområde sig fra anvendelsesområdet for den Europrivacy-certificering efter artikel 42, stk. 1, som er omhandlet i punkt 3 i denne udtalelse, idet den fastsætter specifikke kriterier, der skal anvendes og overholdes, når en Europrivacy-certificering udstedes til ansøgere (dataansvarlige eller databehandlere), der er etableret uden for EØS og skal fungere som dataimportører.

33 Europrivacy-certificeringsordningen som et redskab til overførsler er en ordning, der er beregnet til at blive anvendt på såvel en enkelt overførsel som en række overførsler, når

[16] Retningslinjer 07/2022, afsnit 2.

[17] Se den definition af "kompetent tilsynsmyndighed", der er fastsat i Europrivacy-kriterierne: "*"Kompetent databeskyttelsesmyndighed" henviser til databeskyttelsesmyndigheder i EØS. Overordnet set henviser det til de nationale databeskyttelsesmyndigheder, der har kompetence til at håndhæve overholdelsen af reglerne for de personoplysninger, der behandles af den evaluerede mekanisme. Når der er tale om en certificering i henhold til databeskyttelsesforordningen, der er udstedt til en dataimportør i henhold til databeskyttelsesforordningens artikel 46, er den kompetente databeskyttelsesmyndighed den myndighed i EØS, der er kompetent for dataeksportøren, bortset fra ved indgivelse af en klage, hvor enhver myndighed i EØS er kompetent*".

sidstnævnte er nært forbundne. Certificeringsordningen indeholder certificeringskriterier for behandlingsaktiviteter inden for den evaluerede mekanisme, som udføres på personoplysninger, der overføres til dataimportøren, herunder transit, når denne er under den samme importørs kontrol[18].

34 Databeskyttelsesrådet bemærker, at denne certificeringsordnings anvendelsesområde ikke omfatter fælles dataansvarlige, og at hvis "fælles dataansvar" indgår i den evaluerede mekanisme, skal certificeringsorganet afslå at udstede certificering[19].

2.2 Behandlingsaktiviteter

35 Certificeringskriterierne omhandler de relevante elementer i de behandlingsaktiviteter, der udføres på de personoplysninger, som er omfattet af den evaluerede mekanisme. Certificeringskriterierne indeholder navnlig beskyttelsesforanstaltninger for behandling af særlige kategorier af personoplysninger (afsnit GI.2 i kriterierne om behandling af særlige kategorier af personoplysninger). Databeskyttelsesrådet hilser i den forbindelse velkommen, at certificeringskriterierne (kriterium GI.2.1.3 om yderligere beskyttelsesforanstaltninger ved behandling af særlige kategorier af personoplysninger) kræver, at ansøgeren har etableret yderligere begrænsninger og beskyttelsesforanstaltninger, der er tilpasset oplysningernes art og de dermed forbundne risici, når behandlingen omfatter særlige kategorier af personoplysninger.

2.3 Databehandlingsprincipper

36 I afsnit GI.1 behandler certificeringskriterierne på passende vis databeskyttelsesprincipperne i overensstemmelse med databeskyttelsesforordningens artikel 5 med det formål at sikre, at databehandlingen i den evaluerede mekanisme er lovlig og forholdsmæssig.

37 Navnlig er princippet om formålsbegrænsning og ansøgerens relevante forpligtelser med henblik på at overholde dette princip behørigt uddybet i certificeringskriterium GI.1.1.2. Databeskyttelsesrådet bemærker, at overførte personoplysninger kun må behandles til de formål, hvortil de er blevet overført. Certificeringskriterium GI.1.1.3 identificerer, i overensstemmelse med de gældende standardkontraktbestemmelser, som Kommissionen har vedtaget[20], de eneste undtagelser, hvor personoplysninger kan viderebehandles til andre formål end dem, hvortil de oprindeligt blev indsamlet (dvs. forudgående informeret samtykke, retlig forpligtelse, de registreredes vitale interesser og retskrav).

38 Databeskyttelsesrådet bemærker desuden, at ansøgeren skal fremlægge en skriftlig vurdering for at sikre, at lovgivning og praksis i tredjelandet ikke hindrer ansøgeren i at overholde Europrivacy-kriterierne, at de respekterer kernen i de registreredes grundlæggende rettigheder og friheder, og at de ikke går videre end, hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at beskytte et af de mål, der er anført i databeskyttelsesforordningens artikel 23, stk. 1. Den certificerede enhed skal revidere vurderingen, hver gang lovgivningsmæssige eller organisatoriske ændringer kan hindre overholdelsen af kriterierne eller påvirke den evaluerede mekanisme eller de registreredes rettigheder, og certificeringsorganet skal underrettes (kriterium GI 1.1.1).

[18] Se certificeringskriterierne GI.11.1.5 og GI.11.1.6.
[19] Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR, EP-CS.1.DI, afsnit 3.2.2., hvor det også klart fremgår, at fælles dataansvar er udelukket fra ordningens anvendelsesområde for ansøgere efter artikel 46.
[20] Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679.

2.4 Dataansvarliges og databehandleres generelle forpligtelser

39 Certificeringskriterierne afspejler den dataansvarliges forpligtelser i henhold til databeskyttelsesforordningens artikel 24 (afsnit GI.4 i kriterierne) og kræver en vurdering af de kontraktmæssige aftaler mellem databehandler og dataansvarlig i overensstemmelse med databeskyttelsesforordningens artikel 28 (afsnit GI.5 i certificeringskriterierne om databehandlere eller underdatabehandlere) med det formål at sikre, at de databehandlere, der deltager i databehandlingen i den evaluerede mekanisme, sikrer samme databeskyttelsesniveau som det, der kræves i Europrivacy-kriterierne. I den forbindelse glæder Databeskyttelsesrådet sig over de forskellige certificeringskriterier vedrørende anvendelsen af underdatabehandlere for ansøgere, der optræder som dataansvarlige eller som databehandlere, da denne sondring gør det muligt bedre at afspejle adskillelsen af roller og ansvar mellem aktørerne i behandlingskæden (afsnit GI.5.1).

40 Certificeringskriterierne kræver, at alle ansøgere udpeger en databeskyttelsesrådgiver, selv i tilfælde hvor ansøgeren ikke er forpligtet til at udpege en databeskyttelsesrådgiver i henhold til databeskyttelsesforordningens artikel 37. Certificeringskriterierne omfatter en kontrol af, at databeskyttelsesrådgiveren opfylder de samme krav som dem, der er fastsat i artikel 37-39 (afsnit GI.9 i certificeringskriterierne om udpegelse af en databeskyttelsesrådgiver), for at sikre, at den databeskyttelsesrådgiver, der fører tilsyn med overholdelsen af databehandlingen i den evaluerede mekanisme, med hensyn til rolle, funktion og kvalifikationer opfylder de "nødvendige krav". I den forbindelse bemærker Databeskyttelsesrådet, at udpegelsen af en databeskyttelsesrådgiver ikke er en obligatorisk forpligtelse for dataansvarlige og databehandlere i henhold til databeskyttelsesforordningen, medmindre betingelserne i databeskyttelsesforordningens artikel 37, stk. 1, er opfyldt.

41 Certificeringskriterierne kræver, at indholdet af fortegnelserne over aktiviteter kontrolleres i overensstemmelse med databeskyttelsesforordningens artikel 30 (afsnit GI.5.3 i kriterierne om fortegnelser over behandlingsaktiviteter). I den forbindelse glæder Databeskyttelsesrådet sig over, at certificeringskriterierne klart kræver, at ansøgerne samarbejder med de databeskyttelsesmyndigheder i EØS, der er kompetente for eksportørerne, når disse fremsætter anmodninger, og efter anmodning stiller fortegnelsen over behandlingsaktiviteter til rådighed for dem (kriterium GI.5.3.5).

2.5 De registreredes rettigheder

42 Certificeringskriterierne omfatter de registreredes rettigheder i overensstemmelse med databeskyttelsesforordningens kapitel III og kræver, at der træffes relevante foranstaltninger med det formål at sikre, at behandlingen i den evaluerede mekanisme respekterer og muliggør en effektiv udøvelse af de registreredes rettigheder. Afsnit GI.3 i certificeringskriterierne om gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder foreskriver bl.a., at registrerede har ret til at blive informeret om behandlingen af personoplysninger og om, hvordan de kan udøve deres rettigheder. Databeskyttelsesrådet glæder sig navnlig over, at certificeringskriterierne fastsætter, at ansøgeren skal have procedurer eller en mekanisme på plads til at håndtere anmodninger fra registrerede og, hvis der ikke træffes foranstaltninger i anledning af den registreredes anmodning, underrette vedkommende om årsagerne til, at der ikke træffes foranstaltninger, om muligheden for at indgive en klage til en databeskyttelsesmyndighed i EØS og om muligheden for at indbringe sagen for en retsinstans.

2.6 Tekniske og organisatoriske foranstaltninger og vurdering af risiciene for de registreredes rettigheder og friheder

43 Certificeringskriterierne kræver, at der anvendes tekniske og organisatoriske foranstaltninger, som påviser et sikkerhedsniveau, der er passende i forhold til risikoen ved behandlingen, og gennemfører databeskyttelse gennem design og standardindstillinger i henhold til databeskyttelsesforordningens artikel 25 og 32 (afsnit GI.6 i certificeringskriterierne om databeskyttelse gennem design og gennem standardindstillinger og behandlingssikkerhed), med det formål at sikre, at de oplysninger, der behandles inden for den evaluerede mekanisme, har et passende sikkerhedsniveau og er omfattet af databeskyttelse gennem design og gennem standardindstillinger. Herudover indeholder certificeringskriterierne et afsnit (dvs. kriterium T om kontroller af teknologiske og organisatoriske foranstaltninger), hvor tekniske og organisatoriske foranstaltninger behandles nærmere.

44 Certificeringskriterierne kræver, at der anvendes foranstaltninger til at sikre, at anmeldelsespligter om brud på persondatasikkerheden udføres rettidigt og omfangsmæssigt i overensstemmelse med databeskyttelsesforordningens artikel 33 og 34 (afsnit GI.7 i kriterierne om håndtering af brud på persondatasikkerheden).

45 I den forbindelse bemærker Databeskyttelsesrådet, at certificeringskriterierne indeholder en detaljeret liste (kriterium GI.7.1.1. om pligten til at dokumentere brud på persondatasikkerheden) over de oplysninger, som ansøgeren skal dokumentere, når der sker et brud på persondatasikkerheden (f.eks. de kategorier af personoplysninger, der er eller kan være berørt, det omtrentlige antal registrerede, der er eller kan være berørt, kategorierne af og det omtrentlige antal registreringer af personoplysninger, som det vedrører eller kan vedrøre, samt de sandsynlige konsekvenser af bruddet på persondatasikkerheden). Desuden glæder Databeskyttelsesrådet sig over, at certificeringskriterierne klart fastsætter, at ansøgeren, når et brud på persondatasikkerheden sandsynligvis vil indebære en risiko for fysiske personers rettigheder og frihedsrettigheder, skal have regler, en procedure eller en mekanisme til at underrette den databeskyttelsesmyndighed i EØS, der er kompetent for eksportøren eller eksportørerne, og de registrerede i overensstemmelse med kravene i databeskyttelsesforordningens artikel 33 og 34 (kriterium GI.7.1.2 om den dataansvarliges pligt til at anmelde og underrette om brud på persondatasikkerheden og GI 7.2 om underretning om brud på persondatasikkerheden til den registrerede).

46 Databeskyttelsesrådet glæder sig også over, at certificeringskriterierne kræver, at risikoen for fysiske personers rettigheder og friheder i forbindelse med den databehandling, som er omfattet af den evaluerede mekanisme, vurderes, og at den databeskyttelsesmyndighed i EØS, der er kompetent for eksportøren eller eksportørerne, inddrages i overensstemmelse med databeskyttelsesforordningens artikel 35 (afsnit GI.8 i certificeringskriterierne om pligten til at vurdere, om der kræves en konsekvensanalyse vedrørende databeskyttelse (DPIA)).

2.7 Kriterier med henblik på at påvise tilstedeværelse af fornødne garantier for overførsel af personoplysninger

47 Certificeringskriterierne kræver, at alle overførsler af persondata til tredjelande og til internationale organisationer, der er omfattet af den evaluerede mekanisme, identificeres, og at valget med hensyn til overførselsmekanismen, som giver fornødne garantier som svarer til dem i databeskyttelsesforordningens kapitel V, underbygges i henhold til (afsnit GI.10 om overførsel af personoplysninger til tredjelande eller internationale organisationer). Databeskyttelsesrådet anerkender, at disse certificeringskriterier vil finde anvendelse i tilfælde af "videreoverførsler" af personoplysninger, der er omfattet af den evaluerede mekanisme, til

det samme tredjeland, hvor ansøgeren er etableret eller til et andet tredjeland. Databeskyttelsesrådet glæder sig over, at disse certificeringskriterier specifikt kræver, at ansøgeren skal have en klar kortlægning eller registrering af alle strømme af personoplysninger, der er omfattet af den evaluerede mekanisme, samt af identificerede overførsler til tredjelande og internationale organisationer, og anvende det passende grundlag for overførsel af personoplysninger i overensstemmelse med databeskyttelsesforordningens kapitel V under hensyntagen til forpligtelsen til ikke at underminere det beskyttelsesniveau for personoplysninger, der sikres inden for EØS.

48 Databeskyttelsesrådet bemærker også, at certificeringskriterierne kræver, at ansøgeren har gennemført en konsekvensanalyse vedrørende overførsel af personoplysninger og, hvor det er nødvendigt, truffet supplerende foranstaltninger for at sikre, at beskyttelsesniveauet for de overførte personoplysninger ikke undermineres (kriterium GI.10.1.5).

3 Yderligere kriterier for europæisk databeskyttelsesmærkning, der skal anvendes som et redskab til overførsler

49 Ifølge retningslinjerne om certificering som et redskab til overførsler bør certificeringsordningen sikre, at dataimportøren "har vurderet reglerne og praksisserne i det tredjeland, hvor den opererer, og om de forhindrer importøren i at overholde sine forpligtelser i henhold til certificeringen". I denne forbindelse bemærker Databeskyttelsesrådet, at kriterium ADI.2.1.5 fastsætter betingelser, som ansøgerne skal opfylde ved fastlæggelsen af den evaluerede mekanisme under gennemgangen af deres certificeringsansøgning. Det kræver navnlig, at certificeringsorganet, inden det tager en certificeringskontrol op til overvejelse, kontrollerer, at ansøgeren kan godtgøre, at lovgivningen og praksis i det pågældende tredjeland ikke hindrer ansøgerens overholdelse af certificeringskravene. Hvis dette ikke er tilfældet, standses certificeringsprocessen i ansøgningsfasen.

50 Databeskyttelsesrådet bemærker også, at ansøgeren i henhold til kriterium GI.11.1.3 bør analysere lovgivningen og praksis i tredjelandet og identificere den potentielle indvirkning på de registreredes rettigheder og friheder, hvis oplysninger kan importeres, samt have "regler, procedurer eller politikker, der sikrer, at ansøgerens skriftlige analyse af den lokale lovgivning og praksis stilles til rådighed for certificeringsorganet og de kompetente databeskyttelsesmyndigheder efter anmodning".

51 Desuden fastsætter certificeringskriterierne, som anført i retningslinjerne om certificering som et redskab til overførsler, at ansøgeren, hvor det er nødvendigt, skal have truffet supplerende foranstaltninger for at sikre, at beskyttelsesniveauet for de overførte personoplysninger ikke undermineres, og at dataimportøren, hvis dette ikke er muligt, skal underrette dataeksportøren, og at overførslen af personoplysninger bør suspenderes eller standses (kriterium GI 11.1.3).

52 Databeskyttelsesrådet bemærker endvidere, at Europrivacy-ordningen i overensstemmelse med databeskyttelsesforordningens artikel 42, stk. 2, fastsætter, at der, inden enhver overførsel finder sted, skal underskrives en kontrakt mellem dataimportøren og dataeksportøren, der indeholder de relevante bindende tilsagn, som kan håndhæves, og at ordningen indeholder en skabelon for en sådan kontrakt. I den forbindelse noterer Databeskyttelsesrådet sig, at certificeringskriterierne i overensstemmelse med retningslinjerne om certificering som et redskab til overførsler indeholder en detaljeret liste over indholdet af de bindende tilsagn, som kan håndhæves, og som ansøgeren skal påtage

sig over for hver eksportør i EØS, herunder forpligtelsen til at anerkende de registrerede som begunstigede tredjemænd med ret til over for den dataimportør, der er indehaver af en certificering, at håndhæve reglerne i certificeringen, til at samarbejde med de databeskyttelsesmyndigheder i EØS, der er kompetente for dataeksportørerne (herunder ved at acceptere deres kontroller og inspektioner, tage hensyn til deres rådgivning og efterkomme deres afgørelser), til at efterkomme enhver bindende afgørelse vedrørende certificeringen, der træffes inden for EØS-medlemsstaternes jurisdiktion, herunder af deres domstole, kun at behandle de modtagne oplysninger, så længe certifikatet er gyldigt, og at returnere og/eller slette de modtagne oplysninger, hvis certifikatet trækkes tilbage. Certificeringskriterierne fastsætter også, at ansøgeren bør garantere, at den ikke har grund til at tro, at lovgivningen og praksis i det tredjeland, der finder anvendelse på behandlingen inden for den evaluerede mekanisme, herunder eventuelle krav om at udlevere personoplysninger eller foranstaltninger, der giver offentlige myndigheder adgang, hindrer den i at opfylde sine forpligtelser i henhold til certificeringen, og at den underretter dataeksportøren om enhver relevant ændring i lovgivningen eller praksis i denne henseende (kriterium GI.11.1.1 om bindende tilsagn, som kan håndhæves, for dataimportører).

4 Konklusioner/anbefalinger

53 Sammenfattende er det Databeskyttelsesrådets opfattelse, at Europrivacy-certificeringskriterierne, som skal anvendes som et redskab til overførsler, er i overensstemmelse med databeskyttelsesforordningen, og de godkendes i henhold til Databeskyttelsesrådets opgave som defineret i databeskyttelsesforordningens artikel 70, stk. 1, litra o), hvilket medfører en fælles certificering (den europæiske databeskyttelsesmærkning), som skal anvendes som et redskab til overførsler.

54 Databeskyttelsesrådet anser certificeringskriterierne for at udgøre en integreret del af certificeringsordningen og vil registrere Europrivacy-certificeringsordningen i det offentlige register over certificeringsmekanismer og databeskyttelsesmærkninger og -mærker og gøre kriterierne offentligt tilgængelige i henhold til databeskyttelsesforordningens artikel 42, stk. 8.

5 Afsluttende bemærkninger

55 Denne udtalelse er rettet til den luxembourgske tilsynsmyndighed og offentliggøres i henhold til databeskyttelsesforordningens artikel 64, stk. 5, litra b).

På vegne af Det Europæiske Databeskyttelsesråd

Formanden

Anu Talus