Yttrande 14/2026 om certifieringskriterierna i Europrivacy-systemet angående styrelsens godkännande av dem som europeiskt sigill för dataskydd enligt artikel 42.5 i den allmänna dataskyddsförordningen

Antaget den 15 April 2026

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande yttrande

med beaktande av artiklarna 63, 64.2 och 42 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*den allmänna dataskyddsförordningen*),

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet (*EES*), särskilt bilaga XI och protokoll 37, i dess lydelse enligt gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 10 och 22 i arbetsordningen, och

av följande skäl:

1. Medlemsstaterna, tillsynsmyndigheterna, Europeiska dataskyddsstyrelsen (*EDPB* eller *styrelsen*) och Europeiska kommissionen ska, särskilt på unionsnivå, uppmuntra införandet av certifieringsmekanismer för dataskydd (*certifieringsmekanismer*) samt sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas och personuppgiftsbiträdens behandling är förenlig med den allmänna dataskyddsförordningen, med beaktande av de särskilda behoven hos mikroföretag samt små och medelstora företag. Införandet av certifieringsmekanismer kan även öka öppenheten och ge de registrerade möjlighet att bedöma nivån på relevanta produkters och tjänsters dataskydd.
2. Certifieringskriterierna utgör en integrerad del av en certifieringsmekanism. Följaktligen kräver dataskyddsförordningen att kriterierna för en nationell certifieringsmekanism godkänns av den behöriga tillsynsmyndigheten (artiklarna 42.5 och 43.2 b i dataskyddsförordningen), eller, i fråga om ett europeiskt sigill för dataskydd, av EDPB (artiklarna 42.5 och 70.1 o i dataskyddsförordningen).
3. När en tillsynsmyndighet avser att föreslå att EDPB ska godkänna ett europeiskt sigill för dataskydd i enlighet med artikel 42.5 i dataskyddsförordningen, bör tillsynsmyndigheten ange att den systemansvarige har för avsikt att erbjuda certifieringsmekanismen i alla medlemsstater. I detta fall är EDPB:s huvudsakliga roll att säkerställa en konsekvent tillämpning av dataskyddsförordningen genom den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 i dataskyddsförordningen. Inom denna ram godkänner EDPB certifieringskriterierna enligt artikel 64.2 i dataskyddsförordningen.
4. Syftet med detta yttrande är att säkerställa en konsekvent tillämpning av dataskyddsförordningen, däribland av tillsynsmyndigheter, personuppgiftsansvariga och personuppgiftsbiträden, med hänsyn till de centrala inslag som certifieringsmekanismerna måste inbegripa. EDPB:s bedömning utförs särskilt på grundval av riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen (*riktlinjerna*) och deras tillägg med vägledning om bedömning av certifieringskriterier (*Guidance on certification criteria assessment*, nedan *tillägget*), för vilka det offentliga samrådet avslutades den 26 maj 2021.
5. Följaktligen konstaterar EDPB att varje certifieringsmekanism bör behandlas enskilt och utan att det påverkar bedömningen av andra certifieringsmekanismer.
6. Certifieringsmekanismer bör ge personuppgiftsansvariga och personuppgiftsbiträden möjlighet att visa att de följer den allmänna dataskyddsförordningen. Därför bör mekanismernas kriterier återspegla de krav och principer för skydd av personuppgifter som fastställs i den allmänna dataskyddsförordningen och bidra till dess enhetliga tillämpning.

[1] Hänvisningar till ”medlemsstater” i detta dokument ska tolkas som hänvisningar till ”medlemsstater i EES”.

7. Samtidigt bör den systemansvarige säkerställa att certifieringsmekanismen är anpassad till och förenlig med varje ISO-standard och certifieringsförfarande som ingår eller används.

8. Således bör certifieringar skapa mervärde för personuppgiftsansvariga och personuppgiftsbiträden genom att bidra till genomförandet av standardiserade och specificerade organisatoriska och tekniska åtgärder som bevisligen underlättar och förbättrar behandlingens överensstämmelse med den allmänna dataskyddsförordningen, med beaktande av sektorsspecifika krav.

9. EDPB välkomnar de ansträngningar som gjorts av systemansvariga för att utveckla certifieringsmekanismerna till praktiska och potentiellt kostnadseffektiva verktyg som säkerställer en bättre överensstämmelse med den allmänna dataskyddsförordningen och främjar de registrerades rätt till integritet och uppgiftsskydd genom att öka öppenheten.

10. EDPB erinrar om att certifieringar är frivilliga verktyg för ansvarsskyldighet och att anslutningen till en certifieringsmekanism varken minskar de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar att uppfylla kraven i den allmänna dataskyddsförordningen eller hindrar tillsynsmyndigheterna att utöva sina uppgifter och befogenheter enligt den allmänna dataskyddsförordningen och den relevanta nationella lagstiftningen.

11. I detta yttrande behandlar EDPB ett antal olika frågor, däribland kriteriernas tillämpningsområde och deras tillämplighet och relevans i alla medlemsstater.

12. Detta yttrande av EDPB är enbart inriktat på certifieringskriterierna. För att kunna göra en grundlig bedömning av möjligheten att granska kriterierna kan EDPB komma att begära information på hög nivå om utvärderingsmetoderna. Detta omfattar dock ingen form av godkännande av dessa utvärderingsmetoder.

13. EDPB:s yttrande ska antas i enlighet med artikel 64.2 i den allmänna dataskyddsförordningen, jämförd med artikel 10.2 i styrelsens arbetsordning, inom åtta veckor från den första arbetsdagen efter det att ordföranden och den behöriga tillsynsmyndigheten har fastställt att handlingarna i ärendet är fullständiga. Ordföranden får besluta att förlänga denna period med ytterligare sex veckor med hänsyn till sakfrågans komplexitet. Om EDPB i sitt yttrande drar slutsatsen att kriterierna inte kan godkännas får tillsynsmyndigheten lämna in kriterierna för godkännande på nytt när åtgärder har vidtagits med anledning av de betänkligheter som uttrycks i EDPB:s första yttrande.

Härigenom antas följande:

1 Sammanfattning av sakförhållandena

14. I enlighet med artikel 42.5 i den allmänna dataskyddsförordningen och riktlinjerna utarbetades certifieringskriterierna för Europrivacy (version 82) (*certifieringskriterierna*) av European Center for Certification and Privacy (*den systemansvarige*).

15. Tillsynsmyndigheten i Luxemburg lämnade in Europrivacy-systemets certifieringskriterier (version 82) till EDPB den 29 januari 2026 för godkännande i enlighet med artikel 64.2 i den allmänna dataskyddsförordningen.

16. Beslutet om att handlingarna i ärendet var fullständiga fattades den 31 mars 2026.

17. EDPB erinrar om att den godkände Europrivacy-systemets certifieringskriterier (version 60) som europeiskt sigill för dataskydd den 10 oktober 2022 genom sitt yttrande 28/2022 i enlighet med artikel 42.5 i dataskyddsförordningen (*EDPB:s tidigare yttrande*).

18. I detta yttrande behandlas den ändrade versionen av Europrivacy-systemets certifieringskriterier (version 82). För det första noterar styrelsen att tillämpningsområdet i denna version av certifieringskriterierna, som nyligen lämnats in till EDPB, har utvidgats till att omfatta sökande som omfattas av artikel 3.2 i den allmänna dataskyddsförordningen och att ett kriterium om potentiell konflikt mellan tredjeländers lagstiftning har införts i detta avseende. Dessutom noterar styrelsen att vissa av de certifieringskriterier som godkändes av EDPB 2022 har justerats, anpassats och/eller förtydligats i den ändrade versionen av Europrivacy-systemets certifieringskriterier (version 82). Dessa ändringar gäller särskilt följande: Utnämningen av en företrädare i EES och samarbetet i samband med begäranden från behöriga dataskyddsmyndigheter i EES. Utvärderingsrapporten om efterlevnaden av nationella skyldigheter (*National Obligations Compliance Assessment Report*, Nocar), den ytterligare behandlingen, de skyddsåtgärder som åtföljer behandlingen av särskilda kategorier av personuppgifter, de registrerades rättigheter, deltagandet av underentreprenörer, hanteringen av personuppgiftsincidenter, riskbedömningen för databehandlingen samt säkerhetspolicyn och säkerhetskraven.

19. EDPB understryker att ändringen av de certifieringskriterier som godkändes redan 2022 kommer att påverka såväl de certifieringar som hittills utfärdats som de pågående certifieringsprocesserna. Därför bör en övergångsperiod mellan de europeiska sigill för dataskydd som tillhandahållits i enlighet med de certifieringskriterier som godkändes genom EDPB:s tidigare yttrande (version 60) och de som utfärdats i enlighet med certifieringskriterierna (version 82), vilka bedöms i detta yttrande, hanteras på ett lämpligt och öppet sätt. I detta avseende gör styrelsen tolkningen, på grundval av den dokumentation som lämnats av den systemansvarige, att alla pågående certifieringsprocesser måste slutföras före utgången av 2026 och att de certifieringskriterier som godkändes i enlighet med EDPB:s tidigare yttrande (version 60) inte längre kommer att användas för att utfärda nya certifikat efter den tidpunkten. De certifikat som hittills har utfärdats kommer att fortsätta att vara giltiga fram till utgången av deras treåriga giltighetstid, varefter de kommer att förnyas enligt certifieringskriterierna (version 82). Efter utgången av 2029 kommer därför de certifieringskriterier som godkändes i enlighet med EDPB:s tidigare yttrande (version 60) att helt och hållet ersättas av certifieringskriterierna (version 82). Dessutom kommer informationen om denna övergångsplan att offentliggöras av den systemansvarige. Vissa ändringar kan behöva göras när det gäller ackrediteringen av certifieringsorganen, men denna fråga behandlas inte i detta yttrande eftersom den inte ingår i EDPB:s behörighet.

20. Det allmänna Europrivacy-certifieringssystemet är inte avsett att användas som ett verktyg för överföringar enligt artikel 42.2 och artikel 46 f i dataskyddsförordningen. Den 29 januari 2026 lämnade tillsynsmyndigheten i Luxemburg in ytterligare en uppsättning certifieringskriterier (”Extension of the Europrivacy Certification Scheme for Certification Data Importers under Article 46”) till EDPB för godkännande i enlighet med artikel 64.2 i den allmänna dataskyddsförordningen. Kriteriernas tillämpningsområde omfattar personuppgiftsansvariga och personuppgiftsbiträden utanför EES som inte direkt omfattas av den allmänna dataskyddsförordningen enligt artikel 3.2 i den allmänna dataskyddsförordningen, men som behandlar personuppgifter som tagits emot från en annan personuppgiftsansvarig eller ett annat personuppgiftsbiträde som omfattas av den allmänna dataskyddsförordningen. När det gäller denna uppsättning certifieringskriterier, vilka är avsedda att användas som verktyg för överföringar enligt artikel 46.2 f i den allmänna dataskyddsförordningen, har EDPB antagit yttrande 15/2026.

2 Bedömning

21. EDPB har utfört sin bedömning av certifieringskriterierna för deras godkännande enligt artikel 42.5 i den allmänna dataskyddsförordningen i överensstämmelse med det förfarande som föreskrivs i bilaga 2 till riktlinjerna (*bilagan*) och dess tillägg.

22. I samband med detta yttrande och för att godkänna certifieringskriterierna har EDPB bedömt tre aspekter av kriterierna, närmare bestämt de preliminära kontrollerna av tillämpning och evalueringsobjekt (A), de centrala kriterierna för Europrivacy-systemets överensstämmelse med den allmänna dataskyddsförordningen (G) och kontrollerna av tekniska och organisatoriska åtgärder (T), vilka föreskrivs vid sidan av certifieringskriterierna.

23. Vidare noterar styrelsen i detta avseende att de ”kompletterande kontextuella kontroller”[2] som föreskrivs vid sidan av de certifieringskriterier som godkändes i EDPB:s tidigare yttrande (version 60), och som syftar till att säkerställa att behandlingen av uppgifter som utförs av evalueringsobjektet uppfyller domänspecifika och teknikspecifika krav[3], inte godkändes av EDPB i dess tidigare yttrande och att sådana ”kompletterande kontextuella kontroller” inte längre finns med i den uppdaterade dokumentation som tillhandahållits inom ramen för detta yttrande.

24. Styrelsen noterar att hänvisningar till ”behöriga dataskyddsmyndigheter” i hela systemet ska tolkas som hänvisningar till dataskyddsmyndigheter i EES[4], vilket även klargörs i definitionerna av systemet.

25. När det gäller definitionerna av lagstiftningen i tredjeland tolkar styrelsen det som att de hänvisar till den lag som är tillämplig på sökanden och/eller till de personuppgifter som behandlas av evalueringsobjektet, i den mån lagstiftningen inte medför begränsningar av dataskyddsrättigheterna som går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda något av de mål som anges i artikel 23.1 i den allmänna dataskyddsförordningen, står i proportion till det eftersträvade målet, är förenligt med det väsentliga innehållet i rätten till dataskydd samt föreskriver särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

2.1 Certifieringsmekanismens tillämpningsområde och evalueringsobjektet

26. EDPB erinrar om[5] att Europrivacy-certifieringssystemet är ett allmänt system i den meningen att det är riktat till en rad olika behandlingar som utförs av personuppgiftsansvariga och personuppgiftsbiträden från olika verksamhetsområden.

[2] EDPB godkände inte de ”kompletterande kontextuella kontrollerna” i sitt tidigare yttrande.
[3] EDPB:s tidigare yttrande, punkterna 7 och 8.
[4] Se definitionen av *behörig tillsynsmyndighet* i Europrivacy-systemets kriterier: Med *behörig dataskyddsmyndighet* avses dataskyddsmyndigheter inom EES. Generellt sett avses de nationella dataskyddsmyndigheter som har behörighet att säkerställa att den behandling av personuppgifter som utförs av evalueringsobjektet uppfyller kraven. När det gäller en certifiering enligt den allmänna dataskyddsförordningen som lämnas till en uppgiftsinförare enligt artikel 46 i dataskyddsförordningen är den behöriga dataskyddsmyndigheten den myndighet som är behörig för uppgiftsutföraren i EES, utom vid inlämning av ett klagomål, då alla myndigheter i EES är behöriga.
[5] EDPB:s tidigare yttrande, punkt 6.

27. Styrelsen välkomnar att det ändrade Europrivacy-systemet, enligt den dokumentation om tillämpningsområdet för detta certifieringssystem som tillhandahållits av tillsynsmyndigheten i Luxemburg, gäller för **i)** personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet (EES), **ii)** personuppgiftsansvariga och personuppgiftsbiträden som är etablerade utanför EES och som omfattas av den allmänna dataskyddsförordningen i enlighet med artikel 3.2 i den allmänna dataskyddsförordningen, antingen på grund av att de erbjuder varor eller tjänster till registrerade i EES eller på grund av att de övervakar de registrerades beteende i EES[6]. Kriteriernas tillämplighet fastställs beroende på den sökandes roll och ansvarsområden.

28. När det gäller sökande enligt artikel 3.2 i den allmänna dataskyddsförordningen som är etablerade i ett tredjeland och som inte omfattas av ett beslut om adekvat skyddsnivå som inbegriper evalueringsobjektet fastställs i kriterium A.2.1.6 ett antal villkor som ska vara uppfyllda när evalueringsobjektet definieras i samband med omprövningen av deras ansökan om certifiering. Särskilt anges att certifieringsorganet, innan det överväger en certifieringsrevision, ska kontrollera att sökanden kan visa att nationell lagstiftning och praxis i tredjelandet inte hindrar sökanden från att uppfylla certifieringskraven. Om detta inte är fallet kommer certifieringsprocessen att avbrytas under ansökningsfasen.

29. Styrelsen noterar att en personuppgiftsansvarig kan lämna in ett evalueringsobjekt som omfattas av gemensamt personuppgiftsansvar till certifieringsprocessen i Europrivacy-systemet (kriterium A.2.1.5). I de fall då evalueringsobjektet omfattas av gemensamt personuppgiftsansvar vill styrelsen understryka att det ackrediterade certifieringsorganet kommer att behöva genomföra en noggrann ansökningsprocess för att säkerställa att evalueringsobjektet är meningsfullt och att sökanden har det fulla ansvaret för att evalueringsobjektet uppfyller alla skyldigheter i den allmänna dataskyddsförordningen som certifieringssystemet syftar till att påvisa. Följaktligen kan den överenskommelse som slutits mellan sökanden och andra personuppgiftsansvariga med anknytning till evalueringsobjektet när det gäller deras respektive ansvar för efterlevnaden av skyldigheterna enligt den allmänna dataskyddsförordningen – beroende på sammanhanget för evalueringsobjektets behandling – hindra sökanden från att uppfylla certifieringskriterierna.

2.2 Behandling

30. Som EDPB noterade i sitt tidigare yttrande omfattar certifieringskriterierna de relevanta delarna av behandlingen (data, system och behandling) med avseende på certifieringssystemets allmänna tillämpningsområde. Certifieringskriterierna gör framför allt att det går att identifiera särskilda kategorier av personuppgifter enligt definitionen i artikel 9 i den allmänna dataskyddsförordningen (avsnitt G.2 av kriterierna om särskild behandling av uppgifter).

2.3 Behandlingens laglighet

31. Som EDPB uppgav i sitt tidigare yttrande om de certifieringskriterier som redan godkänts (version 60) kräver certifieringskriterierna att lagligheten hos behandlingen av uppgifter för varje enskild behandling i evalueringsobjektet kontrolleras, liksom kraven på en rättslig grund i enlighet med artikel 6 i den allmänna dataskyddsförordningen (avsnitt G.1 i kriterierna om uppgiftsbehandlingens laglighet). Styrelsen välkomnar framför allt att de uppdaterade

[6] Se EDPB:s riktlinjer om den allmänna dataskyddsförordningens territoriella tillämpningsområde (artikel 3), version 2.1, antagna den 12 november 2019, avsnitt 2.

certifieringskriterierna ställer krav på att de registrerades samtycke ska omfatta varje ändamål med behandlingen och att återkallandet av samtycket inte får skada den registrerade.

32. Som konstateras i EDPB:s tidigare yttrande kräver certifieringskriterierna också att de särskilda kraven för de villkor enligt vilka behandling av särskilda kategorier av personuppgifter är tillåten enligt artikel 9.2 i den allmänna dataskyddsförordningen (avsnitt G.2.1 i kriterierna om särskild databehandling) kontrolleras och att ytterligare begränsningar och skyddsåtgärder för den registrerades rättigheter och friheter tillhandahålls. Enligt certifieringskriterierna ska även kraven i de villkor som fastställs i artikel 10 i den allmänna dataskyddsförordningen för behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott (avsnitt G.2.2 i kriterierna) kontrolleras i tillämpliga fall. I detta avseende välkomnar styrelsen även att sökanden enligt certifieringskriterierna (kriterium GI.2.1.3 om ytterligare skyddsåtgärder för behandling av särskilda kategorier av personuppgifter) ska ha infört ytterligare begränsningar och skyddsåtgärder som är anpassade till uppgifternas specifika karaktär och de medföljande riskerna när särskilda kategorier av personuppgifter berörs av behandlingen.

33. När det gäller sökande enligt artikel 3.2 i den allmänna dataskyddsförordningen som är etablerade i ett tredjeland som inte är föremål för ett beslut om adekvat skyddsnivå som inbegriper evalueringsobjektet innebär de uppdaterade certifieringskriterierna därtill att sökanden måste lämna in en rapport som utarbetats av en juridisk expert för att bedöma att tredjelandets nationella lagstiftning och praxis inte hindrar fullgörandet av dess dataskyddsskyldigheter enligt den allmänna dataskyddsförordningen. På samma sätt ska bedömningen omfatta en kontroll av att tredjelandets nationella lagstiftning inte innebär några begränsningar av rätten till dataskydd som går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda något av de mål som anges i artikel 23.1 i dataskyddsförordningen, står i proportion till det eftersträvade målet, är förenligt med det väsentliga innehållet i rätten till dataskydd samt föreskriver särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Detta måste även kontrolleras närhelst förändringar i lagstiftningen eller organisationen kan hindra uppfyllandet av kriterierna eller påverka evalueringsobjektet eller de registrerades rättigheter, och när certifieringsorganet bör underrättas (kriterium G.1.1.5).

34. I detta sammanhang klargör de uppdaterade certifieringskriterierna i vägledningen att om en sökande är etablerad utanför EES och omfattas av ett beslut om adekvat skyddsnivå som är relevant för den behandling som utförs i evalueringsobjektet kan efterlevnaden av detta krav visas genom en förenklad rapport. Enligt dessa kriterier bör rapporten innehålla en bedömning av huruvida beslutet om adekvat skyddsnivå är i kraft samt en dokumentation av skälen till att evalueringsobjektet omfattas av beslutet om adekvat skyddsnivå (kriterium G.1.1.5, led F).

2.4 Uppgiftsbehandlingens principer

35. EDPB erinrar om att certifieringskriterierna på ett tillfredsställande sätt följer dataskyddsprinciperna enligt artikel 5 i dataskyddsförordningen. Framför allt innebär de uppdaterade certifieringskriterierna att principen om ändamålsbegränsning utvidgas och vidareutvecklas, eftersom de omfattar ett särskilt kriterium som kräver att det kan bevisas att personuppgifterna inte behandlas ytterligare på ett sätt som är oförenligt med dessa ändamål och att all ytterligare behandling bör bedömas separat som laglig, samt att en bedömning av ändamålets förenlighet genomförs och vederbörligen dokumenteras för vidare behandling av uppgifterna (kriterium G.1.1.6).

2.5 Allmänna skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

36. EDPB påminner om att certifieringskriterierna [7] speglar den personuppgiftsansvariges skyldigheter enligt artikel 24 i den allmänna dataskyddsförordningen (G.4 om den personuppgiftsansvariges ansvar) och ställer krav på att avtalsmässiga överenskommelser mellan personuppgiftsansvariga och personuppgiftsbiträden utvärderas i enlighet med artikel 28 i den allmänna dataskyddsförordningen (avsnitt G.5 av kriterierna om personuppgiftsansvariga eller underentreprenörer).

37. Dessutom välkomnar styrelsen tillägget i certifieringskriterierna att sökanden enligt artikel 3.2 i den allmänna dataskyddsförordningen ska utse en myndighet eller en företrädare inom EES i enlighet med artikel 27 i den allmänna dataskyddsförordningen, vars kontaktuppgifter ska finnas tillgängliga på sökandens webbplats (kriterium G.4.1.4). Styrelsen noterar dessa certifieringskriterier och påminner om att detta inte alltid är en obligatorisk skyldighet för personuppgiftsansvariga och personuppgiftsbiträden enligt den allmänna dataskyddsförordningen, och att villkoren i artikel 27 i den allmänna dataskyddsförordningen därför ska beaktas.

38. Vidare noterar EDPB, såsom anges i dess tidigare yttrande, att alla sökande enligt certifieringskriterierna ska utse ett dataskyddsombud, även i de fall då sökanden inte är skyldig att utse ett dataskyddsombud enligt artikel 37 i den allmänna dataskyddsförordningen. Kriterierna används för att kontrollera att dataskyddsombudet uppfyller kraven enligt artiklarna 37–39 (avsnitt G.9 av kriterierna om dataskyddsombud).

39. På liknande sätt innehåller certifieringskriterierna ett krav på att kontrollera innehållet i registret över behandling, i enlighet med artikel 30 i den allmänna dataskyddsförordningen (avsnitt GI.5.3 i kriterierna om register över behandling). I detta avseende välkomnar styrelsen att de uppdaterade certifieringskriterierna för sökande enligt artikel 3.2 i den allmänna dataskyddsförordningen kräver att de samarbetar i samband med begäranden från de behöriga dataskyddsmyndigheterna i EES och på begäran gör uppgifter om behandlingen tillgängliga för dem (kriterium G.5.3.5).

40. Likaså noterar EDPB att vissa ytterligare certifieringskriterier har införts när det gäller anlitande av underentreprenörer för sökande som agerar som personuppgiftsansvariga eller som personuppgiftsbiträden (avsnitt G.5.1.2 om anlitande av underentreprenörer). Denna åtskillnad gör det möjligt att bättre återspegla uppdelningen av roller och ansvarsområden mellan aktörerna i behandlingskedjan.

2.6 De registrerades rättigheter

41. Liksom i sitt tidigare yttrande påminner EDPB om att certifieringskriterierna på ett tillfredsställande sätt omfattar den registrerades rätt till information i enlighet med kapitel III i den allmänna dataskyddsförordningen och ställer krav på att motsvarande åtgärder vidtas[8]. Certifieringskriterierna ställer även krav på åtgärder som gör det möjligt att ingripa i behandlingen för att skydda de registrerades rättigheter och möjliggöra korrigeringar, raderingar eller begränsningar (avsnitt G.3 av kriterierna om de registrerades rättigheter).

42. Dessutom välkomnar EDPB de förbättringar som gjorts i certifieringskriterierna när det gäller den information som ska lämnas till registrerade (avsnitt G 3.2 om information som ska

[7] EDPB:s tidigare yttrande, punkt 15.
[8] EDPB:s tidigare yttrande, punkt 19.

tillhandahållas när personuppgifter samlas in från den registrerade och avsnitt G.3.3 om information som ska tillhandahållas om personuppgifter inte har erhållits från den registrerade), formerna för kommunikation till registrerade [9] och för utövandet av de registrerades rättigheter [10] (avsnitt G 3.1 om transparent information, kommunikation och former för utövande av de registrerades rättigheter) samt rätten till tillgång (avsnitt G 3.4 om den registrerades rätt till tillgång), radering (avsnitt G.3.6 om rätten till radering av personuppgifter (”rätten att bli bortglömd”)), begränsning av behandling (kriterium G 3.7.1 om rätten till begränsning av behandling), anmälningsskyldigheten avseende rättelse eller radering av personuppgifter eller begränsning av behandling (kriterium G.3.8.2 om skyldigheten att informera registrerade om mottagare på begäran), rätten att invända (avsnitt G.3.10 om rätten att invända) och rätten att inte bli föremål för automatiserat individuellt beslutsfattande, inbegripet profilering (avsnitt G.3.11 om rätten att inte bli föremål för automatiserat individuellt beslutsfattande, inbegripet profilering).

2.7 Risker för rättigheter och friheter

43. EDPB fastslog redan i sitt tidigare yttrande att certifieringskriterierna omfattar krav på en bedömning av risken för fysiska personers rättigheter och friheter i samband med uppgiftsbehandlingen med anknytning till evalueringsobjektet i enlighet med artikel 35 i den allmänna dataskyddsförordningen (avsnitt G.8 i kriterierna om skyldigheten att bedöma behovet av en konsekvensbedömning avseende dataskydd)[11].

44. EDPB välkomnar de ändringar som gjorts i certifieringskriterierna för att föreskriva att den sökande med en repeterbar metod ska ha bedömt de risker med behandlingen som kan påverka fysiska personers rättigheter och friheter (avsnitt G.6.2.4 om riskbedömning för databehandling).

45. Dessutom välkomnar EDPB de ytterligare tillägg och närmare uppgifter som införts i certifieringskriterierna. EDPB noterar till exempel det tillägg som gjorts i processen för konsekvensbedömning avseende dataskydd i situationer där sökanden inte är skyldig att utföra en konsekvensbedömning avseende dataskydd (avsnitt G.8.2.1 om kraven i processen för konsekvensbedömning avseende dataskydd).

2.8 Tekniska och organisatoriska åtgärder för att garantera skydd

46. Som påpekas i EDPB:s tidigare yttrande ställer certifieringskriterierna krav på att tekniska och organisatoriska åtgärder tillämpas med avseende på behandlingens konfidentialitet, integritet och tillgänglighet. I kriterierna ställs även krav på tillämpning av tekniska åtgärder för att genomföra inbyggt dataskydd och dataskydd som standard i enlighet med artiklarna 25 och 32 i den allmänna dataskyddsförordningen (avsnitt G.6 i kriterierna om inbyggt dataskydd och dataskydd som standard samt säkerhet i samband med behandlingen, avsnitt G.6.2 om

[9] Till exempel innehåller kriterium G.3.1.1, om skyldigheten att informera på ett tydligt språk, ytterligare detaljer om den information om databehandlingen som sökanden ska tillhandahålla till den registrerade, vilket nu inbegriper att i) den bör tillhandahållas skriftligen eller på annat sätt, ii) den bör finnas tillgänglig på sökandens officiella språk och iii) den bör finnas tillgänglig på de berörda registrerades språk.

[10] Till exempel omfattar kriterium G.3.1.3, om att säkerställa korrekt hantering och registrering av registrerades rättigheter, numera krav på att sökanden även ska införa ett förfarande eller en mekanism för att bekräfta mottagandet av begäran till den registrerade och att föra register över den registrerades begäranden med datumet för mottagandet.

[11] EDPB:s tidigare yttrande, punkt 20.

kriterierna för säkerhet i samband med behandlingen samt avsnitt T om kriterierna)[12]. I detta avseende välkomnar styrelsen att de ändrade certifieringskriterierna har utarbetats ytterligare (avsnitt G.6.1.2 om dataminimering som standard) när det gäller de regler och förfaranden som sökanden ska tillämpa för att uppfylla dessa kriterier.

47. Som betonas i EDPB:s tidigare yttrande ställer certifieringskriterierna krav på att åtgärder tillämpas för att säkerställa att personuppgiftsincidenter anmäls i rätt tid och omfattning i enlighet med artiklarna 33 och 34 i den allmänna dataskyddsförordningen (avsnitt G.7 av kriterierna om hantering av personuppgiftsincidenter).

48. I detta avseende konstaterar styrelsen att certifieringskriterierna har förbättrats och utarbetats ytterligare. Närmare bestämt innehåller certifieringskriterierna nu en mer detaljerad förteckning (avsnitt G.7.1.1 om skyldigheten att dokumentera personuppgiftsincidenter) över den information som sökanden ska dokumentera när en personuppgiftsincident har inträffat (t.ex. vilka kategorier av personuppgifter som påverkas eller kan påverkas, det ungefärliga antalet registrerade som påverkas eller kan påverkas, vilka kategorier av personuppgifter som incidenten berör eller kan beröra och deras ungefärliga antal, de sannolika konsekvenserna av personuppgiftsincidenten).

2.9 Kriterier för att styrka förekomsten av lämpliga skyddsåtgärder vid överföring av personuppgifter

49. Som styrelsen bekräftade i sitt tidigare yttrande ställer certifieringskriterierna krav på att alla överföringar av personuppgifter till tredjeländer och till internationella organisationer som utförs av evalueringsobjektet ska identifieras och att det val som gjorts avseende den mekanism för överföring av uppgifter som säkerställer lämpliga skyddsåtgärder ska bekräftas enligt kapitel V i den allmänna dataskyddsförordningen (avsnitt G.10 om överföringar av personuppgifter till tredjeländer eller internationella organisationer).

50. EDPB konstaterar att dessa certifieringskriterier, för sökande som omfattas av artikel 3.2 i den allmänna dataskyddsförordningen, kommer att tillämpas både vid överföring av personuppgifter med anknytning till evalueringsobjektet till enheter i samma tredjeland där sökanden är etablerad eller i ett annat tredjeland.

51. Styrelsen välkomnar även att certifieringskriterierna för överföring av personuppgifter nu har utarbetats ytterligare för att tydliggöra sökandens skyldigheter i denna fråga (avsnitt G.10.1 om allmänna skyldigheter för internationella överföringar av personuppgifter till tredjeländer eller till internationella organisationer).

3 Ytterligare kriterier för ett europeiskt sigill för dataskydd

52. Enligt riktlinjerna ska bedömningen innefatta frågan om huruvida ”det i kriterierna [tas] hänsyn till medlemsstaternas lagstiftning eller scenarion för dataskydd”. Som bekräftades i EDPB:s tidigare yttrande ska sökanden, enligt avsnitt G.1.1.3 av certifieringskriterierna, tillhandahålla

[12] EDPB:s tidigare yttrande, punkt 21.

en sådan bedömning i en utvärderingsrapport om efterlevnaden av nationella skyldigheter (*National Obligations Compliance Assessment Report*, Nocar). Rapporten ska innehålla en bedömning av de nationella skyldigheter som är tillämpliga för evalueringsobjektet och dokumentera de åtgärder som vidtagits av sökanden för att uppfylla de tillämpliga reglerna och, i förekommande fall, de pågående korrigeringsåtgärderna. Sökanden ska inte använda den förteckning över viktiga kompletterande nationella krav som tillhandahållits av den systemansvarige för varje land som en uttömmande förteckning över nationella skyldigheter som är relevanta för evalueringsobjektet. Den vägledande förteckning över minimikrav på kompletterande kontroller som tillhandahållits av den systemansvarige utgör inte certifieringskriterier inom ramen för detta yttrande.

53. Styrelsen välkomnar de justeringar av Nocar-rapporten som gjorts i de uppdaterade kriterierna (avsnitt G.1.1.3 om bedömning av efterlevnaden av nationella skyldigheter). Framför allt klargörs det nu att sökanden bör dokumentera den bedömning som gjorts avseende databehandlingens överensstämmelse med de kompletterande nationella skyldigheterna för EES i fråga om skydd av personuppgifter som är tillämpliga på sökanden i en utvärderingsrapport om efterlevnaden av nationella skyldigheter (Nocar). I synnerhet bör Nocar-rapporten bland annat innehålla en tydlig identifiering av det evalueringsobjekt som har bedömts, en förteckning över identifierade kompletterande nationella dataskyddsskyldigheter för EES som är tillämpliga på evalueringsobjektet samt en utvärdering av evalueringsobjektets efterlevnad av de identifierade kompletterande nationella dataskyddsskyldigheterna för EES. Om sökanden är etablerad utanför EES och omfattas av artikel 3.2 i den allmänna dataskyddsförordningen anser styrelsen att de nationella dataskyddsskyldigheter för EES som är tillämpliga på evalueringsobjektet ska fastställas utifrån den plats där de registrerade till vilka sökanden erbjuder varor eller tjänster eller vars beteende övervakas befinner sig.

4 Slutsatser och rekommendationer

54. Sammanfattningsvis anser EDPB att Europrivacy-systemets certifieringskriterier är förenliga med den allmänna dataskyddsförordningen och godkänner dem i enlighet med den uppgift som styrelsen har enligt artikel 70.1 o i den allmänna dataskyddsförordningen, vilket leder till en gemensam certifiering (det europeiska sigillet för dataskydd).

55. EDPB anser att certifieringskriterierna utgör en integrerad del av certifieringssystemet och kommer att registrera Europrivacy-certifieringssystemet i det offentliga registret över certifieringsmekanismer och sigill och märkningar för dataskydd samt offentliggöra kriterierna i enlighet med artikel 42.8 i den allmänna dataskyddsförordningen.

5 Avslutande kommentarer

56. Detta yttrande riktar sig till tillsynsmyndigheten i Luxemburg och kommer att offentliggöras i enlighet med artikel 64.5 b i dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

Anu Talus