Yttrande 28/2022 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 10 oktober 2022

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

Europeiska dataskyddsstyrelsen har antagit detta 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 (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet (EES), särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1], och

med beaktande av artiklarna 10 och 22 i arbetsordningen.

(1) Medlemsstaterna, tillsynsmyndigheterna, Europeiska dataskyddsstyrelsen (nedan kallad *EDPB* eller *dataskyddsstyrelsen*) och Europeiska kommissionen ska, särskilt på unionsnivå, uppmuntra införandet av certifieringsmekanismer för dataskydd (nedan kallade *certifieringsmekanismer*) och 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.[2] Införandet av certifieringsmekanismer kan dessutom förbättra öppenheten och ge de registrerade möjlighet att bedöma nivån på relevanta produkters och tjänsters dataskydd.[3]

(2) Certifieringskriterierna utgör en integrerad del av en certifieringsmekanism. Enligt den allmänna dataskyddsförordningen ska kriterierna i en nationell certifieringsmekanism godkännas av den behöriga tillsynsmyndigheten (artiklarna 42.5 och 43.2 b i den allmänna dataskyddsförordningen) eller, när det gäller ett europeiskt sigill för dataskydd, av EDPB (artiklarna 42.5 och 70.1 o i den allmänna dataskyddsförordningen).

(3) Om en tillsynsmyndighet har för avsikt att föreslå att EDPB ska godkänna ett europeiskt sigill för dataskydd i enlighet med artikel 42.5 i den allmänna dataskyddsförordningen bör tillsynsmyndigheten uppge om den systemansvarige avser att erbjuda certifieringsmekanismen i alla medlemsstater. I sådana fall är EDPB:s huvudsakliga uppgift att säkerställa en enhetlig tillämpning av den allmänna dataskyddsförordningen genom den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 i den allmänna dataskyddsförordningen. Inom denna ram ska EDPB godkänna certifieringskriterierna enligt artikel 64.2 i den allmänna dataskyddsförordningen.

(4) Syftet med detta yttrande är att säkerställa en enhetlig tillämpning av den allmänna dataskyddsförordningen, inbegripet av tillsynsmyndigheter, personuppgiftsansvariga och personuppgiftsbiträden, mot bakgrund av de centrala delar som måste utvecklas för certifieringsmekanismerna. 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 (nedan kallade *riktlinjerna*) och deras tillägg med vägledning om bedömning av certifieringskriterier

[1] Hänvisningar till ”medlemsstater” som görs i hela detta yttrande ska förstås som hänvisningar till ”EES-medlemsstater”.
[2] Artikel 42.1 i den allmänna dataskyddsförordningen.
[3] Skäl 100 i den allmänna dataskyddsförordningen.

(*Guidance on certification criteria assessment*, nedan kallat *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.

(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) Yttrandet är inriktat på certifieringskriterierna. Om EDPB begär information på hög nivå om utvärderingsmetoderna för att kunna göra en grundlig bedömning av möjligheten att granska kriterierna i samband med sitt yttrande om dessa omfattar det sistnämnda inte någon 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 beslutat att handlingarna i ärendet är fullständiga. På beslut av ordföranden får denna period förlängas 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 FRAMFÖRS FÖLJANDE.

SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. I enlighet med artikel 42.5 i den allmänna dataskyddsförordningen och riktlinjerna utarbetades kriterierna för Europrivacy v.60 (nedan kallade *utkastet till certifieringskriterier*, *certifieringskriterierna* eller *kriterierna*) av European Center for Certification and Privacy (nedan kallad *den systemansvarige*).

2. Tillsynsmyndigheten i Luxemburg lämnade in Europrivacy-systemets certifieringskriterier till EDPB den 28 september 2022 för godkännande i enlighet med artikel 64.2 i den allmänna dataskyddsförordningen. Beslutet om att handlingarna i ärendet var fullständiga fattades den 28 september 2022.

3. Europrivacy-systemets certifieringsmekanism är inte en certifiering som är avsedd för internationella överföringar av personuppgifter enligt artikel 46.2 f i den allmänna dataskyddsförordningen och omfattar därför inte lämpliga skyddsåtgärder inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt de villkor som anges i artikel 46.2 f. Personuppgifter får endast överföras till ett tredjeland eller en internationell organisation om bestämmelserna i kapitel V i den allmänna dataskyddsförordningen efterlevs.

2 BEDÖMNING

4. 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 (nedan kallad *bilagan*) och dess tillägg.

5. EDPB noterar att vägledningen för genomförandet och de metoder för verifiering av certifieringsmekanismen som föreslås av den systemansvarige inte alltid är konsekventa i hela uppsättningen av kriterier. Till exempel föreskrivs i avsnitt T.2.3.2 att regler, riktlinjer, förfaranden eller mekanismer ska införas för att upptäcka och rapportera intrång (t.ex. ett system som övervakar nätverkstrafiken för att upptäcka misstänkt verksamhet och varnar om sådan verksamhet upptäcks), samtidigt som de föreslagna metoderna för verifiering avser kontroll- och penetrationstest (ett krav enligt avsnitt T.2.3.1). Även om sådana inkonsekvenser faller utanför bedömningens räckvidd understryker EDPB att de kan vara ett hinder för certifieringsorganets ackreditering om de inte åtgärdas av den systemansvarige.

2.1 Certifieringsmekanismens tillämpningsområde och evalueringsobjektet

6. Europrivacy-systemets certifieringsmekanism är ett allmänt system på så sätt att det är riktat till en rad olika behandlingar som utförs av personuppgiftsansvariga och personuppgiftsbiträden från olika verksamhetsområden. De viktigaste kriterierna i denna certifieringsmekanism utgörs av ”kärnkriterier” och ”kontroller av tekniska och organisatoriska åtgärder” avseende de tekniska och organisatoriska åtgärder som införts för att skydda de personuppgifter som behandlas. En uppsättning av kriterierna för ”kontroller av tekniska och organisatoriska åtgärder” är endast tillämplig om evalueringsobjektet behandlar särskilda kategorier av uppgifter, brottsrelaterade uppgifter eller minderårigas personuppgifter.

7. Dessutom omfattar kriterierna även ”kompletterande kontextuella kontroller” som syftar till att säkerställa att den behandling av uppgifter som evalueringsobjektet utför uppfyller de domänspecifika och teknikspecifika kraven. I en informativ matris som tillhandahållits av den systemansvarige beskrivs vilka kategorier av uppgiftsbehandling som varje uppsättning av ”kompletterande kontextuella kontroller” är tillämpliga på.

8. EDPB välkomnar allmänna system med specifika kriterier som kan anpassas till och göras tillämpliga för särskilda behandlingar eller verksamhetssektorer. EDPB vill emellertid även klargöra att fullständigheten hos kriterierna för specifika behandlingar inte behöver bedömas inom ramen för ett

allmänt system och att den därför inte har bedömts i samband med detta yttrande. Dessutom erinrar EDPB om att de dokument som dataskyddsstyrelsen offentliggör med avseende på specifika behandlingar ska beaktas av den systemansvarige och de ackrediterade certifieringsorganen.

9. De kriterier som är tillämpliga för specificeringen av evalueringsobjektet fastställs i de krav som anges i A.2.1.1. De särskilda regler som är tillämpliga på det förfarande som ska följas av sökanden och av certifieringsorganet för att fastställa evalueringsobjektet specificeras av Europrivacy-systemet (10.2 – Verksamhet före certifiering).

10. Dataskyddsstyrelsen noterar i den dokumentation avseende certifieringsmekanismens tillämpningsområde som tillhandahållits av tillsynsmyndigheten i Luxemburg att Europrivacy-systemet gäller för personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i Europeiska unionen (EU) eller i Europeiska ekonomiska samarbetsområdet (EES). Kriteriernas tillämplighet fastställs beroende på sökandens uppgifter och ansvarsområden.

11. Dataskyddsstyrelsen noterar att en personuppgiftsansvarig kan lämna in ett evalueringsobjekt som omfattas av gemensamt personuppgiftsansvar till certifieringsprocessen i Europrivacy (kriterium A.2.7.1). I de fall då evalueringsobjektet omfattas av gemensamt personuppgiftsansvar vill dataskyddsstyrelsen 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 certifieringsmekanismen ska påvisa. Som en följd av detta 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[4] – beroende på sammanhanget för evalueringsobjektets behandling – hindra sökanden från att uppfylla kriterierna för certifieringen.

12. Dataskyddsstyrelsen noterar att behandlingen av genetiska uppgifter är undantagen från tillämpningsområdet för Europrivacy-systemets certifieringsmekanism. Därför omfattar styrelsens bedömning av kriterierna inte kriteriernas lämplighet för evalueringsobjekt som inbegriper sådan behandling.

2.2 Bearbetning

13. Kriterierna gäller behandlingens relevanta komponenter (uppgifter, system och behandling) med avseende på certifieringsmekanismens allmänna tillämpningsområde. Kriterierna 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 – Särskild behandling av uppgifter).

[4] *Fastställandet av deras respektive ansvarsområden måste i synnerhet behandla utövandet av de registrerades rättigheter och skyldigheterna att tillhandahålla information. Utöver detta bör fördelningen av ansvarsområden täcka andra skyldigheter för den personuppgiftsansvarige som allmänna dataskyddsprinciper, juridisk grund, säkerhetsåtgärder, skyldighet att anmäla personuppgiftsincidenter, konsekvensanalys för dataskydd, användning av personuppgiftsbiträden, överföring till tredjeland och kontakter med registrerade och tillsynsmyndigheter* (Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i den allmänna dataskyddsförordningen).

2.3 Behandlingens laglighet

14. Enligt kriterierna måste 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 av kriterierna – Uppgiftsbehandlingens laglighet).

2.4 Uppgiftsbehandlingens principer

15. Kriterierna omfattar dataskyddsprinciperna enligt artikel 5 i den allmänna dataskyddsförordningen på ett tillfredsställande sätt. Framför allt ställer kriterierna krav på att sökanden ska visa att personuppgifterna är adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för (uppgiftsminimering).

2.5 Allmänna skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

16. Kriterierna speglar den personuppgiftsansvariges skyldigheter enligt artikel 24 i den allmänna dataskyddsförordningen (G.4 – 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 – Personuppgiftsansvariga eller underentreprenörer).

17. Enligt kriterierna måste alla sökande utse ett dataskyddsombud, även i de fall då sökanden inte är skyldig att utnämna 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 – Dataskyddsombud).

18. Kriterierna används även för att kontrollera innehållet i registren över behandlingen i enlighet med artikel 30 i den allmänna dataskyddsförordningen (avsnitt G.5.3 av kriterierna – Register över behandling).

2.6 De registrerades rättigheter

19. Kriterierna omfattar på ett tillfredsställande sätt den registrerades rätt till information i enlighet med kapitel III i den allmänna dataskyddsförordningen och ställer krav på att motsvarande åtgärder ska införas. Kriterierna 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 – De registrerades rättigheter).

2.7 Risker för rättigheter och friheter

20. Kriterierna innebär att riskerna för fysiska personers rättigheter och friheter i samband med den behandling av uppgifter som utförs av evalueringsobjektet måste bedömas i enlighet med artikel 35 i den allmänna dataskyddsförordningen (avsnitt G.8 av kriterierna – Konsekvensbedömning avseende dataskydd).

2.8 Tekniska och organisatoriska åtgärder för att garantera skydd

21. Kriterierna ställer krav på att tekniska och organisatoriska åtgärder tillämpas med avseende på behandlingens konfidentialitet, integritet och tillgänglighet. Enligt kriterierna är det även nödvändigt att tillämpa 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 av kriterierna

– Säkerhet i samband med behandlingen och inbyggt dataskydd, avsnitt T.1/T.2 av kriterierna – Grundläggande säkerhetskrav/Utökade säkerhetskrav).

22. Kriterierna ställer 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 – Hantering av personuppgiftsincidenter).

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

23. Kriterierna ställer 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 av kriterierna – Överföringar av personuppgifter till tredjeländer eller internationella organisationer).

3. YTTERLIGARE KRITERIER FÖR ETT EUROPEISKT SIGILL FÖR DATASKYDD

24. Enligt riktlinjerna ska bedömningen innefatta frågan om huruvida ”det i kriterierna [tas] hänsyn till medlemsstaternas lagstiftning eller scenarion för dataskydd”. Enligt avsnitt G.1.1.3 av kriterierna ska sökanden tillhandahålla en sådan bedömning i en utvärderingsrapport om efterlevnaden av nationella skyldigheter (National Obligations Compliance Assessment Report, NOCAR). Dataskyddsstyrelsen noterar att denna rapport ska innehålla en bedömning av de nationella skyldigheter som är tillämpliga för evalueringsobjektet och kommer att 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.

SLUTSATSER OCH REKOMMENDATIONER

25. Avslutningsvis anser EDPB att Europrivacy-systemets certifieringskriterier uppfyller kraven i den allmänna dataskyddsförordningen och godkänner dem i enlighet med den uppgift som fastställs för dataskyddsstyrelsen i artikel 70.1 o i den allmänna dataskyddsförordningen, vilket leder till en gemensam certifiering (det europeiska sigillet för dataskydd).

26. EDPB kommer att registrera Europrivacy-systemets certifieringsmekanism i det offentliga registret över certifieringsmekanismer och sigill och märkningar för dataskydd i enlighet med artikel 42.8.

AVSLUTANDE ANMÄRKNINGAR

27. Detta yttrande riktas till tillsynsmyndigheten i Luxemburg och kommer att offentliggöras i enlighet med artikel 64.5 b i den allmänna dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordföranden