Databeskyttelsesrådets udtalelser (artikel 64)

Udtalelse 19/2024 om EuroPrise-certificeringskriterierne, vedrørende Databeskyttelsesrådets godkendelse heraf som europæisk databeskyttelsesmærkning i medfør af artikel 42, stk. 5, i GDPR

Vedtaget den 16. juli 2024

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

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 63, artikel 64, stk. 2, og artikel 42 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 (herefter "GDPR"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS), særlig bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1],

under henvisning til artikel 10 og 22 i forretningsordenen.

(1) Medlemsstater, tilsynsmyndigheder, Det Europæiske Databeskyttelsesråd (herefter "Databeskyttelsesrådet") og Europa-Kommissionen tilskynder navnlig på EU-plan til fastlæggelse af certificeringsmekanismer for databeskyttelse (herefter "certificeringsmekanismer") samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder GDPR under hensyntagen til mikrovirksomheders og små og mellemstore virksomheders særlige behov.[2] Fastlæggelsen af certificeringsmekanismer kan desuden forbedre gennemsigtigheden og give de registrerede mulighed for at vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenesteydelser.[3]

(2) Certificeringskriterierne udgør en integreret del af en certificeringsmekanisme. Følgelig kræver GDPR, at kriterierne for en national certificeringsmekanisme godkendes af den kompetente tilsynsmyndighed (artikel 42, stk. 5, og artikel 43, stk. 2, litra b), i GDPR), eller, i tilfælde af en europæisk databeskyttelsesmærkning, af Databeskyttelsesrådet (artikel 42, stk. 5, og artikel 70, stk. 1, litra o), i GDPR).

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

(4) Denne udtalelse har til formål at sikre ensartet anvendelse af GDPR, herunder af tilsynsmyndighederne, de dataansvarlige og databehandlerne i lyset af de centrale elementer, som certificeringsmekanismerne skal udvikle. Databeskyttelsesrådets vurdering foretages navnlig på grundlag af "Retningslinjerne 1/2018 vedrørende certificering og identifikation af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordningen" (herefter "retningslinjerne") og tillægget hertil med vejledning om vurdering af certificeringskriterier ("Guidance on certification criteria assessment") (herefter "tillægget"), for hvilke den offentlige høringsperiode udløb den 26. maj 2021.

[1] Henvisninger til "medlemsstater" i denne udtalelse bør forstås som henvisninger til "EØS-medlemsstater".
[2] Artikel 42, stk. 1, i GDPR.
[3] Betragtning 100 i GDPR.

(5) Databeskyttelsesrådet anerkender følgelig, at hver certificeringsmekanisme bør behandles individuelt, uden at dette berører vurderingen af andre certificeringsmekanismer.

(6) Certificeringsmekanismer bør sætte dataansvarlige og databehandlere i stand til at påvise overholdelse af GDPR. Derfor bør deres kriterier på korrekt vis afspejle de krav og principper om beskyttelse af personoplysninger, som er fastsat i GDPR, og bidrage til ensartet anvendelse heraf.

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

(8) Certificeringer bør følgelig tilføre værdi for dataansvarlige og databehandlere ved at bidrage til gennemførelsen af standardiserede og konkrete organisatoriske og tekniske foranstaltninger, der påviseligt letter og fremmer behandlingsaktiviteternes overholdelse af GDPR under hensyntagen til sektorspecifikke krav.

(9) Databeskyttelsesrådet bifalder den indsats, som de ansvarlige for ordningerne har gjort for at udvikle certificeringsmekanismer, som er praktiske og potentielt omkostningseffektive værktøjer til at sikre bedre overensstemmelse med GDPR og fremme de registreredes ret til privatlivets fred og databeskyttelse ved øge gennemsigtigheden.

(10) Databeskyttelsesrådet minder om, at certificeringer er frivillige ansvarlighedsværktøjer, og at overholdelsen af en certificeringsmekanisme ikke mindsker dataansvarliges eller databehandleres forpligtelse til at overholde GDPR eller hindrer tilsynsmyndighederne i at udøve deres opgaver og beføjelser i henhold til GDPR og den relevante nationale lovgivning.

(11) I denne udtalelse behandler Databeskyttelsesrådet spørgsmål, såsom kriteriernes anvendelsesområde og deres anvendelighed og relevans i alle medlemsstater.

(12) Denne udtalelse har fokus på certificeringskriterierne. Såfremt Databeskyttelsesrådet kræver et højt informationsniveau, hvad angår evalueringsmetoderne, for grundigt at kunne vurdere kriteriernes kontrollerbarhed inden for rammerne af sin udtalelse herom, omfatter sidstnævnte ikke nogen form for godkendelse af sådanne evalueringsmetoder.

(13) Databeskyttelsesrådets udtalelse vedtages i overensstemmelse med artikel 64, stk. 2, i GDPR 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

1. I overensstemmelse med artikel 42, stk. 5, i GDPR og retningslinjerne blev udkastet til "EuroPrise Criteria Catalogue for the certification of processing operations by processors (scope: EU) v1.5" (herefter "udkastet til certificeringskriterier", "certificeringskriterierne" eller "kriterierne") udarbejdet af EuroPrise Cert GmbH (herefter "ordningens ejer"), en juridisk enhed i Tyskland, og indsendt til Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, den kompetente tyske tilsynsmyndighed i Nordrhein-Westfalen (herefter "DE-NRW SA").

2. Den tyske tilsynsmyndighed forelagde udkastet til certificeringskriterier for Databeskyttelsesrådet til godkendelse i henhold til artikel 64, stk. 2, i GDPR den 29. april 2024. Konklusionen om, at sagsakterne er komplette, blev truffet den 29. maj 2024.

3. EuroPrise-certificeringsmekanismen er ikke en certificering i henhold til artikel 46, stk. 2, litra f), i GDPR bestemt til internationale overførsler af persondata og indeholder derfor ikke fornødne garantier inden for rammerne af overførsler af persondata til tredjelande eller internationale organisationer i henhold til artikel 46, stk. 2, litra f). Enhver overførsel af persondata til et tredjeland eller til en international organisation må kun foretages, hvis bestemmelserne i kapitel V i GDPR overholdes.

2. VURDERING

4. Databeskyttelsesrådet har foretaget sin vurdering af certificeringskriterierne, som er forelagt til godkendelse i henhold til artikel 42, stk. 5, i GDPR i overensstemmelse med den struktur, som er fastlagt i bilag 2 til retningslinjerne (herefter "bilaget") og tillægget hertil.

2.1 Omfanget af certificeringsmekanismen og målet med evalueringen

5. EuroPrise-certificeringsmekanismen indeholder certificeringskriterier for en EU-dækkende certificeringsordning for certificering af behandling foretaget af databehandlere. Emnet for certificeringer, som certificeringskriterierne gælder for, er behandlingsaktiviteter, der udføres i produkter, processer og tjenesteydelser eller ved hjælp af (flere) produkter og tjenesteydelser, og med hensyn til hvilke ansøgeren om certificering fungerer som en databehandler. Hovedkriterierne for denne certificeringsmekanisme er opdelt i tre sæt af krav, dvs. anskuet fra et juridisk perspektiv (sæt 1), fra et perspektiv, der knytter sig til tekniske og organisatoriske foranstaltninger (sæt 2), og fra et perspektiv, der knytter sig til de registreredes rettigheder (sæt 3).

6. Ansøgere om certificering i henhold til denne ordning skal være databehandlere. Dette omfatter databehandlere, der er direkte betroet behandlingen af personoplysninger af en dataansvarlig i den i artikel 4, stk. 7, i GDPR omhandlede betydning. Ansøgere om certificering kan dog også være databehandlere i den i artikel 28, stk. 2 og 4, i GDPR omhandlede betydning (underdatabehandlere).

7. Når en databehandler – certificeret i henhold til EuroPrise-certificeringsordningen – anvender en underdatabehandler, kan sidstnævnte ikke hævde, at den er blevet certificeret i henhold til EuroPrise-certificeringsordningen. Kun behandlingsaktiviteter udført af den oprindelige og certificerede databehandler er omfattet af certificeringen i et sådant tilfælde. Underdatabehandlere kan dog også ansøge om certificering, hvilket ville resultere i en selvstændig og uafhængig procedure.

8. Databeskyttelsesrådet bemærker i dokumentationen vedrørende anvendelsesområdet for den certificeringsmekanisme, som den tyske tilsynsmyndighed har forelagt, at EuroPrise-ordningen finder anvendelse på databehandlere etableret i Den Europæiske Union (EU) eller i Det Europæiske Økonomiske Samarbejdsområde (EØS).

2.2 Behandling

9. Disse kriteriers anvendelsesområde er ikke begrænset til visse typer af behandlingsaktiviteter. Det er snarere metodologien, der ligger til grund for en EuroPrise-evaluering, som giver mulighed for certificering af alle behandlingsaktiviteter foretaget af databehandlere. Det er derfor en universel metodologisk tilgang, på grundlag af hvilken et stort antal meget forskellige behandlingsaktiviteter

kan certificeres. Derfor er det af afgørende betydning, at de metodologiske krav overholdes, da dette er den eneste måde, hvorpå der kan sikres en ensartet anvendelse af certificeringskriterierne og et sammenligneligt testniveau på tværs af forskellige certificeringsprocedurer. Målet er at sikre sammenlignelighed og reproducerbarhed af de udstedte certificeringer og deres resultater.

2.3 Lovlighed af og principper for databehandling

10. Kriterierne kræver en undersøgelse af, om de behandlingsaktiviteter, der skal certificeres, overholder principperne om databeskyttelse gennem design og gennem standardindstillinger (afsnit 1.5 i kriterierne), hvilket indebærer, at ansøgeren skal bistå den dataansvarlige med at gennemføre disse principper. Dette gør det muligt at vurdere overholdelsen af artikel 25 i GDPR sammenholdt med artikel 5 i GDPR. Selv om der ikke er kriterier, der direkte sigter mod overholdelse af artikel 6 i GDPR – i betragtning af, at den dataansvarlige er ansvarlig for behandlingens lovlighed – har kriterierne til formål at sikre, at databehandlere-ansøgere udformer de behandlingsaktiviteter, der skal certificeres, på en måde, der letter de dataansvarliges implementering af databeskyttelsesprincipperne i artikel 5 i GDPR, herunder princippet om behandlingens lovlighed.

2.4 Dataansvarliges og databehandleres generelle forpligtelser

11. Kriterierne afspejler forholdet mellem databehandleren og den dataansvarlige. Kriterierne fastsætter navnlig databehandlerens forpligtelse til at anvende en model for en databehandlingsaftale med den dataansvarlige, som omfatter alle kravene i artikel 28 i GDPR (afsnit 1.2 i kriterierne).

12. I henhold til kriterierne skal ansøgere udpege en databeskyttelsesrådgiver i henhold til artikel 37 i GDPR og fremlægge dokumentation for udnævnelsen af databeskyttelsesrådgiveren (f.eks. udnævnelsesattest). Kriterierne kontrollerer, at databeskyttelsesrådgiveren opfylder kravene i henhold til artikel 37-39 (sæt 1, afsnit 1.1 i kriterierne).

13. Kriterierne kontrollerer indholdet af fortegnelserne over behandlingsaktiviteter i overensstemmelse med artikel 30 i GDPR (sæt 1, afsnit 1.1 i kriterierne).

2.5 De registreredes rettigheder

14. Kriterierne tager i tilstrækkelig grad højde for registreredes ret til information i overensstemmelse med kapitel III i GDPR og kræver, at der indføres respektive foranstaltninger. Kriterierne kræver endvidere, at der gennemføres foranstaltninger, der giver mulighed for at gribe ind i behandlingsaktiviteterne for at sikre registreredes rettigheder og tillade korrektioner, sletning eller begrænsninger (sæt 3 i kriterierne).

2.6 Risici for rettigheder og friheder

15. Kriterierne kræver, at databehandleren er opmærksom på de mulige risici for fysiske personers rettigheder og friheder i forbindelse med den databehandling, der er omfattet af målet med evalueringen. Hvis behandlingen af personoplysninger sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og friheder, sikrer flere kriterier, at ansøgeren påviser, at kravene i artikel 35 i GDPR er opfyldt i overensstemmelse med artikel 35 i GDPR (afsnit 1.2.2 i kriterierne, krav nr. 6, afsnit 1.3.2 i kriterierne, afsnit 1.3.3 i kriterierne, afsnit 2.1.5.1 i kriterierne, afsnit 2.1.5.9 i kriterierne).

2.7 Tekniske og organisatoriske foranstaltninger, der garanterer beskyttelse

16. Kriterierne kræver anvendelse af tekniske og organisatoriske foranstaltninger, der sikrer behandlingsaktiviteternes fortrolighed, integritet og tilgængelighed. Kriterierne kræver også, at der anvendes tekniske foranstaltninger til at gennemføre databeskyttelse gennem design og gennem standardindstillinger i overensstemmelse med artikel 25 og 32 i GDPR (afsnit 1.5 i kriterierne, afsnit 2.1 i kriterierne/andre dokumenter).

17. Kriterierne kræver, at der anvendes foranstaltninger til at sikre, at pligten til at anmelde brud på persondatasikkerheden udføres rettidigt og i tilstrækkeligt omfang i overensstemmelse med artikel 33 i GDPR (afsnit 1.2.2 i kriterierne, krav nr. 6).

2.8 Kriterier med henblik på at påvise tilstedeværelsen af fornødne garantier for overførsel af personoplysninger

18. Kriterierne kræver identifikation af alle overførsler af personoplysninger til tredjelande og til internationale organisationer, der er omfattet af målet med evalueringen, og begrundelse for valget af overførselsmekanisme, der giver passende garantier, i medfør af kapitel V i GDPR (afsnit 1.4 i kriterierne).

3. YDERLIGERE KRITERIER FOR EN EUROPÆISK DATABESKYTTELSESMÆRKNING

19. Ifølge retningslinjerne skal vurderingen omfatte spørgsmålet om, "hvorvidt kriterierne kan tage hensyn til medlemsstaternes databeskyttelseslovgivning eller -scenarier". Afsnit 4 i kriterierne kræver, at ansøgeren overholder gældende national og relevant sektorspecifik databeskyttelseslovgivning. Desuden forstår Databeskyttelsesrådet, at en "rapport om overholdelse af national lovgivning" – der især vurderer overholdelsen af krav i den gældende nationale databeskyttelseslovgivning, for så vidt angår målet med evalueringen – skal udarbejdes af juridiske eksperter, forudsat at disse eksperter har demonstreret det nødvendige niveau af ekspertise inden for den gældende nationale lovgivning.

KONKLUSIONER/ANBEFALINGER

20. Sammenfattende finder Databeskyttelsesrådet, at udkastet til certificeringskriterier er i overensstemmelse med GDPR og godkender dem i henhold til Databeskyttelsesrådets opgave som defineret i artikel 70, stk. 1, litra o), i GDPR, hvilket medfører en fælles certificering (europæisk databeskyttelsesmærkning).

21. Databeskyttelsesrådet vil registrere certificeringsmekanismen "EuroPrise Criteria Catalogue for the certification of processing operations by processors" i det offentlige register over certificeringsmekanismer og databeskyttelsesmærkninger og -mærker i medfør af artikel 42, stk. 8.

AFSLUTTENDE BEMÆRKNINGER

22. Denne udtalelse er rettet til den tyske tilsynsmyndighed i Nordrhein-Westfalen og vil blive offentliggjort i medfør af artikel 64, stk. 5, litra b), i GDPR.

På vegne af Det Europæiske Databeskyttelsesråd

Formanden
Anu Talus