Databeskyttelsesrådets udtalelser (artikel 64)

Udtalelse 9/2019 om den østrigske tilsynsmyndighed for databeskyttelses udkast til kravene til akkreditering af et organ til kontrol af adfærdskodekser i henhold til artikel 41 i databeskyttelsesforordningen

Vedtaget den 9. juli 2019

vedtaget

Indhold

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 63, artikel 64, stk. 1, litra c), og stk. 3-8, samt artikel 41, stk. 3 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "databeskyttelsesforordningen"),

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

under henvisning til forretningsordenens artikel 10 og artikel 22 af 25. maj 2018, som ændret den 23. november 2018,

ud fra følgende betragtninger:

(1) Den primære rolle, der varetages af Det Europæiske Databeskyttelsesråd (i det følgende benævnt Databeskyttelsesrådet) er at sikre ensartet anvendelse af databeskyttelsesforordningen, når en tilsynsmyndighed har til hensigt at godkende kravene til akkreditering af et organ til kontrol af adfærdskodekser (i det følgende benævnt "kodeks") i henhold til artikel 41. Formålet med denne udtalelse er derfor at bidrage til en harmoniseret tilgang med hensyn til de foreslåede krav, som en tilsynsmyndighed for databeskyttelse skal udarbejde, og som finder anvendelse ved den kompetente tilsynsmyndigheds akkreditering af et organ til kontrol af adfærdskodekser. Selv om databeskyttelsesforordningen ikke direkte pålægger et enkelt sæt krav til akkreditering, fremmer den dog ensartethed. Databeskyttelsesrådet søger at opnå dette mål i sine udtalelse ved for det første at anmode de kompetente tilsynsmyndigheder om at udarbejde deres krav til akkreditering af kontrolorganer på basis af Databeskyttelsesrådets retningslinjer 1/2019 om adfærdskodekser og kontrolorganer i henhold til forordning 2016/679 (Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679; i det følgende benævnt "retningslinjerne"), ved at bruge de otte krav som anført i retningslinjernes afsnit om krav til akkreditering (afsnit 12); dernæst ved at forelægge en skriftlig vejledning, som forklarer kravene til akkreditering; og slutteligt ved at anmode dem om at vedtage disse krav i overensstemmelse med denne udtalelse med henblik på at opnå en harmoniseret tilgang.

(2) Med henvisning til artikel 41 i databeskyttelsesforordningen, skal de kompetente tilsynsmyndigheder vedtage kravene for akkreditering af kontrolorganer af godkendte kodekser. De skal dog anvende sammenhængsmekanismen, så det bliver muligt at fastsætte passende krav for at sikre, at tilsynsorganer fører kontrol med overholdelsen af kodekser på en kompetent, sammenhængende og uafhængig måde, og således fremme korrekt implementering af kodekser i hele Unionen og, som resultat heraf, bidrage til korrekt anvendelse af databeskyttelsesforordningen.

(3) For at en kodeks for ikkeoffentlige myndigheder og organer kan godkendes, skal et kontrolorgan (eller flere) anføres som en del af kodeksen og akkrediteres af den kompetente tilsynsmyndighed som

værende i stand til at føre effektiv kontrol med kodeksen. Begrebet "akkreditering" defineres ikke i Databeskyttelsesforordningen. Dog beskriver artikel 41, stk. 2, i databeskyttelsesforordningen, de generelle krav til akkreditering af kontrolorganet. Der er en række krav, som skal overholdes, for at den kompetente tilsynsmyndighed kan akkreditere et kontrolorgan. Kodeksindehavere er forpligtet til at forklare og demonstrere, hvordan deres foreslåede kontrolorgan overholder kravene i artikel 41, stk. 2, til at opnå akkreditering.

(4) Selvom kravene til akkreditering af kontrolorganer er underlagt sammenhængsmekanismen, bør udviklingen af kravene til akkreditering i retningslinjerne tage højde for kodeksens sektor eller særtræk. De kompetente tilsynsmyndigheder har skønsbeføjelse med henblik på hver kodeks' omfang og særtræk og bør tage den relevante lovgivning i betragtning. Formålet med databeskyttelsesrådets udtalelse er derfor at undgå betydelige uoverensstemmelser, som kan påvirke kontrolorganernes præstationer og dermed også påvirke databeskyttelsesforordningens adfærdskodeksers eller deres kontrolorganers omdømme.

(5) I det henseende vil de af Databeskyttelsesrådet vedtagne retningslinjer fungere som en ledetråd inden for rammerne af sammenhængsmekanismen. Navnlig har Databeskyttelsesrådet i retningslinjerne præciseret, at selvom akkreditering af et kontrolorgan kun gælder for en specifik kodeks, kan et kontrolorgan akkrediteres for flere kodekser, forudsat at det overholder kravene til akkreditering for hver kodeks.

(6) Databeskyttelsesrådets udtalelse vedtages i overensstemmelse med artikel 64, stk. 3, i databeskyttelsesforordningen 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 afgørelse fra formandskabet kan denne frist forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet.

VEDTAGET DENNE UDTALELSE:

1 KORT FREMSTILLING AF DE FAKTISKE OMSTÆNDIGHEDER

1. Den østrigske tilsynsmyndighed har indgivet sit udkast til afgørelse, som omfatter kravene til akkreditering af et kontrolorgan for adfærdskodekser, til Databeskyttelsesrådet via IMI-systemet med anmodning om en udtalelse fra Databeskyttelsesrådet i henhold til artikel 64, stk. 1, litra c), for en sammenhængende og konsekvent tilgang på EU-plan. Afgørelsen vedrørende sagsakternes fuldstændighed blev truffet den 9. april 2019.

2. Den østrigske tilsynsmyndighed indgav udkastet til kravene til akkreditering af kodekskontrolorganer i en engelsk udgave, selvom det oprindeligt var på tysk. Databeskyttelsesrådets fremsætter derfor udtalelse om den engelske udgave af udkastet til krav til akkreditering og anbefaler den østrigske tilsynsmyndighed at ændre og tilpasse begge udgaver i overensstemmelse med denne udtalelse.

3. I overensstemmelse med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden [1], valgte Databeskyttelsesrådet på grund af sagens kompleksitet at forlænge den oprindelige vedtagelsesperiode på otte uger med yderligere seks uger til den 16. juli 2019.

2 VURDERING

2.1 Databeskyttelsesrådets generelle ræsonnement vedrørende udkastet til afgørelse

4. Alle krav til akkreditering, der indgives til Databeskyttelsesrådet med henblik på en udtalelse, skal tage fuldt hensyn til kriterierne i artikel 41, stk. 2, i databeskyttelsesforordningen og være i overensstemmelse med de otte områder, Databeskyttelsesrådet har præciseret i akkrediteringsafsnittet i retningslinjerne (afsnit 12, side 21-25). Databeskyttelsesrådets udtalelse sigter efter at sikre sammenhæng og en korrekt anvendelse af artikel 41, stk. 2, i databeskyttelsesforordningen, hvad angår det fremlagte udkast.

5. Dette betyder, at alle tilsynsmyndighederne, når de udarbejder krav til akkreditering af et kontrolorgan for adfærdskodekser i henhold til artikel 41, stk. 3, og artikel 57, stk. 1, litra p), i databeskyttelsesforordningen, skal dække disse grundlæggende kernekrav i retningslinjerne, og Databeskyttelsesrådet anbefaler, at tilsynsmyndighederne ændrer deres udkast i overensstemmelse hermed for at sikre sammenhæng.

6. Alle kodekser, der dækker ikkeoffentlige myndigheder og organer, skal have akkrediterede kontrolorganer. Databeskyttelsesforordningen anmoder specifikt om, at tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen "tilskynder til udarbejdelse af adfærdskodekser, der under hensyntagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov bidrager til korrekt anvendelse af denne forordning" (artikel 40, stk. 1, i databeskyttelsesforordningen). Databeskyttelsesrådet anerkender derfor, at kravene skal kunne fungere for forskellige typer kodekser, idet de gælder for sektorer af forskellig størrelse, tager hensyn til de forskellige interesser og dækker behandlingsaktiviteter med forskellige risikoniveauer.

7. På nogle områder vil Databeskyttelsesrådet støtte udviklingen af harmoniserede krav ved at opfordre tilsynsmyndigheden til at kun at betragte de fremsatte eksempler som illustration. Derfor behøver opfordringerne og eksemplerne i denne udtalelse ikke at blive fulgt. Dog er formålet med disse eksempler at hjælpe den østrigske tilsynsmyndighed med at videreudvikle sammenhængende krav til akkreditering i overensstemmelse med denne udtalelse.

8. I tilfælde, hvor denne udtalelse ikke indeholder et specifikt krav, betyder det, at Databeskyttelsesrådet ikke anmoder den østrigske tilsynsmyndighed om at træffe yderligere foranstaltninger.

[1] Udgave 2, som senest ændret og vedtaget den 23. november 2018

9. Databeskyttelsesrådet bemærker, at dokumentet indgivet af den østrigske tilsynsmyndighed er et udkast til afgørelse om kravene til akkreditering af kontrolorganer bestående af to dele:

    1) "Forklarende bemærkninger", som indeholder generelle og specifikke forklaringer.

    2) "Bekendtgørelsen", som fastsætter de østrigske krav til akkreditering.

10. Denne udtalelse omfatter ikke forhold fremlagt af den østrigske tilsynsmyndighed, som falder uden for anvendelsesområdet for artikel 41, stk. 2, i databeskyttelsesforordningen, såsom henvisninger til national lovgivning. Ikke desto mindre konstaterer Databeskyttelsesrådet, at national lovgivning bør være i overensstemmelse med databeskyttelsesforordningen, hvor det er påkrævet.

2.2 Analyse af udkastet til afgørelse (bestående af de forklarende bemærkninger og bekendtgørelsen)

11. Under hensyntagen til:

    a. artikel 57, stk. 1, litra p) og q), i databeskyttelsesforordningen, fastsætter, at en kompetent tilsynsmyndighed skal udarbejde og offentliggøre kravene til akkreditering af kontrolorganer samt foretage akkrediteringen
    b. artikel 41, stk. 4, i databeskyttelsesforordningen fastlægger, at alle kodekser (undtagen kodekser, der omfatter offentlige myndigheder efter artikel 41, stk. 6) har et akkrediteret kontrolorgan, og
    c. artikel 41, stk. 2, i databeskyttelsesforordningen indeholder en liste over de akkrediteringspunkter, et kontrolorgan skal opfylde for at blive akkrediteret

    er Databeskyttelsesrådet af følgende holdning:

2.2.1 UAFHÆNGIGHED

12. Med hensyn til § 3 i den østrigske tilsynsmyndigheds bekendtgørelse fremhæver Databeskyttelsesrådet, at forpligtelsen til at påvise et kontrolorgans uafhængighed påhviler det organ, der ansøger om akkreditering (se artikel 41, stk. 2, litra a), i databeskyttelsesforordningen). Databeskyttelsesrådet anbefaler, at dette præciseres i den østrigske tilsynsmyndigheds krav.

13. Databeskyttelsesrådet bemærker, at der i afsnittet "generelle bemærkninger" i den østrigske tilsynsmyndigheds forklarende bemærkninger vedrørende kravene henvises til uafhængighed "*for så vidt angår kodeksens genstand*". Retningslinjerne indeholder yderligere oplysninger om, hvad dette betyder, dvs. det pågældende organs uafhængighed bør påvises i forbindelse med medlemmerne af kodeksen eller den profession, branche eller sektor, som kodeksen finder anvendelse på, samt kodeksindehaveren selv. Derfor anbefaler Databeskyttelsesrådet, at den østrigske tilsynsmyndighed omformulerer denne henvisning i overensstemmelse med retningslinjerne.

14. Databeskyttelsesrådet er af den holdning, at et kontrolorgans uafhængighed skal forstås som en række formelle regler og procedurer for udnævnelsen, mandatet og driften af kontrolorganet. Disse regler og procedurer sætter kontrolorganet i stand til at føre tilsyn med overholdelsen af en adfærdskodeks fuldstændigt uafhængigt, uden direkte eller indirekte påvirkning eller nogen form for pres, der kunne påvirke dets beslutninger. Dette betyder, at et kontrolorgan ikke bør kunne modtage nogen instrukser vedrørende udførelsen af sine opgaver fra medlemmer af kodeksen eller fra den profession, branche eller sektor, som kodeksen finder anvendelser på, eller fra kodeksindehaveren selv.

15. Hvor kontrolorganet er en del af kodeksindehaverens organisationen, skal der sættes særlig fokus på dets evne til at handle uafhængigt. Eksempler på interne kontrolorganer kunne blandt andet være et internt ad hoc-udvalg eller en selvstændig afdeling i kodeksindehaverens organisation. Der skal etableres regler og procedurer for at sikre, at et sådant "udvalg" handler selvstændigt og uden pres fra kodeksindehaveren eller -medlemmerne.

16. Databeskyttelsesrådet bemærker, at den østrigske tilsynsmyndighedens krav ikke indeholder nogen henvisning til de to hovedtilsynsmodeller, der anføres i retningslinjerne. Databeskyttelsesrådet anbefaler derfor, at den østrigske tilsynsmyndighed ændrer kravene for at afspejle denne fleksibilitet. Én mulighed kunne være at kræve, at et internt kontrolorgan forelægger dokumentation for yderligere foranstaltninger, for at sikre, at forholdet til den retlige enhed (som kontrolorganet er en del af) ikke kompromitterer uafhængigheden af dets tilsynsaktiviteter.

17. Databeskyttelsesrådet bemærker, at en specifik bestemmelse i det af den østrigske tilsynsmyndigheds udkast til krav til akkreditering vedrører kontrolorganets påvisning af selvstændighed (§ 3.2 i den østrigske bekendtgørelse). Den nævnte bestemmelse anmoder om oplysninger om de personer, der er bemyndiget til at træffe afgørelser, for at vise, at der ikke er nogen personlig tilknytning til de enheder, der skal kontrolleres. Desuden præciseres det i den forklarende bemærkning vedrørende uafhængighedskravene, at kontrolorganet ikke må være juridisk, økonomisk, personligt eller erhvervsmæssigt underlagt de kontrollerede enheder eller have tætte tilhørsforhold hertil, idet der i så tilfælde vil kunne sættes spørgsmålstegn ved kontrolorganets dømmekraft eller uafhængighed og integritet i dets funktion som kontrolorgan.

18. Databeskyttelsesrådet er af den overbevisning, at kravene til akkreditering skal kvalificere, hvad der udgør uafhængighed, og klart redegøre for de områder, hvor kontrolorganet skal påvise uafhængighed. I den henseende anbefaler Databeskyttelsesrådet, at den østrigske tilsynsmyndighed yderligere styrker afsnittet om uafhængighed i overensstemmelse med de fire nedenfor anførte områder.

1) RETLIGE PROCEDURER OG BESLUTNINGSPROCEDURER

19. Kontrolorganets juridiske form og arrangement skal beskytte kontrolorganet mod utilbørlig påvirkning fra kodeksmedlemmerne eller -indehaveren, som kunne påvirke kontrollen med overholdelsen af en kodeks. For eksempel bør varigheden af eller udløbsdatoen for kontrolorganets mandat fastsættes på en sådan måde, at det forhindrer overdreven afhængighed af fornyelse eller frygt for at miste

udnævnelsen, i et sådant omfang at det har en negativ indvirkning på uafhængigheden i forbindelse med kontrolorganets udførelse af kontrolaktiviteterne.

20. Et kontrolorgans beslutningsproces skal også bevare dets autonomi og selvstændighed. For eksempel skal et kontrolorgan kunne handle uafhængigt i sine valg og sin anvendelse af sanktioner mod en dataansvarlig eller databehandler, som overholder kodeksen.

2) ØKONOMI

21. Kontrolorganerne skal have den økonomiske stabilitet og ressourcerne til effektiv udførelse af deres opgaver samt til at forvalte deres budgetter uafhængigt. Måderne, hvorpå kontrolorganet opnår økonomisk støtte (f.eks. gebyrer, der betales af adfærdskodeksens medlemmer), bør ikke have en negativ indvirkning på uafhængigheden af dets opgave med at kontrollere overholdelsen af en kodeks.

22. F.eks. ville kontrolorganet ikke være at betragte som økonomisk uafhængigt, hvis reglerne for dets økonomiske støtte gør det muligt for et kodeksmedlem, som efterforskes af kontrolorganet, at standse sine økonomiske bidrag til organet for at undgå en eventuel sanktion fra kontrolorganet.

3) ORGANISATORISKE RAMMER

23. Kontrolorganer skal have de menneskelige og tekniske ressourcer, der er nødvendige for effektiv udførelse af deres opgaver. Kontrolorganer skal være sammensat af et tilstrækkeligt antal medarbejdere til at kunne udføre kontrolfunktionen fuldt ud, således at den afspejler den pågældende sektor og de risici, der er forbundet med de behandlingsaktiviteter, der er omhandlet i adfærdskodeksen. Kontrolorganets personale er ansvarlige for og bevarer beføjelser over deres beslutninger vedrørende kontrolaktiviteterne. Disse organisatoriske aspekter kunne udvises gennem proceduren for udvælgelse af personale til kontrolorganet, personalet aflønning samt varigheden af personalets mandat, kontrakt eller anden formel aftale med kontrolorganet.

4) ANSVARLIGHED

24. Kontrolorganet skal kunne demonstrere "ansvarlighed" for sine afgørelser og handlinger for at kunne betragtes som uafhængigt. Dette kan opnås på forskellige måder, såsom præcisering af rollerne og rammerne for beslutningstagning samt organets rapporteringsprocedurer.

2.2.2 INTERESSEKONFLIKT

25. Databeskyttelsesrådet bemærker, at den østrigske tilsynsmyndigheds krav til akkreditering ikke omhandler interessekonflikter. Databeskyttelsesrådet anbefaler, at den østrigske tilsynsmyndighed tilføjer krav, der dækker procedurer til at undgå interessekonflikter. Sådanne procedurer vil sandsynligvis indebære en risikobaseret tilgang og vil variere afhængigt af kodeksen. Der kan opstå risici som følge af kontrolorganets og dets personales aktiviteter og relationer.

26. Et eksempel på en interessekonflikt er, hvis kontrolorganets personale undersøger klager over den organisation, de arbejder for. For at kunne undgå interessekonflikter, oplyser personalet om deres interesse, og arbejdet omfordeles.

27. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at tage følgende praktiske eksempler på krav til akkreditering i betragtning:

- Et kontrolorgan skal identificere situationer, hvor der er sandsynlighed for interessekonflikter (på grund af organets personale, organisation, procedurer osv.), og opstille interne regler for at undgå interessekonflikter.
- Et kontrolorgan skal fastlægge en procedure til håndtering af virkninger af situationer, der kan forventes at skabe interessekonflikt.
- Kontrolorganet skal skriftligt forpligte sig til at overholde dette krav og til at indberette enhver situation, der kan medføre en interessekonflikt, og følge procedurerne for at undgå sådanne konflikter.
- Et kontrolorgan skal løbende identificere og eliminere enhver risiko for uvildighed. Dokumentation herpå inkluderer organets risikohåndteringstilgang og tilknyttede procedurer.

2.2.3 EKSPERTISE

28. Databeskyttelsesrådet bemærker, at den østrigske tilsynsmyndigheds krav til ekspertise omfatter: et særdeles godt kendskab til databeskyttelse og enten en relevant universitetsgrad (eller tilsvarende kvalificering) eller mindst fem års relevant erhvervserfaring inden for branchen, hvor højst to års erhvervserfaring må stamme fra aktiviteter, der ligger uden for kodeksens område (§ 3.4 og 3.5 i den østrigske bekendtgørelse).

29. Databeskyttelsesrådet anerkender, at retningslinjerne sætter niveauet højt ved at kræve, at kontrolorganer har følgende ekspertise: en indgående forståelse af databeskyttelsesaspekter, kendskab til de specifikke behandlingsaktiviteter i forbindelse med kodeksen og passende driftserfaring og uddannelse inden for kontrol, såsom revision.

30. Databeskyttelsesrådet mener, at akkrediteringskravene skal være gennemsigtige. De skal også omfatte kontrolorganer, der søger akkreditering i forbindelse med kodekser, der dækker behandlingsaktiviteterne i mikrovirksomheder og små og mellemstore virksomheder (artikel 40, stk. 1, i databeskyttelsesforordningen).

31. Som foreskrevet i retningslinjerne, skal alle kodekser overholde tilsynsmekanismekriterierne (afsnit 6.4 i retningslinjerne) ved at dokumentere "hvorfor deres forslag til tilsyn er korrekte og operationelt gennemførlige" (punkt 41 på side 17 i retningslinjerne). I denne sammenhæng vil alle kodekser med kontrolorganer skulle forklare det nødvendige ekspertiseniveau for deres kontrolorganer for at kodeksens tilsynsaktiviteter kan udføres effektivt. Dette kan omfatte hensyntagen til faktorer såsom: størrelsen på den pågældende sektor, de forskellige interesser samt risiciene ved de behandlingsaktiviteter, der er omfattet af kodeksen. Dette er med forbehold af databeskyttelseskravene. Dette er også vigtigt, såfremt der er flere kontrolorganer, idet kodeksen hjælper med at sikre en ensartet anvendelse af ekspertisekravene for alle kontrolorganer, der dækker den samme kodeks.

32. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at medregne de yderligere krav til ekspertise, som kan defineres af kodeksen, og sikre, at hvert kontrolorgans ekspertise vurderes i overensstemmelse med den pågældende kodeks. Herved verificerer tilsynsmyndigheden, hvorvidt kontrolorganet besidder de tilstrækkelige kompetencer til de specifikke opgaver og forpligtelser til at varetage effektivt kontrol af kodeksen.

2.2.4 ETABLEREDE PROCEDURER OG STRUKTURER

33. Databeskyttelsesrådet bemærker, at § 4 i bekendtgørelsen er for bredt formuleret. Databeskyttelsesrådet er af den holdning, at kontrolprocedurerne for overholdelsen af adfærdskodekser skal være specifikke nok til at sikre sammenhængende anvendelse af kodekskontrolorganernes forpligtelser.

34. Procedurerne skal omfatte hele tilsynsprocessen, lige fra udarbejdelse af evalueringen til revisionens afslutning samt yderligere kontroller for at sikre, at der træffes passende foranstaltninger til at afhjælpe overtrædelser og forhindre gentagne overtrædelser.

35. Kontrolorganet skal forelægge dokumentation for forhånds- og ad hoc-procedurer og faste procedurer for at kontrollere medlemmernes overholdelse inden for en klar tidsramme samt kontrollere medlemmernes kvalifikation, før de tilslutter sig kodeksen.

36. Desuden skal kontrolorganers personale behandle alle oplysninger, der indhentes eller oprettes under kontrollen, fortroligt, medmindre andet er fastsat i lovgivningen.

37. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at tage følgende eksempler på procedurer i betragtning:

- En procedure, der omfatter revisionsplaner, der skal gennemføres over en bestemt periode (indledende kontrol og tilbagevendende kontrol), på grundlag af kriterier, såsom antal deltagere i adfærdskodeksen, geografisk omfang, antal klager, osv.
- En revisionsprocedure, som definerer den revisionsmetode, der skal anvendes, dvs. en række kriterier, der skal vurderes (fælles evalueringsskema), revisionstype (selvevaluering, ekstern revision eller revision på stedet, ISO-revisionsstandarder), dokumentation af resultaterne osv.
- En procedure for undersøgelse, identificering og forvaltning af overtrædelser af adfærdskodeksen, som, når det er nødvendigt, omfatter sanktioner som fastlagt i adfærdskodeksen (en sanktionsmatriks)

38. Databeskyttelsesrådet anbefaler, at der medtages valgfrie krav vedrørende tilsynsprocedurerne i de østrigske forklarende bemærkninger, og at der præciseres obligatoriske krav i den østrigske bekendtgørelse.

39. Databeskyttelsesrådet anbefaler, at målene for hver enkelt påkrævet procedure defineres udtrykkeligt i kravene til akkreditering.

40. Databeskyttelsesrådet anbefaler, at henvisningen til "relevante certifikater" — som optræder mere end én gang i det østrigske udkast til kravene til akkreditering — præciseres.

2.2.5 GENNEMSIGTIG KLAGEBEHANDLING

41. Hvad angår klagebehandlingsproceduren, bemærker Databeskyttelsesrådet, at den østrigske tilsynsmyndigheds krav til akkreditering (§ 5.3.4 i den østrigske tilsynsmyndigheds bekendtgørelse) omfatter behandlingens varighed og anfører, at "den under alle omstændigheder ikke bør overskride to måneder fra modtagelsen af klagen".

42. Databeskyttelsesrådet anbefaler, at der fastsættes høje krav til klagebehandlingsprocessen, og at der angives rimelige tidsfrister for besvarelse af klager. Et eksempel på en rimelig tidsfrist kunne være, at klageren inden for tre måneder skal meddeles om klagebehandlingens status eller resultat (i lighed med artikel 78, stk. 2, i databeskyttelsesforordningen). Processen skal være: dokumenteret, uafhængig, effektiv og gennemsigtig for at sikre tilliden til adfærdskodeksen. De tilgængelige klageprocedurer skal anføres i selve adfærdskodeksen. Klagebehandlingsprocessen skal være tilgængelig for registrerede personer og for offentligheden.

43. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at tage følgende praktiske eksempler på krav i betragtning:

- Et kontrolorgan skal dokumentere den tilsigtede forvaltning af klageprocedurer og forklare tidsfrister.
- Et kontrolorgan skal skitsere en procedure for modtagelse, forvaltning og behandling af klager. Denne procedure skal være uafhængig og gennemsigtig.
- Klageproceduren skal være offentlig tilgængelig og lettilgængelig.
- Proceduren skal sikre, at alle klager behandles inden for en rimelig tidsfrist.
- Et kontrolorgan skal føre fortegnelse over alle klager, det modtager, og hvilke foranstaltninger der træffes, som den østrigske tilsynsmyndighed til enhver tid kan få adgang til.

2.2.6 KOMMUNIKATION MED DEN KOMPETENTE TILSYNSMYNDIGHED

44. Databeskyttelsesrådet bemærker, at § 6.4 i den østrigske tilsynsmyndigheds bekendtgørelse fastsætter bestemmelse om kontrolorganets årlige rapportering til den kompetente tilsynsmyndighed). Databeskyttelsesrådet anbefaler, at den østrigske tilsynsmyndighed ændrer § 6.4 i bekendtgørelsen for at sikre mere regelmæssig kommunikation med den kompetente tilsynsmyndighed i løbet af året.

45. Databeskyttelsesrådet er af den holdning, at kravene skal omfatte områder såsom: foranstaltningen i tilfælde af overtrædelser af adfærdskodeksen og begrundelser for disse (artikel 41, stk. 4, i

databeskyttelsesforordningen), periodiske rapporter, undersøgelser eller revisionsresultater. Adfærdskodeksen selv skal også skitsere kravene til kommunikation med den kompetente tilsynsmyndighed, herunder relevante ad hoc-rapporter og regelmæssige rapporter. I tilfælde af alvorlige overtrædelser af kodeksen fra kodeksmedlemmers side, som fører til alvorlige foranstaltninger, såsom suspendering eller udelukkelse fra kodeksen, skal de kompetente tilsynsmyndigheder underrettes øjeblikkeligt.

46. Databeskyttelsesrådet definerer "væsentlig ændring" som enhver ændring, der har øjeblikkelig indvirkning på kontrolorganets evne til at udøve sin funktion uafhængigt og effektivt. En væsentlig ændring udløser en genakkrediteringsproces eller en ny akkrediteringsproces. Databeskyttelsesrådet anbefaler, at den østrigske tilsynsmyndighed i kravene til akkreditering tager højde for rapportering af enhver væsentlig ændring til de kompetente tilsynsmyndigheder.

47. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at tage følgende praktiske eksempler på krav i betragtning:

- Et kontrolorgan skal fastsætte rapporteringsmekanismer.
- Et kontrolorgan skal uden unødig forsinkelse informere den kompetente tilsynsmyndighed om enhver væsentlig ændring i kontrolorganet (navnlig for så vidt angår struktur og organisation), som sandsynligvis vil rejse tvivl om dets uafhængighed, ekspertise og fraværet af enhver interessekonflikt, eller som sandsynligvis vil være til skade for dets fulde drift.

2.2.7 REVISIONSMEKANISMER

48. Databeskyttelsesrådet er af den holdning, at kontrolorganet spiller en væsentlig rolle i at bidrage til revision af kodeksen og skal gennemføre opdateringer til kodeksen (ændring eller udvidelse af kodeksen) som bestemt af kodeksindehaveren.

49. Databeskyttelsesrådet opfordrer til krav til akkreditering, som kræver, at et kontrolorgan udvikler mekanismer, der giver mulighed for feedback til kodeksindehaverne. Nogle muligheder ville være at anvende resultaterne fra revisionsprocessen, håndteringen af klager eller foranstaltninger truffet i sager om overtrædelser af kodeksen.

50. F.eks. kan optegnelser over klagebehandlingen (modtagne og behandlede), overtrædelser og afhjælpende midler være en god måde at centralisere relevante oplysninger for at udvikle forbedringer af kodeksen.

51. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at fastsætte krav til akkreditering, som sikrer at kontrolorganet bidrager til alle gennemgange af kodeksen, i overensstemmelse med kodeksindehaverens instrukser.

2.2.8 RETLIG STATUS

52. Databeskyttelsesrådet bemærker, at § 2.2 i den østrigske tilsynsmyndigheds bekendtgørelse fastsætter, at et kontrolorgan kan have hjemsted uden for EØS. Databeskyttelsesrådet er af den holdning, at et kontrolorgan skal være etableret i EØS. Dette er for at sikre, at det kan overholde de registreredes rettigheder, håndtere klager, samt at databeskyttelsesforordningen kan håndhæves og sikrer tilsyn fra den kompetente tilsynsmyndighed. Databeskyttelsesrådet anbefaler, at den østrigske tilsynsmyndighed kræver, at kontrolorganet er etableret i EØS.

53. Desuden bemærker Databeskyttelsesrådet, at den østrigske tilsynsmyndigheds udkast til krav ikke omfatter bestemmelser for akkreditering af kontrolorganer i forbindelse med kodekser, der er godkendt som værktøj til internationale overførsler, sammen med bindende og retskraftige forpligtelser for den dataansvarlige eller databehandleren i tredjelandet til at anvende de fornødne garantier (artikel 46, stk. 2, litra e), i databeskyttelsesforordningen). Det er i den henseende værd at bemærke, at det kan blive nødvendigt at tilføje supplerende krav, når retningslinjer for kodekser som et middel til at fremme internationale overførsler er blevet vedtaget af Databeskyttelsesrådet.

54. Databeskyttelsesrådet bemærker, at den østrigske tilsynsmyndigheds forklarende bemærkning til § 2.1 præciserer, at fysiske personer kan akkrediteres som kontrolorgan. Databeskyttelsesrådet opfordrer den østrigske tilsynsmyndighed til at fastsætte yderligere krav for akkreditering af et sådant kontrolorgan. Disse ville omfatte: at kunne dokumentere at besidde tilstrækkelige ressourcer til de specifikke pligter og ansvarsområder, samt den fulde drift af tilsynsmekanismen over tid. Eksempler på relevante scenarier omfatter: den pågældende persons fratrædelse eller midlertidige utilgængelighed.

55. Databeskyttelsesrådet anbefaler, at de østrigske tilsynsmyndigheder kræver, at kontrolorganet skal have adgang til tilstrækkelige ressourcebehov for at opfylde sine kontrolforpligtelser, særlig med hensyn til akkreditering af en fysisk person som kontrolorgan.

56. Desuden skal selve adfærdskodeksen dokumentere, at driften af kodeksens tilsynsmekanisme er bæredygtig over tid, og tage højde for værst tænkelige scenarier, såsom at kontrolorganet ikke kan varetage kontrolfunktionen. I den henseende ville det være tilrådeligt at kræve, at et kontrolorgan dokumenterer sin evne til at levere adfærdskodeksens tilsynsmekanisme over en passende tidsperiode. Derfor anbefaler Databeskyttelsesrådet, at den østrigske tilsynsmyndighed udtrykkeligt kræver, at kontrolorganer dokumenterer tilsynsfunktionens kontinuitet over tid.

57. Databeskyttelsesrådet er af den holdning, at et kontrolorgan ikke behøver at have en bestemt retlig form for at kunne ansøge om akkreditering, forudsat at det kan holdes juridisk ansvarligt for alle sine kontrolaktiviteter og påvise tilstrækkelige ressourcer til at levere sine kontrolfunktioner (f.eks. virkningen af administrative bøder).

58. Slutteligt bemærker Databeskyttelsesrådet, at den østrigske tilsynsmyndigheds forklarende bemærkninger og bekendtgørelse ikke henviser til underleverandører, således at det overlades til de kontrolorganer, som ansøger om akkreditering, at træffe beslutninger på dette område. Databeskyttelsesrådet anbefaler, at den østrigske tilsynsmyndighed præciserer, hvorvidt kontrolorganet må anvende underleverandører, samt på hvilke vilkår og betingelser, og at disse

afspejles i de forklarende bemærkninger eller bekendtgørelsen i overensstemmelse hermed. Hvis de østrigske tilsynsmyndigheder angiver, at underleverance er tilladt, anbefaler Databeskyttelsesrådet, at de østrigske tilsynsmyndigheder i bekendtgørelsen anfører, at de for kontrolorganet gældende forpligtelser gælder på samme måde for underleverandører.

3 KONKLUSIONER/ANBEFALINGER

59. Den østrigske tilsynsmyndigheds udkast til krav til akkreditering kan føre til en usammenhængende anvendelse af akkrediteringen af kontrolorganer, og følgende ændringer skal foretages:

60. Vedrørende "uafhængighed" anbefaler Databeskyttelsesrådet den østrigske tilsynsmyndighed at:

1. præcisere, at opgaven med forelægge dokumentation for et kontrolorgans uafhængighed til den kompetente tilsynsmyndigheds tilfredshed påhviler det organ, der ansøger om akkreditering

2. omformulere henvisningen i de forklarende bemærkninger til "for så vidt angår kodeksens genstand", så den er i overensstemmelse med retningslinjerne

3. ændre kravene, så de afspejler de to kontrolorganmodeller i retningslinjerne, og

4. skærpe sine krav i overensstemmelse med de fire områder (retlige procedurer og beslutningstagning, økonomi, organisatoriske rammer og ansvarlighed) for at kvalificere, hvad der udgør uafhængighed.

61. Vedrørende "interessekonflikt" anbefaler Databeskyttelsesrådet den østrigske tilsynsmyndighed at:

1. tilføje krav, der omfatter procedurer til at undgå interessekonflikter.

62. Vedrørende "etablerede procedurer og strukturer" anbefaler Databeskyttelsesrådet den østrigske tilsynsmyndighed at:

1. medtage valgfrie krav vedrørende tilsynsprocedurer i de østrigske supplerende bemærkninger og præcisere de obligatoriske krav i den østrigske bekendtgørelse

2. udtrykkeligt definere målene for hver påkrævet procedure i kravene til akkreditering og

3. præcisere henvisningen til "relevante certifikater" — som optræder mere end én gang i det østrigske udkast til krav til akkreditering.

63. Vedrørende "gennemsigtig klagebehandling" anbefaler Databeskyttelsesrådet, at den østrigske tilsynsmyndigheds:

1. krav til klagebehandlingsprocessen sættes på et højt niveau, og at der fastsættes rimelige tidsfrister for besvarelse af klager.

64. Vedrørende "kommunikation med den kompetente tilsynsmyndighed" anbefaler Databeskyttelsesrådet den østrigske tilsynsmyndighed at:

1. ændre § 6.4 i bekendtgørelsen for at sørge for mere regelmæssig kommunikation med den kompetente tilsynsmyndighed i løbet af året og

2. tage højde for rapportering af enhver væsentlig ændring til de kompetente tilsynsmyndigheder i kravene til akkreditering.

65. Vedrørende "retlig status" anbefaler Databeskyttelsesrådet den østrigske tilsynsmyndighed at:

1. kræve, at kontrolorganet er etableret i EØS

2. kræve, at kontrolorganet skal have adgang til tilstrækkelige ressourcebehov for at kunne varetage sine kontrolforpligtelser og demonstrere, at det kan levere kodeksens kontrolmekanisme over en passende tidsperiode, især ved akkreditering af en fysisk person som kontrolorgan, og

3. præcisere, hvorvidt kontrolorganet må anvende underleverandører, samt på hvilke vilkår og betingelser, og at disse omfattes af de forklarende bemærkninger eller bekendtgørelsen. Såfremt anvendelsen af underleverance tillades, ændres bekendtgørelsen, således at de for kontrolorganet gældende forpligtelser gælder for underleverandører på samme måde.

4 AFSLUTTENDE BEMÆRKNINGER

66. Denne udtalelse er rettet til den østrigske tilsynsmyndighed og offentliggøres i henhold til artikel 64, stk. 5, litra b), i databeskyttelsesforordningen.

67. I henhold til artikel 64, stk. 7 og 8, i databeskyttelsesforordningen giver tilsynsmyndigheden senest to uger efter modtagelsen af udtalelsen formanden for Databeskyttelsesrådet elektronisk meddelelse om, hvorvidt den agter at fastholde eller ændre sit udkast til afgørelse. Tilsynsmyndigheden skal inden for samme tidsperiode forelægge det ændrede udkast til afgørelse eller, hvis det helt eller delvist ikke agter at følge udtalelsen fra Databeskyttelsesrådet, give en relevant begrundelse herfor. Tilsynsmyndigheden skal meddele sin endelige afgørelse til Databeskyttelsesrådet med henblik på opførelse i registret over afgørelser, der er blevet behandlet i sammenhængsmekanismen, i overensstemmelse med artikel 70, stk. 1, litra y), i databeskyttelsesforordningen.

På vegne af Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)