Yttrande 16/2020 om utkastet till beslut från Republiken Tjeckiens behöriga tillsynsmyndighet om godkännande av kraven för ackreditering av ett certifieringsorgan i enlighet med artikel 43.3 i den allmänna dataskyddsförordningen

Antaget den 25 maj 2020

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

Antaget

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit detta yttrande

med beaktande av artikel 63, artikel 64.1 c och 64.3–64.8 och artikel 43.3 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 *dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, i dess ändrade lydelse enligt gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018,[1]

med beaktande av artiklarna 10 och 22 i arbetsordningen av den 25 maj 2018

och av följande skäl:

(1) Europeiska dataskyddsstyrelsens viktigaste uppgift är att se till att förordning 2016/679 (nedan kallad *dataskyddsförordningen*) tillämpas enhetligt i hela Europeiska ekonomiska samarbetsområdet. I enlighet med artikel 64.1 i dataskyddsförordningen ska styrelsen avge ett yttrande när en tillsynsmyndighet avser att godkänna kraven för ackreditering av certifieringsorgan enligt artikel 43. Syftet med detta yttrande är således att skapa ett harmoniserat förhållningssätt när det gäller de krav som en tillsynsmyndighet för dataskydd eller det nationella ackrediteringsorganet kommer att tillämpa för ackrediteringen av ett certifieringsorgan. I dataskyddsförordningen föreskrivs inte en enda uppsättning krav för ackreditering, men enhetlighet förordas. Styrelsen försöker uppnå detta mål genom sina yttranden, främst genom att uppmana tillsynsmyndigheterna att utforma sina krav för ackreditering enligt den struktur som fastställs i bilagan till dataskyddsstyrelsens riktlinjer om ackreditering av certifieringsorgan, och vidare genom att analysera dem med hjälp av en mall som styrelsen tillhandahåller, som gör det möjligt att jämföra kraven (med vägledning från ISO 17065 och dataskyddsstyrelsens riktlinjer om ackreditering av certifieringsorgan).

(2) Med hänvisning till artikel 43 i dataskyddsförordningen ska de behöriga tillsynsmyndigheterna anta ackrediteringskrav. De ska emellertid tillämpa mekanismen för enhetlighet för att se till att förtroendet för certifieringsmekanismen ökar, särskilt genom att fastställa höga krav.

(3) Även om kraven för ackreditering omfattas av mekanismen för enhetlighet innebär detta inte att kraven ska vara identiska. De behöriga tillsynsmyndigheterna har ett utrymme för skönsmässig bedömning när det gäller de nationella eller regionala förhållandena, och bör ta hänsyn till sin lokala lagstiftning. Syftet med dataskyddsstyrelsens yttrande är inte att uppnå en enda uppsättning av krav inom EU, utan snarare att undvika väsentliga avvikelser som exempelvis skulle kunna påverka förtroendet när det gäller de ackrediterade certifieringsorganens oberoende eller expertis.

(4) Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i den allmänna dataskyddsförordningen (2016/679) (nedan kallade *riktlinjerna*) och riktlinjer 1/2018 om certifiering och identifiering av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679, kommer att fungera som vägledning med avseende på mekanismen för enhetlighet.

[1] Hänvisningar till ”unionen” som görs i hela detta yttrande ska förstås som hänvisningar till ”EES”.

(5) Om en medlemsstat föreskriver att certifieringsorganen ska ackrediteras av tillsynsmyndigheten bör tillsynsmyndigheten fastställa ackrediteringskrav som inbegriper, men inte är begränsade till, de krav som anges i artikel 43.2. I jämförelse med skyldigheterna avseende nationella ackrediteringsorgans ackreditering av certifieringsorgan innehåller artikel 43 färre uppgifter om kraven för ackreditering när tillsynsmyndigheten själv genomför ackrediteringen. För att bidra till ett harmoniserat förhållningssätt till ackreditering bör de ackrediteringskrav som tillämpas av tillsynsmyndigheten vägledas av ISO/IEC 17065, och de bör kompletteras med ytterligare krav som en tillsynsmyndighet fastställer i enlighet med artikel 43.1 b. Europeiska dataskyddsstyrelsen noterar att man i artikel 43.2 a–e återspeglar och anger kraven i ISO 17065, vilket kommer att bidra till samstämmighet[2].

(6) Europeiska dataskyddsstyrelsens yttrande ska antas i enlighet med artikel 64.1 c, 64.3 och 64.8 i den allmänna dataskyddsförordningen, jämförd med artikel 10.2 i dataskyddsstyrelsens 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.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1 SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. Den tjeckiska tillsynsmyndigheten har lämnat in sitt utkast till ackrediteringskrav enligt artikel 43.1 b till Europeiska dataskyddsstyrelsen. Handlingarna i ärendet ansågs vara fullständiga den 17 februari 2020. Det nationella tjeckiska ackrediteringsorganet kommer att genomföra ackrediteringar av certifieringsorgan för att intyga att dessa tillämpar certifieringskriterier i enlighet med den allmänna dataskyddsförordningen. Detta innebär att det tjeckiska nationella ackrediteringsorganet kommer att tillämpa ISO 17065 och de ytterligare krav som fastställts av den tjeckiska tillsynsmyndigheten, när dessa har godkänts av myndigheten, efter ett yttrande från dataskyddsstyrelsen om utkastet till krav, för att ackreditera certifieringsorgan.
2. I enlighet med artikel 10.2 i styrelsens arbetsordning beslutade ordföranden, med tanke på komplexiteten i det aktuella ärendet, att förlänga den ursprungliga antagandeperioden på åtta veckor med ytterligare sex veckor.

[2] Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i den allmänna dataskyddsförordningen, punkt 39. Tillgängliga på: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_sv

2 BEDÖMNING

2.1 Dataskyddsstyrelsens allmänna resonemang i fråga om det inlämnade utkastet till beslut

3. Syftet med ett yttrande är att utvärdera de ackrediteringskrav som utarbetats av en tillsynsmyndighet, antingen på grundval av ISO 17065 eller en fullständig uppsättning krav, för att göra det möjligt för ett nationellt ackrediteringsorgan eller en tillsynsmyndighet, i enlighet med artikel 43.1 i dataskyddsförordningen, att ackreditera ett certifieringsorgan med ansvar för att utfärda och förnya certifieringar enligt artikel 42 i den förordningen. Detta påverkar inte den behöriga tillsynsmyndighetens uppgifter och befogenheter. I det aktuella fallet noterar dataskyddsstyrelsen att den tjeckiska tillsynsmyndigheten har valt att använda sig av det nationella ackrediteringsorganet för att utfärda ackrediteringar, efter att ha utarbetat ytterligare krav i enlighet med riktlinjerna som ackrediteringsorganet ska använda när det utfärdar en ackreditering.

4. Denna utvärdering av den tjeckiska tillsynsmyndighetens ytterligare ackrediteringskrav syftar till att undersöka hur de skiljer sig från riktlinjerna och i synnerhet bilaga 1 (i fråga om tillägg eller strykningar). Europeiska dataskyddsstyrelsens yttrande är även inriktat på alla aspekter som kan komma att inverka på enhetligheten när det gäller ackrediteringen av certifieringsorgan.

5. Det ska påpekas att riktlinjerna om ackreditering av certifieringsorgan ska tjäna som stöd för tillsynsmyndigheterna när de fastställer sina ackrediteringskrav. Bilagan till riktlinjerna utgör inte i sig ackrediteringskrav. Därför krävs det att tillsynsmyndigheten definierar ackrediteringskraven för certifieringsorgan så att en praktisk och enhetlig tillämpning blir möjlig, mot bakgrund av tillsynsmyndighetens arbete.

6. Med hänsyn till deras sakkunskap anser dataskyddsstyrelsen att det är viktigt att de nationella ackrediteringsorganen får ett visst handlingsutrymme vid utarbetandet av vissa specifika bestämmelser inom ramen för de tillämpliga ackrediteringskraven. Vid utarbetandet av ytterligare krav vill dataskyddsstyrelsen dock betona vikten av att dessa krav fastställs på ett sätt som möjliggör en praktisk och konsekvent tillämpning och granskning efter behov.

7. Dataskyddsstyrelsen konstaterar även att ISO-standarder, och i synnerhet ISO 17065, omfattas av immateriella rättigheter. Därför kommer dataskyddsstyrelsen i sitt yttrande inte att hänvisa till texten i det relaterade dokumentet. Dataskyddsstyrelsen har med anledning av detta beslutat att i förekommande fall hänvisa till specifika avsnitt i ISO-standarden utan att ordagrant återge texten.

8. Slutligen har dataskyddsstyrelsen genomfört sin bedömning i enlighet med den struktur som fastställs i bilaga 1 till riktlinjerna (nedan kallad *bilagan*). Om det inte står något i yttrandet om ett visst avsnitt i utkastet till ackrediteringskrav innebär detta att dataskyddsstyrelsen inte har några synpunkter i det aktuella fallet och att den tjeckiska tillsynsmyndigheten inte behöver vidta några ytterligare åtgärder.

9. I detta yttrande beaktas inte de dokument som lämnats in av den tjeckiska tillsynsmyndigheten som inte omfattas av artikel 43.2 i dataskyddsförordningen, t.ex. hänvisningar till nationell lagstiftning. Dataskyddsstyrelsen konstaterar dock att den nationella lagstiftningen bör överensstämma med dataskyddsförordningen när så krävs.

2.2 De viktigaste punkterna vid bedömningen (artikel 43.2 i dataskyddsförordningen och bilaga 1 till dataskyddsstyrelsens riktlinjer) av om ackrediteringskraven säkerställer att följande kan utvärderas på ett konsekvent sätt:

a. Behandling av alla viktiga områden som lyfts fram i bilagan till riktlinjerna och beaktande av eventuella avvikelser från bilagan.

b. Certifieringsorganets oberoende.

c. Intressekonflikter för certifieringsorganet.

d. Certifieringsorganets expertis.

e. Lämpliga säkerhetsåtgärder för att säkerställa att certifieringsorganet tillämpar certifieringskraven enligt dataskyddsförordningen på ett korrekt sätt.

f. Förfaranden för utfärdande, periodisk översyn och återkallande av en certifiering enligt dataskyddsförordningen.

g. Öppen hantering av klagomål om överträdelser av certifieringen.

10. Med beaktande av att det

a. i artikel 43.2 i dataskyddsförordningen finns en förteckning över krav på ackrediteringsområden som ett certifieringsorgan måste uppfylla för att ackrediteras,

b. i artikel 43.3 i dataskyddsförordningen föreskrivs att kraven för ackreditering av certifieringsorgan ska godkännas av den tillsynsmyndighet som är behörig,

c. i artikel 57.1 p och q i dataskyddsförordningen fastställs att en behörig tillsynsmyndighet måste utarbeta och offentliggöra kraven för ackreditering av certifieringsorgan och kan besluta att själv utföra ackrediteringen av certifieringsorgan,

d. i artikel 64.1 c i dataskyddsförordningen föreskrivs att dataskyddsstyrelsen ska avge ett yttrande när en tillsynsmyndighet avser att godkänna kraven för ackreditering av ett certifieringsorgan enligt artikel 43.3,

e. om ackreditering utförs av det nationella ackrediteringsorganet i enlighet med ISO/IEC 17065/2012 måste även ytterligare krav som fastställts av den behöriga tillsynsmyndigheten tillämpas,

f. bilaga 1 till riktlinjerna om ackreditering av certifieringsorgan innehåller förslag på krav som en tillsynsmyndighet kan upprätta och som ska tillämpas när det nationella ackrediteringsorganet ackrediterar ett certifieringsorgan,

anser dataskyddsstyrelsen följande:

2.2.1 INLEDNING

11. Dataskyddsstyrelsen medger att samarbetsvillkor, som reglerar förhållandet mellan ett nationellt ackrediteringsorgan och tillsynsmyndigheten för dataskydd, i sig inte utgör ett krav för ackreditering av certifieringsorgan. För tydlighetens och öppenhetens skull anser dock dataskyddsstyrelsen att

eventuella samarbetsvillkor ska offentliggöras i ett sådant format som tillsynsmyndigheten finner lämpligt.

2.2.2 ALLMÄNNA ANMÄRKNINGAR

12. Styrelsen konstaterar att utkastet till ackrediteringskrav inte helt följer den struktur som föreskrivs i bilaga 1 till riktlinjerna. Till exempel saknas avsnitten om ”tillämpningsområde” och ”begrepp och definitioner”. I detta hänseende anser styrelsen, för tydlighetens skull och för att underlätta bedömningen av kraven, att numreringen i dokumentet och dess övergripande struktur skulle kunna förbättras. I syfte att underlätta bedömningen uppmanar styrelsen därför den tjeckiska tillsynsmyndigheten att följa strukturen i bilagan i sitt utkast till ackrediteringskrav och lägga till de avsnitt som saknas, särskilt definitionerna av de begrepp som används genomgående i dokumentet. Vidare noterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav innehåller flera hänvisningar till respektive avsnitt i ISO 17065 eller till de respektive avsnitten i bilagan, dock utan att dessa referenser specificeras. Således uppmanar styrelsen den tjeckiska tillsynsmyndigheten att förtydliga hänvisningarna till avsnitten i ISO 17065 och i bilagan.

13. Styrelsen konstaterar att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav innehåller flera hänvisningar till det ”utvärderade objektet” (t.ex. avsnitten 3.2.1.2.1.2.10, 3.2.1.2.6.3.1, 3.2.1.2.8.1.6.3, 3.2.1.2.10.4.1, 3.1.2.10.7.3.1, 3.1.2.10.7.3.2 och 3.2.1.2.10.10.2). Styrelsen förstår att detta begrepp används som synonym till ”evalueringsobjekt”. För att säkerställa tydlighet uppmanar styrelsen emellertid den tjeckiska tillsynsmyndigheten att använda begreppet ”evalueringsobjekt” på ett enhetligt sätt.

14. Styrelsen konstaterar att flera krav inte är formulerade som en skyldighet för certifieringsorganet (t.ex. 3.2.1.2.2 och 3.2.1.2.3). Styrelsen uppmanar den tjeckiska tillsynsmyndigheten att omformulera kraven för att klargöra att de är tvingande, dvs. inleda kravet med ”certifieringsorganet ska [...]”

2.2.3 ALLMÄNNA KRAV FÖR ACKREDITERING

15. Vad gäller certifieringsavtalet (avsnitt 3.2.1.2.1.2 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav) noterar styrelsen att underavsnitt 3.2.1.2.1.2.2 inte innehåller någon hänvisning till ”frågor som är konfidentiella enligt avtal”, till vilka tillsynsmyndigheten också ska ha tillgång. Därför rekommenderar styrelsen den tjeckiska tillsynsmyndigheten att ändra utkastet genom att inkludera skyldigheten att även ge tillsynsmyndigheten tillgång till frågor som är konfidentiella enligt avtal.

16. Vad gäller underavsnitt 3.2.1.2.1.2.8 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav konstaterar styrelsen att det är oklart till vem informationen ska lämnas ut. Därför uppmanar styrelsen den tjeckiska tillsynsmyndigheten att klargöra vem som ska ta emot denna information. Vidare ska den utlämnade informationen vara ”nödvändig för att utfärda en certifiering”, såsom föreskrivs i punkt 7 i avsnitt 4.1.2 i bilagan. Styrelsen rekommenderar den tjeckiska tillsynsmyndigheten att ersätta ”information om utfärdande av en certifiering” med ”information nödvändig för att utfärda en certifiering”.

17. När det gäller underavsnitt 3.2.1.2.1.2.9 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav är det oklart vilken typ av information som ska meddelas direkt till styrelsen. Enligt artikel 42.8 i den allmänna dataskyddsförordningen föreskrivs en skyldighet för styrelsen att, bland annat, samla alla certifieringsmekanismer. I detta sammanhang antas de behöriga tillsynsmyndigheterna tillhandahålla den relevanta informationen till styrelsen, som sedan

offentliggör den i det offentliga registret. Därför rekommenderar styrelsen den tjeckiska tillsynsmyndigheten att förtydliga underavsnitt 3.2.1.2.1.2.9 i utkastet till krav i enlighet med artikel 42.8 i dataskyddsförordningen.

18. När det gäller underavsnitt 3.2.1.2.1.2.12 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav noterar styrelsen det faktum att den tjeckiska tillsynsmyndigheten har omformulerat delar av det krav som föreskrivs i bilagan. Den tjeckiska tillsynsmyndigheten har dock utelämnat en hänvisning (i förekommande fall) till att ”konsekvenserna för kunden även bör beaktas”. Styrelsen rekommenderar därför den tjeckiska tillsynsmyndigheten att lägga till den del av kravet ovan som saknas.

19. I underavsnitt 3.2.1.2.1.2.13 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav fastställs dessutom en skyldighet att ”innehålla ett åtagande från sökanden att informera certifieringsorganet om alla ändringar som kan påverka det certifierade objektets överensstämmelse med certifieringskriterierna”. Styrelsen anser att denna formulering är för allmän och rekommenderar den tjeckiska tillsynsmyndigheten att ändra utkastet till krav så att det omfattar ”alla förändringar i dess faktiska eller rättsliga situation och i de av dess produkter, processer och tjänster som berörs av certifieringen”.

20. När det gäller användningen av dataskyddsförsegling och dataskyddsmärkning (avsnitt 3.2.1.2.1.3 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav), konstaterar styrelsen att det i den tjeckiska tillsynsmyndighetens utkast till krav fastställs att certifieringsavtalet ska innehålla ”bestämmelser om användning av certifikat, försegling och märkning om dessa tillhandahålls av ägaren av certifieringssystemet”. Samma formulering återfinns i underavsnitt 3.2.1.2.1.2.14. Styrelsen anser att denna skyldighet redan omfattas av punkt 4.1.2.2 led I) i ISO 17065 och därför bör ingå i alla certifieringssystem (se även punkt 4.1.3 i ISO 17065). För tydlighetens skull rekommenderar styrelsen därför den tjeckiska tillsynsmyndigheten att radera ovannämnda avsnitt.

21. Vad gäller kraven på opartisk förvaltning omfattas avsnitt 4.2.1.b och 4.2.2 i bilagan, i enlighet med den information som den tjeckiska tillsynsmyndigheten har tillhandahållit i mallen, i tillräcklig utsträckning av punkt 4.2 i ISO 17065. Styrelsen anser emellertid att dessa krav uttryckligen ska tas med i det utkast till ackrediteringskrav som tillsynsmyndigheten har utarbetat i enlighet med bilagan. Därför rekommenderar styrelsen den tjeckiska tillsynsmyndigheten att inkludera de krav som saknas beträffande opartisk förvaltning som föreskrivs i bilagan.

22. Vad gäller kravet på ansvarighet och finansiering (avsnitt 3.2.1.2.3.1 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav) uppmanar styrelsen den tjeckiska tillsynsmyndigheten att specificera att det ska säkerställas regelbundet.

2.2.4 RESURSKRAV

23. När det gäller certifieringsorganets personal (avsnitt 3.2.1.2.8.1.6 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav), konstaterar styrelsen att kraven på personal med ansvar för utvärderingar (underavsnitt 3.2.1.2.8.1.6.3) omfattar *”fem års erfarenhet med minst tio genomförda revisioner som utförts inom certifieringsverksamhet inom samma eller ett liknande område [...] eller fem års erfarenhet inom certifiering av de objekt på vilka certifieringsorganet fokuserar)”*. På liknande sätt omfattar kraven för personal med ansvar för beslut (underavsnitt 3.2.1.2.8.1.6.4) ”*minst fem års erfarenhet med minst tio genomförda revisioner som utförts inom certifieringsverksamhet inom samma eller ett liknande område”*. Styrelsen anser att kraven på expertis för utvärderare och

beslutsfattare bör utformas med hänsyn till de olika arbetsuppgifter de utför. I detta avseende anser styrelsen att utvärderare bör ha en mer specialiserad expertis och yrkesmässig erfarenhet av tekniska förfaranden (t.ex. revisioner och certifiering), medan beslutsfattare bör ha en mer generell och övergripande expertis och yrkesmässig erfarenhet av dataskydd. Mot denna bakgrund uppmanar styrelsen den tjeckiska tillsynsmyndigheten att omformulera detta underavsnitt med hänsyn till skillnaderna när det gäller konkreta kunskaper och/eller krav på expertis för utvärderare och beslutsfattare.

24. Vidare noterar styrelsen att det i punkt 3.2.1.2.9.1 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav anges att det inte är tillåtet att anlita underleverantörer för certifieringsverksamhet. Enligt de följande punkterna är det emellertid tillåtet att använda externa revisorer och externa experter för utvärdering, såvida det inte är frågan om certifieringsverksamhet. Styrelsen anser att det bör specificeras i utkastet till ackrediteringskrav när ”det är frågan om certifieringsverksamhet” eller klargöras att certifieringsorganet fortsatt ansvarar för beslutsfattandet, även om det använder externa experter. Styrelsen rekommenderar därför den tjeckiska tillsynsmyndigheten att ändra utkastet i enlighet med detta.

2.2.5 PROCESSKRAV

25. Styrelsen konstaterar att det i avsnitt 3.2.1.2.10.1.1 i den tjeckiska tillsynsmyndighetens utkast till ytterligare krav finns en hänvisning till ”alla ytterligare krav som rör en intressekonflikt (7.1 punkt 1)”. Den tjeckiska tillsynsmyndighetens utkast till ytterligare krav innehåller emellertid inte några ytterligare krav avseende intressekonflikter. Styrelsen uppmanar därför den tjeckiska tillsynsmyndigheten att ändra utkastet för att undvika missförstånd.

26. När det gäller ansökningskraven noterar styrelsen att underavsnitt 3.2.1.2.10.2.3 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav antyder att information om de överförda uppgifterna endast ska tillhandahållas i ansökan om överföringen görs till ett tredjeland eller till en internationell organisation. Styrelsen understryker emellertid att sökanden alltid ska tillhandahålla en beskrivning av de uppgifter som överförs till andra system eller organisationer, oberoende av var de är lokaliserade. Därför rekommenderar styrelsen den tjeckiska tillsynsmyndigheten att ändra ordalydelsen för att undvika missförstånd.

27. Styrelsen noterar att skyldigheten att fastställa de bindande utvärderingsmetoderna i certifieringsavtalet (avsnitt 3.2.1.2.1.2.6 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav) inte innehåller någon hänvisning till evalueringsobjektet, såsom föreskrivs i punkt 1 i avsnitt 7.3 i bilagan till riktlinjerna. I klargörande syfte uppmanar styrelsen den tjeckiska tillsynsmyndigheten att inkludera en sådan hänvisning.

28. Vidare konstaterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav regler situationer när personuppgiftsbiträden används för att genomföra databehandling, i enlighet med bilagan till riktlinjerna (avsnitt 3.2.1.2.10.2 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav). Styrelsen uppmanar den tjeckiska tillsynsmyndigheten att överväga huruvida det i detta fall även bör införas en hänvisning till gemensamma personuppgiftsansvariga och deras specifika överenskommelser.

29. När det gäller utvärderingskrav (avsnitt 3.2.1.2.10.4 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav), konstaterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till

ackrediteringskrav inte innehåller någon skyldighet för certifieringsorganet att ange i sin certifieringsmekanism hur den information som krävs i punkt 7.4.6 i ISO 17065 om avvikelser från en certifieringsmekanism ska tillhandahållas sökanden. Såsom föreskrivs i bilagan (underavsnitt 7.4) bör åtminstone informationens typ och tidpunkten för den anges. Styrelsen rekommenderar därför den tjeckiska tillsynsmyndigheten att lägga till ovannämnda skyldighet.

30. I underavsnitt 3.2.1.2.10.4.2 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav förefaller utvärderingsmetoderna vidare vara begränsade till testning, revision eller inspektioner. Styrelsen anser att andra utvärderingsmetoder också kan användas och uppmanar därför den tjeckiska tillsynsmyndigheten att ändra utkastet för att klargöra att uppräkningen inte är uttömmande.

31. När det gäller underavsnitt 3.2.1.2.10.4.4.1.4 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav anser styrelsen att det klart bör anges i kraven att certifieringsorganet är skyldigt att kontrollera efterlevnaden av kriterierna och uppmanar den tjeckiska tillsynsmyndigheten att ändra utkastet i enlighet med detta.

32. Med hänsyn till utvärderingskraven (underavsnitt 3.2.1.2.10.5 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav) noterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav inte innehåller någon hänvisning till skyldigheten att fastställa förfaranden för beviljande och återkallande av certifieringar. Styrelsen rekommenderar den tjeckiska tillsynsmyndigheten att ändra utkastet i enlighet med detta.

33. Vad gäller kraven på certifieringsdokumentation noterar styrelsen att det i avsnitt 3.1.2.10.7.2 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav anges att certifieringsorganet ska specificera att övervakning är ett villkor för att certifieringen ska vara giltig ”om övervakning krävs enligt ett certifieringssystem [...]”. I frågan om certifiering enligt dataskyddsförordningen anser styrelsen att övervakning alltid är obligatorisk och rekommenderar därför den tjeckiska tillsynsmyndigheten att inkludera en sådan skyldighet.

34. När det gäller kraven rörande katalogen över certifierade produkter (avsnitt 3.2.1.2.10.8 i den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav och punkt 7.8 i bilagan), och i synnerhet skyldigheten att informera den behöriga tillsynsmyndigheten om skälen till beviljande eller återkallande av den begärda certifieringen, noterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav hänvisar till avsnitt 3.2.1.2.10.4.5. Detta avsnitt rör emellertid skyldigheten att på begäran ge den tjeckiska tillsynsmyndigheten tillgång till utvärderingsdokumentation, medan kravet i avsnitt 7.8 i bilagan till riktlinjerna innehåller en skyldighet att proaktivt informera tillsynsmyndigheten om skälen till beviljande eller återkallande av certifieringen. Styrelsen rekommenderar därför den tjeckiska tillsynsmyndigheten att ändra utkastet i enlighet med detta.

35. Vad gäller de ändringar som påverkar certifieringen noterar styrelsen att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav, bland de förfaranden som man kommer överens om, saknar en hänvisning till den behöriga tillsynsmyndighetens godkännandeförfarande, till vilket hänvisas i bilagan till riktlinjerna (sidan 19). Styrelsen medger att den förteckning som tillhandahålls i avsnitt 7.10 i bilagan inte är bindande. För att säkerställa enhetlighet uppmanar styrelsen emellertid den tjeckiska tillsynsmyndigheten att lägga till en hänvisning till tillsynsmyndighetens godkännandeförfarande.

36. Dataskyddsstyrelsen noterar att den tjeckiska tillsynsmyndighetens utkast till ackrediteringskrav inte tydligt omfattar certifieringsorganets skyldighet att godta beslut och påbud från den behöriga tillsynsmyndigheten om att återkalla eller inte utfärda certifiering till en sökande om kraven inte längre är uppfyllda. Styrelsen rekommenderar den tjeckiska tillsynsmyndigheten att på ett tydligt sätt lägga till en sådan skyldighet i utkastet till krav för ackreditering. Vad gäller avslutande, begränsning, tillfällig indragning eller återkallelse av certifiering noterar styrelsen att avsnitten 3.2.1.2.10.10.2 och 3.2.1.2.10.10.3 i utkastet till krav hänvisar till en ”anstiftan”. Om avsikten är att hänvisa till ”beslut och förelägganden” från tillsynsmyndigheten, enligt vad som fastställs i artikel 58.2 h i dataskyddsförordningen, uppmanar styrelsen den tjeckiska tillsynsmyndigheten att använda samma terminologi som i dataskyddsförordningen och hänvisa till ”beslut och förelägganden”.

2.2.6 FÖRVALTNINGSSYSTEM

37. Styrelsen anser att avsnitt 3.2.1.2.11 i den tjeckiska tillsynsmyndighetens ytterligare krav inte innehåller skyldigheten från certifieringsorganet att ”permanent och kontinuerligt offentliggöra vilka certifieringar som utförts på vilken grund, hur länge certifieringarna gäller enligt vilka regler och vilka villkor som gäller”, såsom anges i avsnitt 8 i bilagan. Styrelsen rekommenderar därför den tjeckiska tillsynsmyndigheten att ändra utkastet till krav genom att inkludera ovannämnda hänvisning.

3 SLUTSATSER OCH REKOMMENDATIONER

38. Den tjeckiska tillsynsmyndighetens utkast till krav för ackreditering kan leda till inkonsekvent tillämpning av ackrediteringen av certifieringsorgan, och följande ändringar behöver göras:

39. Vad gäller ”de allmänna kraven för ackreditering” rekommenderar styrelsen att den tjeckiska tillsynsmyndigheten

    1) inkluderar skyldigheten att ge tillsynsmyndigheten tillgång till ”frågor som är konfidentiella enligt avtal” i avsnitt 3.2.1.2.1.2,

    2) ersätter ”information om utfärdande av en certifiering” med ”information nödvändig för att utfärda en certifiering” i underavsnitt 3.2.1.2.1.2.8,

    3) förtydligar underavsnitt 3.2.1.2.1.2.9 i överensstämmelse med artikel 42.8 i dataskyddsförordningen,

    4) i underavsnitt 3.2.1.2.1.2.12 lägger till en hänvisning (i förekommande fall) till att ”konsekvenserna för kunden även bör beaktas”,

    5) ändrar underavsnitt 3.2.1.2.1.2.13 så att det omfattar ”alla förändringar i dess faktiska eller rättsliga situation och i de av dess produkter, processer och tjänster som berörs av certifieringen”,

    6) raderar avsnitt 3.2.1.2.1.3 och underavsnitt 3.2.1.2.1.2.14,

    7) inkluderar de krav som saknas vad gäller opartisk förvaltning som föreskrivs i bilagan.

40. När det gäller ”resurskraven” rekommenderar styrelsen att den tjeckiska tillsynsmyndigheten

1) ändrar avsnitt 3.2.1.2.9.1 för att specificera när ”det utgör certifieringsverksamhet” eller klargör att certifieringsorganet fortsatt ansvarar för beslutsfattandet, även om det använder externa experter.

41. När det gäller ”processkraven” rekommenderar styrelsen att den tjeckiska tillsynsmyndigheten

1) i avsnitt 3.2.1.2.10.4 inkluderar skyldigheten för certifieringsorganet att ange i sin certifieringsmekanism hur den information som krävs i punkt 7.4.6 i ISO 17065 om avvikelser från en certifieringsmekanism ska tillhandahållas sökanden,

2) ändrar avsnitt 3.2.1.2.10.5 för att hänvisa till skyldigheten att fastställa förfaranden för beviljande och återkallande av certifieringar,

3) ändrar avsnitt 3.1.2.10.7.2 så att det återspeglar att övervakning alltid är obligatorisk när det gäller certifiering enligt dataskyddsförordningen,

4) ändrar avsnitt 3.2.1.2.10.8 för att återspegla certifieringsorganets skyldighet att proaktivt informera tillsynsmyndigheten om skälen till beviljande eller återkallande av certifieringen,

5) inkluderar certifieringsorganets skyldighet att godta beslut och påbud från den behöriga tillsynsmyndigheten om att återkalla eller inte utfärda certifiering till en sökande om kraven för certifiering inte längre är uppfyllda.

42. När det gäller ”förvaltningssystemet” rekommenderar styrelsen att den tjeckiska tillsynsmyndigheten

1) inkluderar certifieringsorganets skyldighet att ”permanent och kontinuerligt offentliggöra vilka certifieringar som utförts på vilken grund, hur länge certifieringarna gäller enligt vilka regler och vilka villkor som gäller”, såsom anges i avsnitt 8 i bilagan.

4 AVSLUTANDE ANMÄRKNINGAR

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

44. Enligt artikel 64.7 och 64.8 i dataskyddsförordningen ska den tjeckiska tillsynsmyndigheten, inom två veckor efter att yttrandet inkommit, på elektronisk väg meddela ordföranden om huruvida den kommer att hålla fast vid eller ändra utkastet till förteckning. Inom samma period ska den tillhandahålla det ändrade utkastet till beslut eller, om den inte avser att följa styrelsens yttrande, tillhandahålla en relevant motivering till varför den inte avser att följa detta yttrande, helt eller delvis.

45. Den tjeckiska tillsynsmyndigheten ska meddela styrelsen om det slutliga beslutet för att det ska införas i registret över beslut som hanteras inom mekanismen för enhetlighet, i enlighet med artikel 70.1 y i dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)

Antaget