Yttrande från styrelsen (art. 64)

Yttrande 05/2021 om utkastet till administrativ överenskommelse för överföring av personuppgifter mellan

Haut Conseil du Commissariat aux Comptes (H3C)
och
Public Company Accounting Oversight Board (PCAOB)

Antaget den 2 februari 2021

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

Innehållsförteckning

Europeiska dataskyddsstyrelsen har avgett detta yttrande

med beaktande av artiklarna 63, 64.2, 64.3–64.8 och 46.3 b i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (den allmänna *dataskyddsförordningen*),

med beaktande av dataskyddsstyrelsens riktlinjer 2/2020 om artikel 46.2 a och 46.3 b i förordning 2016/679 för överföringar av personuppgifter mellan offentliga myndigheter och organ i EES-länder och länder utanför EES, antagna den 15 december 2020,

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 10 och 22 i arbetsordningen, och

av följande skäl:

1) Med hänvisning till artikel 46.1, 46.3 b och 46.4 i dataskyddsförordningen
får en personuppgiftsansvarig eller ett personuppgiftsbiträde, i avsaknad av ett beslut i enlighet med artikel 45.3, endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga. Med förbehåll för tillstånd från den behöriga tillsynsmyndigheten får lämpliga skyddsåtgärder också i synnerhet ta formen av bestämmelser som införs i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

2) Med hänsyn till att de administrativa överenskommelser som föreskrivs i artikel 46.3 b har särskilda egenskaper[2], vilka kan variera avsevärt, bör varje fall hanteras individuellt och utan att det påverkar bedömningen av någon annan administrativ överenskommelse.

3) Enligt artikel 70.1 i den allmänna dataskyddförordningen ska dataskyddsstyrelsen se till att förordning 2016/679 tillämpas enhetligt i hela Europeiska ekonomiska samarbetsområdet. Enligt artikel 64.2 kan mekanismen för enhetlighet
tillämpas av en tillsynsmyndighet, styrelsens ordförande eller kommissionen med avseende på en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat. Styrelsen ska avge ett yttrande i den fråga som ingivits till den, förutsatt att den inte redan har avgett ett yttrande i samma fråga.

4) Styrelsens yttrande ska antas i enlighet med artikel 64.3 i den allmänna dataskyddsförordningen jämförd med artikel 10.2 i styrelsens arbetsordning inom åtta veckor efter det att ordföranden har beslutat att handlingarna är fullständiga. Genom beslut av styrelsens ordförande får denna period förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet.

5) I artikel 65.1 c i den allmänna dataskyddsförordningen föreskrivs att om en behörig tillsynsmyndighet inte följer ett yttrande som styrelsen avger enligt artikel 64 får varje berörd

[1] Hänvisningar till ”medlemsstater” i detta yttrande ska förstås som hänvisningar till ”medlemsstater i EES”.
[2] Se även skäl 108 i den allmänna dataskyddsförordningen.

tillsynsmyndighet eller kommissionen översända ärendet till styrelsen, vilken ska anta ett bindande beslut.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

1 SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. *Haut Conseil du Commissariat aux Comptes* (H3C) har genom en officiell skrivelse till den franska tillsynsmyndigheten (*Commission Nationale de l'Informatique et des Libertés*) lämnat in ett utkast till administrativ överenskommelse (*utkastet*) avsett som en ram för överföringar av personuppgifter från H3C till PCAOB i enlighet med artikel 46.3 b i den allmänna dataskyddsförordningen.

2. Detta utkast översändes till den franska tillsynsmyndigheten den 19 november 2020.

3. Den franska tillsynsmyndigheten har därefter begärt ett yttrande från styrelsen enligt artikel 64.2 i den allmänna dataskyddsförordningen. Beslutet om handlingarnas fullständighet antogs den 9 december 2020.

2 BEDÖMNING

4. Utbytet av personuppgifter mellan H3C och PCAOB är nödvändigt för att säkerställa deras tillsynsfunktion på revisionsområdet i enlighet med *Sarbanes-Oxley Act* och artikel 47 i Europaparlamentets direktiv 2006/43/EG[3], nämligen för revisionstillsyn, inspektioner och granskningar av registrerade revisionsbyråer och personer knutna till dessa som omfattas av PCAOB:s och H3C:s tillsynsbefogenheter.

5. Andra revisionsmyndigheter i EES omfattas av ett liknande behov av att utbyta personuppgifter med PCAOB. Således kan andra revisionsmyndigheter i EES se det aktuella utkast som ingetts till styrelsen för yttrande som en modell att följa när de utformar en ram för samma slags överföringar av personuppgifter till PCAOB i sina särskilda administrativa överenskommelser, vilka i sin tur måste inges till den behöriga tillsynsmyndigheten för godkännande. Mot denna bakgrund får frågan följder i mer än en medlemsstat i den mening som avses i artikel 64.2 i den allmänna dataskyddsförordningen.

6. Vid sin bedömning av bestämmelserna i den särskilda administrativa överenskommelsen har styrelsen beaktat ett antal särskilda inslag, bl.a. vilken typ av personuppgifter överenskommelsen omfattar och de mål som eftersträvas.

7. Utkastet och dess bilagor innehåller följande garantier:

Definitioner av begrepp och registrerades rättigheter:

8. I artikel I i överenskommelsen fastställs de relevanta definitioner som är nödvändiga för att fastställa dess räckvidd samt enhetliga tillämpning. Detta omfattar exempelvis vissa definitioner av centrala begrepp och rättigheter från den unionsrättsliga ramen för dataskydd, såsom ”personuppgifter”, ”behandling av personuppgifter”, ”personuppgiftsincident”, ”rätt till tillgång” och ”rätt till radering”.

[3] Europaparlamentets och rådets direktiv 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG.

Principen om ändamålsbegränsning och förbud mot all ytterligare behandling:

9. I artikel III.1 i överenskommelsen föreskrivs att PCAOB själv endast får behandla personuppgifter som H3C har överfört för att myndigheten ska kunna fullgöra sina tillsynsuppgifter på revisionsområdet i enlighet med *Sarbanes-Oxley Act* för revisionstillsyn, inspektioner och granskningar av registrerade revisionsbyråer och personer knutna till dessa som omfattas av PCAOB:s och H3C:s tillsynsbefogenheter. Enligt principen om ändamålsbegränsning kan överföringar därför endast genomföras inom ramen för sådana bemyndiganden och ett sådant ansvar. PCAOB får inte behandla personuppgifter som myndigheten erhåller för andra ändamål än de som föreskrivs i överenskommelsen.

10. I själva verket efterfrågar PCAOB huvudsakligen namn på enskilda personer (tillsammans med information som hänför sig till deras yrkesverksamhet) som varit ansvariga för eller deltagit i revisionsuppdrag som valts ut för översyn under en inspektion eller en granskning, eller som spelar en viktig roll i företagets förvaltning och kvalitetskontroll. PCAOB kommer att använda sådan information för att bedöma i vilken grad de registrerade revisionsbyråerna och personer som är knutna till dessa följer bestämmelserna i *Sarbanes-Oxley Act*, värdepapperslagstiftningen beträffande utarbetande och utfärdande av revisionsberättelser, PCAOB:s regler, SEC:s regler samt relevanta yrkesstandarder med koppling till genomförandet av revisioner, utfärdandet av revisionsberättelser och relaterade frågor som rör emittenter (såsom de definieras i *Sarbanes-Oxley Act*).

Principen om datakvalitet och proportionalitet:

11. Enligt artikel III.2 i överenskommelsen ska de personuppgifter som H3C överför vara korrekta, adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de överförs och senare behandlas.

12. Dessutom ska varje part informera den andra parten om den får kännedom om att information som överförts eller erhållits tidigare är felaktig och/eller måste uppdateras. Parterna ska, med beaktande av de ändamål för vilka personuppgifterna har överförts, vidta lämpliga rättelser av sina respektive handlingar, vilket i förekommande fall kan omfatta att komplettera, radera, begränsa behandlingen av, korrigera eller på annat sätt rätta personuppgifterna.

Öppenhetsprincipen:

13. Såsom föreskrivs i artikel III.3 i överenskommelsen kommer både H3C och PCAOB att tillhandahålla allmän information till de registrerade genom att själva överenskommelsen offentliggörs på deras webbplatser. Utöver överenskommelsen kommer H3C att tillhandahålla information beträffande den behandling som utförs, inbegripet överföringen, den typ av enheter till vilka uppgifterna kan komma att överföras, de rättigheter som är tillgängliga till dem i enlighet med de tillämpliga rättsliga kraven, inbegripet hur dessa rättigheter kan utövas, samt information om eventuella dröjsmål eller restriktioner angående utövandet av sådana rättigheter och kontaktuppgifter för hänskjutande av en tvist eller ett anspråk. PCAOB kommer även att offentliggöra lämplig information om sin behandling av personuppgifter på sin webbplats, inbegripet den information som anges ovan, såsom beskrivs i överenskommelsen. Vidare kommer H3C att lämna information till enskilda registrerade i enlighet med den allmänna dataskyddsförordningen. H3C ska i förväg underrätta PCAOB om sådan information till enskilda.

Principen om lagring av uppgifter:

14. I artikel III.2 i överenskommelsen föreskrivs att personuppgifter ska lagras på ett sätt som inte möjliggör identifiering av de registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in och sedan behandlades, alternativt under den tid som krävs enligt tillämpliga lagar och regler. Parterna ska ha inrättat lämpliga förfaranden för radering av uppgifter med avseende på all information som erhållits enligt denna överenskommelse.

Säkerhets- och sekretessåtgärder:

15. I artikel III.4 i överenskommelsen föreskrivs att PCAOB ska tillhandahålla information (bilaga I i överenskommelsen) som beskriver dess tekniska och organisatoriska säkerhetsåtgärder för att skydda mot oavsiktlig eller olaglig förstöring, förlust, ändring eller utlämnande av eller åtkomst till personuppgifter. PCAOB förbinder sig att informera H3C om eventuella ändringar av de tekniska och organisatoriska säkerhetsåtgärder som skulle inverka negativt på skyddsnivån för personuppgifter enligt överenskommelsen. PCAOB ska även uppdatera informationen i bilaga I om sådana ändringar företas. Om PCAOB lämnar sådan information till H3C ska sistnämnda myndighet underrätta den franska dataskyddsmyndigheten om dessa ändringar.

16. PCAOB har även gett H3C en beskrivning av sina tillämpliga lagar och/eller bestämmelser om konfidentialitet och följderna av eventuellt olagliga utlämnanden av icke-offentlig eller konfidentiell information eller misstänkta överträdelser av dessa lagar och/eller bestämmelser.

17. Slutligen ska PCAOB, om myndigheten får kännedom om en personuppgiftsincident, utan onödigt dröjsmål och, om så är möjligt, inom 24 timmar efter att ha fått vetskap om att incidenten påverkar sådana personuppgifter, underrätta H3C om den. PCAOB ska även så snart som möjligt vidta rimliga och lämpliga åtgärder för att avhjälpa incidenten och minimera de potentiella negativa effekterna.

Åtgärder för att skydda de registrerades rättigheter:

18. I artikel III.5 i överenskommelsen föreskrivs säkerhetsåtgärder som hänför sig till de registrerades rättigheter. I synnerhet kan registrerade vars personuppgifter har överförts till PCAOB utöva sina rättigheter såsom de definieras i artikel I.j i överenskommelsen, bl.a. genom att begära att H3C identifierar eventuella personuppgifter som har överförts till PCAOB. Vidare kan registrerade direkt begära att H3C får bekräftat av PCAOB att deras personuppgifter är fullständiga, korrekta och, i förekommande fall, uppdaterade och att behandlingen överensstämmer med principerna i denna överenskommelse. PCAOB ska hantera sådana eventuella förfrågningar från H3C om personuppgifter som H3C överfört till PCAOB inom rimlig tid. Registrerade kan även kontakta PCAOB direkt.

19. Eventuella begränsningar av dessa rättigheter måste föreskrivas i lag samt vara nödvändiga och ska pågå endast så länge som skälet för begränsningen fortfarande föreligger. Sådana begränsningar kan vara tillåtna för att undvika påverkan eller skada på tillsyns- eller verkställighetsfunktioner från parterna när de agerar inom ramen för sin myndighetsutövning, såsom övervakning eller bedömning av efterlevnaden av partens tillämpliga lagar eller förebyggande eller utredning av misstänkta brott. Vidare kan de vara tillåtna för viktiga mål av allmänt intresse som är erkända i Förenta staterna och i Frankrike eller i Europeiska unionen, inbegripet av hänsyn till andan av ömsesidighet inom internationellt samarbete eller för övervakning av reglerade personer och enheter.

Automatiserat beslutsfattande:

20. I artikel III.5 föreskrivs att PCAOB inte kommer att fatta några rättsliga beslut om en registrerad som enbart grundas på automatiserad behandling av personuppgifter, inbegripet profilering, utan personlig kontakt.

Särskilda kategorier av personuppgifter/känsliga uppgifter:

21. I artikel III.6 föreskrivs att H3C inte ska överföra särskilda kategorier av personuppgifter/känsliga uppgifter till PCAOB.

Begränsningar av vidare överföring av personuppgifter:

22. Enligt artikel III.7 i överenskommelsen ska PCAOB enbart dela personuppgifter som erhållits från H3C med de enheter som anges i bilaga II till överenskommelsen. Vid sådan delning, förutom med den amerikanska *Securities and Exchange Commission*, ska PCAOB i förväg begära skriftligt godkännande från H3C och kommer endast att dela sådana personuppgifter om den tredje parten lämnar lämpliga garantier som överensstämmer med säkerhetsåtgärderna i överenskommelsen. När PCAOB begär sådant skriftligt godkännande i förväg ska myndigheten underrätta H3C om vilken typ av personuppgifter den avser dela och skälen och de ändamål för vilka delningen ska äga rum, för att H3C ska kunna lämna samtycke. Om H3C inte lämnar skriftligt samtycke till sådan delning inom högst tio dagar ska PCAOB samråda med H3C och beakta eventuella invändningar från sistnämnda myndighet. Om PCAOB beslutar att dela personuppgifter utan skriftligt godkännande från H3C, ska PCAOB underrätta H3C och den sistnämnda kan då besluta om att eventuellt avbryta överföringen av personuppgifter. Beslutet ska anmälas till den franska dataskyddsmyndigheten. Om den tredje parten inte kan tillhandahålla nödvändiga garantier kan personuppgifterna dessutom, undantagsvis, delas med den tredje parten med H3C:s samtycke om delningen av personuppgifterna sker på grund av viktiga skäl av allmänt intresse, såsom de erkänns i Förenta staterna och i Frankrike eller i Europeiska unionen, eller om delningen är nödvändig för fastställande eller utövande av eller försvar mot rättsliga anspråk.

23. Vad gäller delning av personuppgifter med den amerikanska *Securities and Exchange Commission*, ska PCAOB erhålla lämpliga garantier från förstnämnda myndighet som överensstämmer med säkerhetsåtgärderna i överenskommelsen. Dessutom kommer PCAOB regelbundet att informera H3C om vilken typ av personuppgifter som delas och skälet för delningen, såvida denna information inte riskerar att äventyra en pågående utredning. Sådana begränsningar av information som hänför sig till en pågående utredning ska fortsätta tillämpas endast så länge som skälet för begränsningen fortfarande består.

24. Slutligen kan en registrerad begära viss information från H3C om de personuppgifter myndigheten har överfört till PCAOB som rör honom eller henne. H3C är skyldig att tillhandahålla sådan information i enlighet med de tillämpliga rättsliga kraven i den allmänna dataskyddsförordningen och i den franska dataskyddslagen.

Prövning:

25. I artikel III.8 i överenskommelsen fastställs en prövningsmekanism. Enligt överenskommelsen har den registrerade tillgång till fyra prövningsnivåer. Inledningsvis kan eventuella tvister eller anspråk från den registrerade som rör behandlingen av dennes personuppgifter enligt överenskommelsen riktas mot H3C, PCAOB eller i förekommande fall mot båda dessa myndigheter. Varje part ska informera den andra parten om sådana eventuella tvister eller anspråk och ska göra sitt bästa för att reglera tvisten eller anspråket i godo inom rimlig tid.

26. PCAOB ska informera H3C om anmälningar som myndigheten erhåller från registrerade och ska samråda med H3C om hur ärendet ska hanteras.

27. I ett andra steg, om en part eller parterna inte kan lösa ett problem eller ett klagomål från en registrerad och ärendet inte är uppenbarligen ogrundat eller orimligt, kan den registrerade, parten eller parterna tillämpa ett första steg från en lämplig tvistlösningsmekanism som genomförs av en oberoende funktion inom PCAOB, kallad förhörsombudet (*Hearing Officer*).

28. I ett tredje steg kan det beslut som antagits genom denna tvistlösningsmekanism överlämnas för en andra oberoende granskning, vilken genomförs av en separat oberoende prövningsgranskare (*Redress Reviewer*). Såväl beslut från förhörsombudet som från prövningsgranskaren är bindande för PCAOB. Tvistlösningsmekanismerna beskrivs i detalj i bilaga III till överenskommelsen.

29. I situationer där H3C anser att PCAOB inte har agerat i enlighet med de säkerhetsåtgärder som föreskrivs i överenskommelsen, får H3C avbryta överföringarna fram till dess att frågan har behandlats på ett tillfredsställande sätt och får informera den registrerade om detta.

30. Slutligen kan den registrerade i vart fall utöva sin rätt till rättslig eller administrativ prövning (inbegripet skadestånd) enligt den franska lagstiftningen om dataskydd.

Tillsynsmekanism:

31. I artikel III.9 i överenskommelsen föreskrivs en tillsynsmekanism som ska säkerställa att skyddsåtgärderna i överenskommelsen genomförs. Tillsynsmekanismen består av en kombination av intern och extern tillsyn.

32. Vad gäller intern tillsyn, ska varje part regelbundet se över sina egna riktlinjer och rutiner för genomförandet av säkerhetsåtgärderna i överenskommelsen. En part ska se över sina riktlinjer och rutiner på motiverad begäran från den andra parten för att säkerställa och bekräfta att de säkerhetsåtgärder som anges i denna överenskommelse genomförs på ett effektivt sätt och översända en sammanfattning av översynen till den andra parten.

33. Vad gäller extern tillsyn, kan H3C begära att PCAOB genomför en oberoende granskning av efterlevnaden av säkerhetsåtgärderna i överenskommelsen. PCAOB ska då begära att byrån för intern översyn och resultatgarantier (*Office of Internal Oversight and Performance Assurance*, IOPA), vilken utgör en oberoende byrå inom PCAOB, genomför en granskning för att säkerställa och bekräfta att säkerhetsåtgärderna i överenskommelsen genomförs på ett effektivt sätt. Närmare uppgifter om IOPA:s funktion tillhandahålls i bilaga IV till överenskommelsen. IOPA ska tillhandahålla en sammanfattning av resultaten från sin granskning till H3C så snart PCAOB:s styrelse har godkänt utlämnandet av sammanfattningen till H3C.

34. Om H3C inte har erhållit resultaten från IOPA:s granskning och anser att PCAOB inte har handlat i överensstämmelse med de särskilda säkerhetsåtgärder som gäller för dess skyldigheter enligt överenskommelsen, får H3C avbryta överföringarna till PCAOB till dess att sistnämnda myndighet har hanterat frågan på ett tillfredsställande sätt. Ett sådant avbrott måste anmälas till den franska dataskyddsmyndigheten.

3 SLUTSATSER/REKOMMENDATIONER

35. Styrelsen välkomnar de ansträngningar som gjorts i denna överenskommelse, vilket omfattar ett antal viktiga säkerhetsåtgärder som överensstämmer med den allmänna dataskyddsförordningen samt även med de säkerhetsåtgärder som föreskrivs i styrelsens riktlinjer 2/2020. För att säkerställa att dessa säkerhetsåtgärder fortfarande garanterar en lämplig dataskyddsnivå när uppgifter överförs till PCAOB

vill dataskyddsstyrelsen, med hänsyn till den unika karaktär som sådana icke-bindande överenskommelser har, framhålla följande:

- Den franska tillsynsmyndigheten kommer att övervaka överenskommelsen och dess tillämpning i praktiken, särskilt i förhållande till artikel III.7, III.8 och III.9 avseende vidare överföringar, prövning och tillsynsmekanismer. Detta för att säkerställa att de registrerade har tillgång till faktiska och verkställbara rättigheter, lämplig prövning och att efterlevnaden av överenskommelsen övervakas på ett effektivt sätt.
- Den franska tillsynsmyndigheten ska endast godkänna denna överenskommelse som en lämplig dataskyddsmekanism med avseende på gränsöverskridande överföring av uppgifter, under förutsättning att de undertecknande parterna till fullo uppfyller alla klausuler i överenskommelsen.
- Den franska tillsynsmyndigheten ska avbryta det relevanta dataflödet från H3C i enlighet med godkännandet om det inte längre föreskrivs lämpliga säkerhetsåtgärder i den mening som avses i den allmänna dataskyddsförordningen i överenskommelsen.

4 AVSLUTANDE KOMMENTARER

36. Detta yttrande ska offentliggöras i enlighet med artikel 64.5 b i den allmänna dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)