

Parere del comitato (articolo 64)



**Parere 5/2021 sul progetto di accordo amministrativo per il
trasferimento di dati personali tra**

**l'Haut Conseil du Commissariat aux Comptes (H3C)
e
il Public Company Accounting Oversight Board (PCAOB)**

Adottato il 2 febbraio 2021

Indice

1	Sintesi dei fatti.....	4
2	Valutazione.....	4
3	Conclusioni e raccomandazioni.....	9
4	Osservazioni conclusive.....	9

Il Comitato europeo per la protezione dei dati

visto l'articolo 63, l'articolo 64, paragrafo 2 e paragrafi da 3 a 8, l'articolo 46, paragrafo 3, lettera b), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (in appresso "GDPR"),

viste le linee-guida 2/2020 dell'EDPB sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità pubbliche e organismi pubblici del SEE e di paesi non appartenenti al SEE, adottate il 15 dicembre 2020,

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018¹,

visti gli articoli 10 e 22 del proprio regolamento interno,

considerando quanto segue:

1) Con riferimento all'articolo 46, paragrafo 1 e paragrafo 3, lettera b) e all'articolo 46, paragrafo 4, del GDPR, in mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

2) Tenuto conto delle caratteristiche specifiche degli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b)², che possono variare considerevolmente, ciascun caso dovrebbe essere trattato individualmente e non pregiudica la valutazione di ogni altro accordo amministrativo.

3) L'EDPB garantisce, a norma dell'articolo 70, paragrafo 1, del GDPR, l'applicazione coerente del regolamento (UE) 2016/679 in tutto lo Spazio economico europeo. Conformemente all'articolo 64, paragrafo 2, il meccanismo di coerenza può essere attivato da un'autorità di controllo, dal presidente dell'EDPB o dalla Commissione per qualsiasi questione di applicazione generale o che produce effetti in più di uno Stato membro. L'EDPB emette un parere sulla questione che gli è stata presentata, purché non abbia già emesso un parere sulla medesima.

4) Ai sensi dell'articolo 64, paragrafo 3, del GDPR, in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno dell'EDPB, il parere del Comitato è adottato entro otto settimane da quando il presidente ha deliberato che il fascicolo è completo. Il termine per l'adozione può essere prorogato di sei settimane – tenendo conto della complessità della questione – per decisione del presidente.

5) A norma dell'articolo 65, paragrafo 1, lettera c), del GDPR, se un'autorità di controllo competente non si conforma al parere dell'EDPB emesso a norma dell'articolo 64, qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al Comitato, il quale adotta una decisione vincolante.

¹ Nel presente parere, i riferimenti agli "Stati membri" sono da intendersi come riferimenti agli "Stati membri del SEE".

² Cfr. anche il considerando 108 del GDPR.

HA ADOTTATO IL SEGUENTE PARERE:

1 SINTESI DEI FATTI

1. L'Haut Conseil du Commissariat aux Comptes (H3C) ha presentato, con lettera ufficiale indirizzata all'autorità di controllo francese (Commission Nationale de l'Informatique et des Libertés), un progetto di accordo amministrativo volto a inquadrare i trasferimenti di dati personali dall'H3C verso il PCAOB conformemente all'articolo 46, paragrafo 3, lettera b), del GDPR.
2. Tale progetto di accordo amministrativo è stato comunicato all'autorità di controllo francese il 19 novembre 2020.
3. A seguito di tale comunicazione, l'autorità di controllo francese ha chiesto al Comitato di emettere un parere ai sensi dell'articolo 64, paragrafo 2, del GDPR. La decisione sulla completezza del fascicolo è stata adottata il 9 dicembre 2020.

2 VALUTAZIONE

4. Lo scambio di dati personali tra l'H3C e il PCAOB è necessario per garantire l'adempimento delle funzioni di regolazione rispettivamente attribuite in materia di revisione dei conti, conformemente al Sarbanes-Oxley Act e all'articolo 47 della direttiva 2006/43/CE del Parlamento europeo³, in particolare ai fini del controllo dei revisori, delle ispezioni e delle indagini sulle imprese di revisione contabile registrate e sulle persone associate soggette alla regolamentazione del PCAOB e dell'H3C.
5. Altre autorità di audit del SEE hanno esigenze analoghe di scambiare dati personali con il PCAOB. Pertanto il progetto di accordo amministrativo attualmente sottoposto all'EDPB per il necessario parere potrebbe essere considerato da altre autorità di audit del SEE come un modello da seguire per inquadrare lo stesso tipo di trasferimenti di dati personali al PCAOB nei propri accordi amministrativi specifici, che a loro volta devono essere sottoposti all'autorità di controllo competente per la necessaria autorizzazione. Di conseguenza, la questione produce effetti in più di uno Stato membro ai sensi dell'articolo 64, paragrafo 2, del GDPR.
6. Nel valutare le disposizioni contenute in questo specifico accordo amministrativo, l'EDPB ha tenuto conto di una serie di elementi specifici, compresi la tipologia di dati personali soggetti all'accordo amministrativo stesso e gli obiettivi perseguiti.
7. Il progetto di accordo amministrativo e i suoi allegati comprendono le garanzie seguenti:

Definizioni e diritti dell'interessato:

8. L'articolo I dell'accordo amministrativo contiene le definizioni pertinenti necessarie per determinare il campo di applicazione dell'accordo stesso e la sua applicazione uniforme. Tra queste vi sono alcune definizioni dei concetti e dei diritti chiave propri del quadro giuridico europeo sulla protezione dei dati, quali "dati personali", "trattamento di dati personali", "violazione di dati personali", "diritto di accesso", "diritto di cancellazione".

³ Direttiva 2006/43/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alla revisione legale dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio.

Principio della limitazione delle finalità e divieto di qualsiasi ulteriore utilizzo:

9. L'articolo III.1 dell'accordo amministrativo prevede che i dati personali trasferiti dall'H3C al PCAOB possano essere trattati da quest'ultimo esclusivamente per svolgere le proprie funzioni di regolazione in materia di revisione dei conti, conformemente al Sarbanes-Oxley Act, ai fini del controllo dei revisori, delle ispezioni e delle indagini sulle imprese di revisione contabile registrate e sulle persone associate soggette alla regolamentazione del PCAOB e dell'H3C. Secondo il principio di limitazione delle finalità, i trasferimenti possono quindi avvenire soltanto nel quadro di tali mandati e responsabilità. Il PCAOB non sarà autorizzato a trattare i dati personali che riceve per finalità diverse da quelle stabilite nell'accordo amministrativo.
10. Il PCAOB chiede infatti principalmente di conoscere i nomi e informazioni relative alle attività professionali delle singole persone che sono state responsabili di o hanno partecipato alle attività di audit sottoposte a controlli durante un'ispezione o un'indagine, o che svolgono un ruolo significativo nel controllo di gestione e di qualità riferito all'impresa di revisione contabile. Tali informazioni verrebbero utilizzate dal PCAOB per valutare il grado di conformità dell'impresa di revisione contabile registrata e delle persone ad essa associate al Sarbanes-Oxley Act, alle leggi sui titoli inerenti alla preparazione e all'emissione di relazioni di revisione, alle norme del PCAOB, alle norme della SEC (Commissione per i titoli e gli scambi) e ai pertinenti standard professionali per quanto riguarda lo svolgimento da parte dell'impresa di revisioni contabili, l'emissione di relazioni di revisione e le questioni correlate che coinvolgono gli emittenti (secondo quanto definito nel Sarbanes-Oxley Act).

Principi di qualità dei dati e di proporzionalità:

11. Secondo l'articolo III.2 dell'accordo amministrativo i dati personali trasferiti dall'H3C devono essere esatti, adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trasferiti e successivamente trattati.
12. Inoltre ciascuna parte informerà l'altra qualora venga a conoscenza del fatto che le informazioni precedentemente trasmesse o ricevute sono inesatte e/o devono essere aggiornate. Tenendo conto delle finalità per le quali i dati personali sono stati trasferiti, le parti apporteranno ai rispettivi fascicoli tutte le correzioni opportune, che possono includere l'integrazione, la cancellazione, la limitazione del trattamento, la correzione o altra rettifica dei dati personali a seconda dei casi.

Principio della trasparenza:

13. Come previsto dall'articolo III.3 dell'accordo amministrativo, sia l'H3C sia il PCAOB forniranno un avviso generale agli interessati, pubblicando l'accordo amministrativo stesso sui rispettivi siti web. Oltre all'accordo amministrativo, l'H3C fornirà informazioni sul trattamento effettuato, compresi il trasferimento, le categorie di soggetti cui i dati possono essere trasferiti, i diritti di cui gli interessati dispongono a norma di legge e le relative modalità di esercizio, informazioni su eventuali proroghe o limitazioni all'esercizio di tali diritti e informazioni di contatto per proporre ricorso o reclamo. Il PCAOB pubblicherà sul proprio sito web opportune informazioni relative al rispettivo trattamento, comprese le informazioni di cui sopra, come descritto nell'accordo. Inoltre l'H3C fornirà agli interessati un'informativa individuale conformemente al GDPR. L'H3C avviserà il PCAOB prima di fornire tale informativa individuale.

Principio della conservazione dei dati:

14. L'articolo III.2 dell'accordo amministrativo prevede che i dati personali debbano essere conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a

quello necessario alle finalità per le quali i dati sono stati raccolti o per le quali vengono ulteriormente trattati, o per il periodo di tempo previsto da leggi, norme e regolamenti applicabili. Le parti sono tenute a prevedere idonee procedure per l'eliminazione di tutte le informazioni ricevute ai sensi dell'accordo amministrativo.

Misure in tema di sicurezza e di riservatezza:

15. L'articolo III.4 dell'accordo amministrativo prevede che il PCAOB abbia fornito informazioni (allegato I dell'accordo amministrativo) che descrivono le misure di sicurezza tecniche e organizzative per evitare la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso accidentali o illegali ai dati personali. Il PCAOB si impegna a notificare all'H3C qualsiasi modifica delle misure di sicurezza tecniche e organizzative che possa incidere sul livello di protezione dei dati personali previsto dall'accordo amministrativo. In tal caso, il PCAOB aggiornerà anche le informazioni nell'allegato I. Qualora il PCAOB comunichi tale notifica all'H3C, quest'ultimo comunicherà le modifiche in questione all'autorità francese per la protezione dei dati.
16. Il PCAOB ha anche fornito all'H3C una descrizione delle norme e/o regole a esso applicabili in materia di riservatezza e delle conseguenze derivanti dalla divulgazione illegale di informazioni non pubbliche o riservate o da sospette violazioni di dette norme e/o regole.
17. Infine nel caso in cui il PCAOB venga a conoscenza di una violazione di dati personali, la comunicherà all'H3C senza indebito ritardo e, se possibile, entro 24 ore dopo essere venuto a conoscenza che la violazione riguarda tali dati personali. Non appena possibile, inoltre, il PCAOB deve impiegare mezzi ragionevoli e adeguati per porre rimedio alla violazione e ridurre al minimo i potenziali effetti negativi.

Garanzie relative ai diritti dell'interessato:

18. L'articolo III.5 dell'accordo amministrativo prevede garanzie relative ai diritti dell'interessato. In particolare, gli interessati i cui dati personali sono stati trasferiti al PCAOB possono esercitare i propri diritti definiti nell'articolo I, lettera j), dell'accordo amministrativo, anche richiedendo che l'H3C specifichi i dati personali che sono stati trasferiti al PCAOB. Inoltre gli interessati possono chiedere direttamente all'H3C di ottenere conferma dal PCAOB che i rispettivi dati personali sono completi, esatti e, se applicabile, aggiornati e che il trattamento è conforme ai principi dell'accordo amministrativo in questione. Il PCAOB risponderà in modo ragionevole e tempestivo a qualsiasi richiesta dell'H3C relativa a qualsiasi dato personale trasferito dall'H3C al PCAOB. L'interessato può anche contattare il PCAOB direttamente.
19. Qualsiasi restrizione a questi diritti dev'essere prevista dalla legge, dovrebbe essere necessaria e permarrà esclusivamente per il periodo di tempo in cui ne sussistono le motivazioni. Tali restrizioni possono essere consentite per evitare danni o pregiudizi alle funzioni di controllo o di applicazione delle norme svolte dalle parti contraenti nella misura in cui queste agiscono nell'esercizio dei pubblici poteri loro conferiti, ad esempio per il monitoraggio o la valutazione della conformità alle leggi applicabili di una parte o la prevenzione o l'indagine su presunti reati; per importanti obiettivi di interesse pubblico generale, come riconosciuto negli Stati Uniti e in Francia o nell'Unione europea, anche nello spirito di reciprocità della cooperazione internazionale; o per il controllo di individui ed entità regolamentati.

Processo decisionale automatizzato:

20. L'articolo III.5 prevede che il PCAOB non prenda decisioni aventi effetti giuridici su un interessato basandosi unicamente sul trattamento automatizzato di dati personali, compresa la profilazione, senza intervento umano.

Categorie particolari di dati personali/dati sensibili:

21. L'articolo III.6 prevede che categorie particolari di dati personali/dati sensibili non siano trasferite dall'H3C verso il PCAOB.

Limitazioni concernenti i trasferimenti successivi:

22. Secondo l'articolo III.7 dell'accordo amministrativo, il PCAOB comunicherà i dati personali ricevuti dall'H3C unicamente ai soggetti che figurano nell'allegato II dell'accordo amministrativo. In caso di tale comunicazione, eccettuata la Commissione per i titoli e gli scambi degli Stati Uniti, il PCAOB richiederà il previo consenso scritto dell'H3C e comunicherà tali dati personali esclusivamente se la terza parte fornisce garanzie adeguate e coerenti con quelle dell'accordo amministrativo. Nel richiedere tale previo consenso scritto, il PCAOB dovrebbe fornire all'H3C gli elementi per consentirgli di prestare il consenso, riguardanti la tipologia di dati personali che intende comunicare e le ragioni e le finalità di tale comunicazione. Se l'H3C non fornisce il proprio consenso scritto a tale comunicazione entro un massimo di dieci giorni, il PCAOB si consulterà con l'H3C e valuterà ogni eventuale obiezione sollevata da quest'ultimo. Se il PCAOB decide di comunicare i dati personali senza il consenso scritto dell'H3C, notificherà a quest'ultimo la propria intenzione in merito alla comunicazione dei dati e l'H3C potrà quindi decidere se sospendere il trasferimento dei dati personali. Tale decisione dovrebbe essere comunicata all'autorità francese responsabile della protezione dei dati. Inoltre, in via eccezionale, quando la terza parte non è in grado di fornire le adeguate garanzie, i dati personali possono essere comunicati a tale parte con il consenso dell'H3C se la comunicazione è fondata su importanti motivi di interesse pubblico riconosciuti negli Stati Uniti e in Francia o nell'Unione europea, oppure se è necessaria per far valere, esercitare o difendere un diritto in sede giudiziaria.
23. Per quanto riguarda la comunicazione di dati personali alla Commissione per i titoli e gli scambi degli Stati Uniti, il PCAOB otterrà da questa garanzie adeguate, coerenti con le garanzie previste nell'accordo amministrativo. Il PCAOB informerà inoltre periodicamente l'H3C della natura dei dati personali comunicati e del motivo di tali comunicazioni, a condizione che tali informazioni non mettano a repentaglio un'indagine in corso. Tale restrizione riguardante le informazioni relative a un'indagine in corso permarrà solo per il periodo di tempo in cui ne sussiste la relativa motivazione.
24. Infine, un interessato può richiedere all'H3C determinate informazioni relative ai propri dati personali trasferiti dall'H3C al PCAOB. Sarà responsabilità dell'H3C fornire tali informazioni conformemente alle disposizioni giuridiche applicabili contenute nel GDPR e nella legge francese sulla protezione dei dati.

Meccanismi di ricorso:

25. L'articolo III.8 dell'accordo amministrativo prevede un meccanismo di ricorso. L'accordo amministrativo prevede quattro livelli di ricorso per l'interessato. Innanzitutto, l'interessato può sollevare qualsiasi controversia o reclamo in merito al trattamento dei suoi dati personali ai sensi dell'accordo amministrativo dinanzi all'H3C, al PCAOB, o a entrambi, a seconda dei casi. Ciascuna parte informerà l'altra di qualsiasi controversia o reclamo e si adopererà per risolvere amichevolmente la controversia o il reclamo in modo tempestivo.

26. Il PCAOB informerà l'H3C delle segnalazioni che riceve dagli interessati e si consulterà con l'H3C sulla risposta da fornire in merito.
27. In secondo luogo, se una delle parti non è in grado di risolvere una segnalazione o un reclamo presentati da un interessato, o se nessuna delle parti è in grado di farlo, e purché tale segnalazione o reclamo non siano manifestamente infondati o eccessivi, l'interessato e la parte o le parti possono fare ricorso a un primo livello del meccanismo di risoluzione delle controversie, guidato da una funzione indipendente all'interno del PCAOB, nota come "Hearing Officer" [funzionario per le audizioni].
28. In terzo luogo, la decisione raggiunta attraverso questo meccanismo di risoluzione delle controversie può essere sottoposta a un riesame indipendente, condotto da una funzione indipendente e distinta nota come "Redress Reviewer" [revisore del ricorso]. Le decisioni dello *Hearing Officer* e del *Redress Reviewer* sono vincolanti per il PCAOB. Questi meccanismi di risoluzione delle controversie sono descritti dettagliatamente nell'allegato III dell'accordo amministrativo.
29. Ove l'H3C ritenga che il PCAOB non abbia agito in modo coerente con le garanzie previste dall'accordo amministrativo, può sospendere i trasferimenti finché la questione non sia stata risolta in modo soddisfacente informandone l'interessato.
30. Infine, in ogni caso, l'interessato può esercitare il diritto a presentare ricorso in sede giudiziaria o amministrativa (anche ai fini del risarcimento dei danni) secondo la legge francese sulla protezione dei dati.

Meccanismo di controllo:

31. L'articolo III.9 dell'accordo amministrativo prevede un meccanismo di controllo che garantisca l'attuazione delle garanzie dello stesso. Tale meccanismo di controllo consiste in una combinazione di controlli interni ed esterni.
32. Per quanto riguarda i controlli interni, ciascuna delle parti condurrà revisioni periodiche delle proprie politiche e procedure di attuazione delle garanzie dell'accordo amministrativo. Su ragionevole richiesta dell'altra parte, una parte riesaminerà le proprie politiche e procedure per accertare e confermare che le garanzie specificate nell'accordo di cui trattasi sono attuate in modo efficace, e trasmetterà una sintesi della revisione all'altra parte.
33. Per quanto riguarda i controlli esterni, a seguito di richiesta dell'H3C di condurre una revisione indipendente della conformità alle garanzie previste dall'accordo amministrativo, il PCAOB comunicherà all'Office of Internal Oversight and Performance Assurance ("IOPA"), un ufficio indipendente del PCAOB, di eseguire un controllo per accertare e confermare l'effettiva attuazione delle garanzie previste nell'accordo amministrativo. I particolari del funzionamento dell'IOPA sono forniti nell'allegato IV dell'accordo di amministrazione. L'IOPA fornirà all'H3C una sintesi dei risultati della propria valutazione previa approvazione, da parte del consiglio direttivo del PCAOB, della comunicazione all'H3C di tale sintesi.
34. Nel caso in cui l'H3C non abbia ricevuto i risultati del controllo condotto dall'IOPA e ritenga che il PCAOB non abbia agito in modo coerente con le garanzie specificamente riferite ai suoi obblighi ai sensi dell'accordo amministrativo, l'H3C può sospendere i trasferimenti verso il PCAOB finché la questione non sia stata risolta in modo soddisfacente dal PCAOB stesso. Tale sospensione dev'essere comunicata all'autorità francese responsabile della protezione dei dati.

3 CONCLUSIONI E RACCOMANDAZIONI

35. L'EDPB apprezza gli sforzi compiuti per l'accordo amministrativo in questione, che prevede una serie di importanti garanzie di protezione dei dati in linea con il GDPR e anche con le garanzie stabilite nelle linee-guida 2/2020 dell'EDPB. Affinché tali garanzie continuino ad assicurare un livello adeguato di protezione dei dati in caso di trasferimento di dati al PCAOB, tenuto conto della natura specialissima di tali accordi non vincolanti, l'EDPB sottolinea quanto segue:
- J l'autorità di controllo francese vigilerà sull'accordo amministrativo e la sua applicazione pratica, in particolare per quanto riguarda gli articoli III.7, 8 e 9 relativi ai trasferimenti successivi e ai meccanismi di ricorso e di controllo, al fine di garantire che gli interessati dispongano di diritti effettivi e azionabili e di adeguati mezzi di ricorso e che sia effettivamente verificata la conformità all'accordo amministrativo;
 - J l'autorità di controllo francese autorizza l'accordo amministrativo solo come garanzia adeguata per la protezione dei dati in vista del loro trasferimento transfrontaliero, a condizione che i firmatari ne rispettino pienamente tutte le clausole;
 - J l'autorità di controllo francese sospenderà i flussi di dati effettuati dall'H3C conformemente all'autorizzazione ove l'accordo amministrativo non preveda più garanzie adeguate ai sensi del GDPR.

4 OSSERVAZIONI CONCLUSIVE

36. Il presente parere sarà reso pubblico ai sensi dell'articolo 64, paragrafo 5, lettera b), del GDPR.

Per il Comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)