Parere del comitato (articolo 64)

Parere 22/2024 su taluni obblighi derivanti dal ricorso a uno o più responsabili del trattamento e a uno o più sub-responsabili del trattamento

Adottato il 7 ottobre 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sintesi

L'autorità di controllo danese ha chiesto al comitato europeo per la protezione dei dati (EDPB) un parere su questioni di applicazione generale ai sensi dell'articolo 64, paragrafo 2, del regolamento generale sulla protezione dei dati (GDPR). Il parere contribuisce a un'interpretazione armonizzata da parte delle autorità di controllo nazionali di taluni aspetti dell'articolo 28 del GDPR, se del caso in combinato disposto con il capo V del GDPR. In particolare, tratta questioni relative all'interpretazione di talune funzioni dei titolari del trattamento che fanno ricorso a responsabili del trattamento e sub-responsabili del trattamento, derivanti in particolare dall'articolo 28 del GDPR, nonché al testo dei contratti tra titolare del trattamento e responsabile del trattamento. Le questioni esaminate riguardano il trattamento dei dati personali nel SEE e il trattamento in seguito a un trasferimento verso un paese terzo.

Nel parere il comitato conclude che i titolari del trattamento dovrebbero avere a disposizione in qualsiasi momento le informazioni sull'identità (ossia nome, indirizzo, referente) di tutti i responsabili del trattamento, i sub-responsabili del trattamento, ecc., in modo da poter adempiere al meglio gli obblighi previsti dall'articolo 28 del GDPR, a prescindere dal rischio associato all'attività di trattamento. A tal fine, il responsabile del trattamento dovrebbe fornire proattivamente al titolare del trattamento tutte queste informazioni e tenerle sempre aggiornate.

L'articolo 28, paragrafo 1, del GDPR dispone che i titolari del trattamento hanno l'obbligo di incaricare responsabili del trattamento che presentino «garanzie sufficienti» per mettere in atto misure «adeguate» in modo tale che il trattamento soddisfi i requisiti del GDPR e assicuri la tutela dei diritti degli interessati. Nel parere l'EDPB afferma che nel valutare il rispetto da parte dei titolari del trattamento di tale obbligo e del principio di responsabilizzazione (articolo 24, paragrafo 1, GDPR), le autorità di controllo dovrebbero tenere conto del fatto che il ricorso a responsabili del trattamento non dovrebbe ridurre il livello di tutela dei diritti degli interessati. L'*obbligo* del titolare del trattamento di verificare se i (sub-)responsabili del trattamento presentino «garanzie sufficienti» per mettere in atto le misure adeguate stabilite dallo stesso titolare del trattamento dovrebbe applicarsi a prescindere dal rischio per i diritti e le libertà degli interessati. Tuttavia, la *portata* di detta verifica varierà in pratica a seconda della natura di tali misure tecniche e organizzative, che possono essere più restrittive o più estese a seconda del livello di tale rischio.

Inoltre, nel parere l'EDPB specifica che, sebbene il primo responsabile del trattamento debba assicurare di proporre sub-responsabili del trattamento che presentino garanzie sufficienti, la decisione finale sull'eventuale ricorso a uno specifico sub-responsabile e la relativa responsabilità, anche per quanto riguarda la verifica delle garanzie, resta in capo al titolare del trattamento. Le autorità di controllo dovrebbero valutare se il titolare del trattamento sia in grado di dimostrare che la verifica della sufficienza delle garanzie presentate dai (sub-)responsabili del trattamento sia stata soddisfacente. Il titolare del trattamento può decidere di fare affidamento sulle informazioni ricevute dal responsabile del trattamento e di approfondirle se necessario (ad esempio, se sembrano incomplete, imprecise o sollevano dubbi). Più specificamente, qualora il trattamento presenti un rischio elevato per i diritti e le libertà degli interessati, il titolare del trattamento dovrebbe aumentare il livello della verifica in termini di controllo delle informazioni fornite. A tale riguardo, l'EDPB ritiene che, ai sensi del GDPR, il titolare del trattamento non sia tenuto a richiedere sistematicamente i

contratti di sub-trattamento per controllare se gli obblighi di protezione dei dati previsti nel contratto iniziale siano stati trasferiti lungo la catena di trattamento. Il titolare del trattamento dovrebbe valutare, caso per caso, se richiedere una copia di tali contratti o esaminarli in qualsiasi momento sia necessario per poter dimostrare la conformità alla luce del principio di responsabilizzazione.

Qualora avvengano trasferimenti di dati personali al di fuori del SEE tra due (sub-)responsabili del trattamento, conformemente all'istruzione del titolare del trattamento, il titolare rimane soggetto agli obblighi derivanti dall'articolo 28, paragrafo 1, del GDPR, relativamente alle «garanzie sufficienti», oltre a quelli di cui all'articolo 44 per assicurare che il livello di tutela garantito dal GDPR non sia compromesso dai trasferimenti di dati personali. Il responsabile del trattamento/l'esportatore dovrebbe preparare la documentazione pertinente, in linea con la giurisprudenza e come chiarito nelle raccomandazioni 01/2020 dell'EDPB. Il titolare del trattamento dovrebbe valutare tale documentazione ed essere in grado di mostrarla all'autorità di controllo competente. Il titolare del trattamento può basarsi sulla documentazione o sulle informazioni ricevute dal responsabile del trattamento/dall'esportatore e, se necessario, approfondirle. La portata e la natura dell'obbligo del titolare del trattamento di valutare tale documentazione possono dipendere dal motivo del trasferimento e dal fatto che si tratti di un trasferimento iniziale o successivo.

Nel parere l'EDPB ha altresì considerato una domanda relativa al testo dei contratti tra titolare del trattamento e responsabile del trattamento. A tale proposito, un elemento fondamentale è l'impegno da parte del responsabile del trattamento di trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che «*lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» [articolo 28, paragrafo 3, lettera a), del GDPR], che richiama il principio generale secondo cui i contratti non possono prevalere sul diritto. Alla luce della libertà contrattuale riconosciuta alle parti di adattare il contratto tra titolare del trattamento e responsabile del trattamento alle loro circostanze, entro i limiti dell'articolo 28, paragrafo 3, del GDPR, l'EDPB ritiene che l'inclusione del testo «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» (alla lettera o in termini molto simili) sia vivamente raccomandata ma non obbligatoria.

In riferimento a varianti simili a «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*», l'EDPB ritiene che il loro utilizzo rimanga nell'ambito delle prerogative della libertà contrattuale delle parti e non violi di per sé l'articolo 28, paragrafo 3, lettera a), del GDPR. Allo stesso tempo, nel parere l'EDPB individua una serie di questioni, in quanto tale clausola non esonera il responsabile del trattamento dall'adempimento degli obblighi previsti dal GDPR.

Per i dati personali trasferiti al di fuori del SEE, l'EDPB considera improbabile che il testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» sia di per sé sufficiente ai fini della conformità all'articolo 28, paragrafo 3, lettera a), del GDPR in combinato disposto con il capo V. Come illustrato dalle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea e dalle raccomandazioni relative alle BCR-C, l'articolo 28, paragrafo 3, lettera a), del GDPR non impedisce, in linea di principio, l'inclusione nel contratto di disposizioni riguardanti i requisiti di legge di paesi terzi per il trattamento di dati personali trasferiti. Tuttavia, come in questi documenti, si dovrebbe distinguere tra le leggi di paesi terzi che pregiudicherebbero il livello di protezione garantito dal GDPR e quelle che non lo farebbero. Infine, l'EDPB ricorda che la possibilità che il diritto di un paese terzo impedisca il rispetto del GDPR dovrebbe essere un fattore considerato dalle parti prima di

concludere il contratto (tra titolare del trattamento e responsabile del trattamento o tra responsabile del trattamento e sub-responsabile del trattamento).

Anche se il responsabile del trattamento tratta dati personali all'interno del SEE, in determinate circostanze può trovarsi a dover tenere conto del diritto di paesi terzi. L'EDPB evidenzia che l'aggiunta nel contratto di un testo simile a «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» non esonera il responsabile del trattamento dagli obblighi previsti dal GDPR.

Infine, l'EDPB ritiene che l'inserimento del testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» (alla lettera o in termini molto simili) dopo l'impegno del responsabile del trattamento a effettuare il trattamento soltanto su istruzione documentata non possa essere interpretato come istruzione documentata del titolare del trattamento.

Indice

Il comitato europeo per la protezione dei dati

visto l'articolo 63 e l'articolo 64, paragrafo 2, 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 (in prosieguo «GDPR»),

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 2018 ([1]),

visti gli articoli 10 e 22 del proprio regolamento interno,

considerando quanto segue:

(1) Il ruolo principale del comitato europeo per la protezione dei dati (in prosieguo «comitato» o «EDPB») è assicurare l'applicazione coerente del GDPR in tutto lo Spazio economico europeo (SEE). L'articolo 64, paragrafo 2, del GDPR stabilisce che qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro del SEE siano esaminate dal comitato al fine di ottenere un parere. Il presente parere ha lo scopo di esaminare una questione di applicazione generale o che produce effetti in più di uno Stato membro del SEE.

(2) Il parere del comitato è adottato ai sensi dell'articolo 64, paragrafo 3, del GDPR in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno dell'EDPB entro otto settimane dalla data in cui il presidente e l'autorità di controllo competente hanno deciso che il fascicolo è completo. Su decisione del presidente, tale termine può essere prorogato di ulteriori sei settimane, a seconda della complessità della questione,

HA ADOTTATO IL SEGUENTE PARERE:

1 INTRODUZIONE

1.1 Sintesi dei fatti

1. Il 5 luglio 2024 l'autorità di controllo danese ha richiesto al comitato europeo per la protezione dei dati (in prosieguo «comitato» o «EDPB») di emettere un parere in merito agli obblighi di responsabilizzazione dei titolari del trattamento per quanto riguarda la catena di trattamento e alla relazione tra i titolari del trattamento e i (sub-)responsabili del trattamento (in prosieguo «richiesta»).

2. L'autorità di controllo danese ha dichiarato completo il fascicolo l'8 luglio 2024. Il presidente del comitato ha considerato completo il fascicolo il 9 luglio 2024. Alla stessa data il fascicolo è stato trasmesso dal segretariato dell'EDPB. Il presidente, considerata la complessità della questione, ha

([1]) Nel presente parere, con il termine «Stati membri» si intendono gli «Stati membri del SEE». I riferimenti all'«Unione» in tutto il parere sono da intendersi come riferimenti al «SEE».

deciso di prorogare il termine legale in linea con l'articolo 64, paragrafo 3, del GDPR e con l'articolo 10, paragrafo 4, del regolamento interno.

3. Nella sua richiesta, l'autorità di controllo danese fa riferimento anche alla relazione adottata dall'EDPB nel gennaio 2023 sulle conclusioni della sua prima azione di applicazione coordinata ([2]) nell'ambito del quadro di applicazione coordinato (CEF) ([3]). Tale azione coordinata si è concentrata sull'utilizzo di servizi basati sul cloud da parte del settore pubblico. Nella relazione dell'EDPB le autorità di controllo partecipanti all'azione coordinata hanno individuato otto sfide, in particolare relativamente all'uso dei servizi basati sul cloud da parte di organismi pubblici, e hanno fornito un elenco di punti di attenzione che i portatori di interessi pertinenti dovrebbero tenere in considerazione nella valutazione dei servizi basati sul cloud e nell'interazione con i fornitori di tali servizi ([4]). Se per la maggior parte di questi punti la portata degli obblighi imposti dal GDPR è chiara sia per i titolari del trattamento che per i responsabili del trattamento, la portata precisa di taluni obblighi previsti dal GDPR rimane poco chiara secondo l'autorità di controllo danese ([5]).

   L'autorità di controllo danese ha posto le domande riportate di seguito.

4. Domanda 1.1: tenendo conto dell'articolo 5, paragrafo 2, e dell'articolo 24, paragrafo 1, del GDPR, quando un titolare del trattamento ricorre a un responsabile del trattamento per l'esecuzione di attività di trattamento per suo conto, al fine di documentare il rispetto, tra l'altro, dell'articolo 28, paragrafi 1 e 2 (anche al momento della presentazione della documentazione all'autorità di controllo in sede di ispezione):

   a. Il titolare del trattamento deve identificare tutti i sub-responsabili del trattamento del responsabile del trattamento, i loro sub-responsabili ecc. lungo l'intera catena di trattamento o soltanto la prima linea di sub-responsabili del trattamento cui il responsabile del trattamento fa ricorso?

   b. In che misura e con quale livello di dettaglio il titolare del trattamento deve verificare e documentare:

      i. l'adeguatezza delle garanzie presentate dai responsabili del trattamento, dai sub-responsabili del trattamento ecc.,
      ii. il contenuto dei contratti tra il primo responsabile del trattamento e i responsabili del trattamento aggiuntivi per accertare se gli stessi obblighi siano stati imposti ai responsabili del trattamento aggiuntivi a norma dell'articolo 28, paragrafo 4, del GDPR, e
      iii. se i responsabili del trattamento, i sub-responsabili del trattamento ecc. soddisfino i requisiti del titolare del trattamento di cui all'articolo 28, paragrafo 1?

5. Domanda 1.2: in caso di trasferimenti o trasferimenti successivi da un (sub-)responsabile del trattamento a un altro (sub-)responsabile, conformemente all'istruzione del titolare del trattamento: in che misura il titolare del trattamento, nell'ambito del suo obbligo di cui all'articolo 28, paragrafo 1, del GDPR, in combinato disposto con l'articolo 44 del GDPR, deve valutare che il livello di protezione

([2]) Relazione sull'azione di applicazione coordinata 2022 - Uso dei servizi basati sul cloud da parte del settore pubblico, 17 gennaio 2023 (in prosieguo «relazione CEF sui servizi basati sul cloud»).
([3]) Il quadro di applicazione coordinato è stato istituito dall'EDPB nell'ottobre 2020 al fine di razionalizzare l'applicazione e la cooperazione tra le autorità di controllo. Cfr. il documento dell'EDPB sul quadro di applicazione coordinato ai sensi del regolamento 2016/679, adottato il 20 ottobre 2020, versione 1.1.
([4]) Relazione CEF sui servizi basati sul cloud, pagg. 10-20.
([5]) Richiesta, pag. 1.

dei dati personali non è compromesso dai trasferimenti (successivi) ed essere in grado di presentare la documentazione dei (sub-)responsabili del trattamento a tale riguardo?

6. Domanda 1.3: la portata degli obblighi di cui all'articolo 28, paragrafi 1 e 2, del GDPR, in combinato disposto con l'articolo 5, paragrafo 2, e l'articolo 24 del GDPR, in linea con le risposte alla domanda 1.1 e alla domanda 1.2, varia a seconda del rischio associato all'attività di trattamento? In caso di risposta affermativa, qual è la portata di tali obblighi per attività di trattamento a basso rischio e per attività di trattamento ad alto rischio?

7. Domanda 2: un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri ai sensi dell'articolo 28, paragrafo 3, del GDPR deve contenere l'eccezione di cui all'articolo 28, paragrafo 3, lettera a), «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» (alla lettera o in termini molto simili) per essere conforme al GDPR?

8. Domanda 2a: in caso di risposta negativa alla domanda 2, il fatto che un contratto o altro atto giuridico ai sensi del diritto dell'Unione o degli Stati membri estenda l'eccezione di cui all'articolo 28, paragrafo 3, lettera a), del GDPR anche al diritto di un paese terzo in generale (ad esempio «salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico») costituisce di per sé una violazione dell'articolo 28, paragrafo 3, lettera a), del GDPR?

9. Domanda 2b: in caso di risposta negativa alla domanda 2a, tale eccezione estesa dovrebbe invece essere interpretata come un'istruzione documentata del titolare del trattamento ai sensi dell'articolo 28, paragrafo 3, lettera a), del GDPR?

1.2 Ammissibilità della richiesta di un parere ai sensi dell'articolo 64, paragrafo 2, del GDPR

10. L'articolo 64, paragrafo 2, del GDPR stabilisce che, in particolare, qualsiasi autorità di controllo può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere.

11. Le prime domande trasmesse dall'autorità di controllo danese si riferiscono agli obblighi di responsabilizzazione dei titolari del trattamento di cui all'articolo 28 del GDPR (domande 1.1, 1.2 e 1.3), mentre l'ultima domanda riguarda il contenuto specifico del contratto o atto giuridico tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafo 3, lettera a), del GDPR (domanda 2).

12. Il comitato ritiene che tali domande siano connesse all'interpretazione del GDPR, in particolare per quanto concerne la relazione tra i titolari del trattamento e i (sub-)responsabili del trattamento e l'interpretazione dell'articolo 5, paragrafo 2, dell'articolo 24 e dell'articolo 28 del GDPR. La richiesta è collegata, da un lato, agli obblighi di responsabilizzazione dei titolari del trattamento e al livello di documentazione che le autorità di controllo dovrebbero aspettarsi dai titolari del trattamento che fanno ricorso a (sub-)responsabili del trattamento per l'esecuzione di attività di trattamento per loro conto e, dall'altro, al contenuto dei contratti o atti giuridici tra titolari del trattamento e responsabili del trattamento. Pertanto, la richiesta riguarda una «*questione di applicazione generale*» ai sensi dell'articolo 64, paragrafo 2, del GDPR.

13. Inoltre, il comitato ritiene che la richiesta dell'autorità di controllo danese sia motivata in linea con l'articolo 10, paragrafo 3, del regolamento interno dell'EDPB, in quanto l'autorità di controllo danese ha esposto argomenti a favore della necessità di un'interpretazione coerente delle questioni affrontate nella richiesta.

14. Ai sensi dell'articolo 64, paragrafo 3, del GDPR, l'EDPB non emette un parere se ha già emesso un parere sulla medesima questione ([6]). L'EDPB non ha ancora fornito risposte alle domande di cui alla richiesta dell'autorità di controllo danese. Inoltre, le linee guida dell'EDPB disponibili, comprese in particolare le linee guida 07/2020 dell'EDPB sui concetti di titolare del trattamento e di responsabile del trattamento ([7]) (in prosieguo «linee guida 07/2020 dell'EDPB»), forniscono alcuni orientamenti sulla portata degli obblighi di responsabilizzazione del titolare del trattamento ai sensi dell'articolo 28 del GDPR. Tuttavia, gli orientamenti esistenti non affrontano in modo completo tutte le domande formulate nella richiesta ([8]). In particolare, ad esempio, gli orientamenti disponibili per quanto riguarda l'articolo 28, paragrafo 3, lettera a), del GDPR non affrontano specificamente la domanda se il testo «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» debba essere inclusa nei contratti o atti giuridici tra titolari del trattamento e responsabili del trattamento formulata nella richiesta dell'autorità di controllo danese.

15. Per tali motivi, il comitato ritiene che la richiesta dell'autorità di controllo danese sia ammissibile e che le domande in essa formulate debbano essere analizzate in un parere adottato ai sensi dell'articolo 64, paragrafo 2, del GDPR.

2 MERITO DELLA RICHIESTAERROR! BOOKMARK NOT DEFINED.

2.1 Interpretazione dell'articolo 28, paragrafi 1, 2 e 4, del GDPR, in combinato disposto con l'articolo 5, paragrafo 2, e l'articolo 24, paragrafo 1 (domande 1.1 e 1.3)

16. La presente sezione verte sulle domande 1.1 e 1.3 trasmesse al comitato, riportate nella precedente sezione relativa all'«ammissibilità».

17. L'articolo 28 del GDPR stabilisce la relazione tra il titolare del trattamento e il responsabile del trattamento e impone obblighi diretti ai titolari del trattamento e ai responsabili del trattamento. Innanzitutto, va osservato che il GDPR definisce il «responsabile del trattamento» all'articolo 4, paragrafo 8, in un modo generale, che include sia il primo responsabile del trattamento, incaricato direttamente dal titolare del trattamento, sia il responsabile del trattamento del responsabile del trattamento e così via lungo la catena di trattamento.

18. L'EDPB rileva che la valutazione del ruolo delle parti (e se agiscano come titolari unici o congiunti del trattamento o come responsabili del trattamento) non rientra nell'ambito della richiesta. L'EDPB ricorda che spetta in primo luogo alle parti valutare il loro ruolo effettivo in base agli elementi di fatto o alle circostanze del caso ([9]), fatta salva la competenza dell'autorità di controllo a verificare la fondatezza della loro valutazione.

19. Alla luce delle suddette domande, il presente parere si concentra esclusivamente sull'ambito e sulla portata degli obblighi del titolare del trattamento di cui all'articolo 28, paragrafo 1, del GDPR, di

([6]) Articolo 64, paragrafo 3, del GDPR e articolo 10, paragrafo 4, del regolamento interno dell'EDPB.
([7]) Linee guida 07/2020 dell'EDPB sui concetti di titolare del trattamento e responsabile del trattamento di cui al GDPR, versione 2.1, adottate il 7 luglio 2021.
([8]) Cfr. in particolare le linee guida 07/2020 dell'EDPB, sezione 1.1 «Scelta del responsabile del trattamento», pagina 30, sezione 1.3.4 «*Obbligo del responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 2, e all'articolo 28, paragrafo 4, per ricorrere a un altro responsabile del trattamento (articolo 28, paragrafo 3, lettera d) del GDPR)*», pagina 37, sezione 1.6 «Sub-responsabili del trattamento», pagina 42.
([9]) Linee guida 07/2020 dell'EDPB, paragrafo 12.

verificare se i (sub-)responsabili del trattamento presentino «garanzie sufficienti», ai sensi dell'articolo 28, paragrafo 2, e dei correlati obblighi di responsabilizzazione del titolare del trattamento di cui all'articolo 5, paragrafo 2, e all'articolo 24, paragrafo 1, del GDPR ([10]).

20. Il comitato osserva altresì che le suddette domande non si riferiscono alla responsabilità del titolare del trattamento nei confronti degli interessati per le attività di trattamento svolte per suo conto, ad esempio per quanto riguarda il diritto degli interessati al risarcimento ai sensi dell'articolo 82 del GDPR. La presente sezione si concentrerà pertanto sull'esposizione di chiarimenti per le autorità di controllo in merito all'interpretazione dell'articolo 28, paragrafi 1 e 2, del GDPR, in combinato disposto con l'articolo 5, paragrafo 2, e l'articolo 24 del GDPR, in merito a determinati obblighi derivanti dal ricorso a responsabili e sub-responsabili del trattamento. Al fine di rispondere a tali domande, il comitato condurrà un'analisi incentrata sulle situazioni in cui non vi sono trasferimenti di dati personali al di fuori del SEE. Per contro, la sezione successiva, relativa alla domanda 1.2, valuterà le situazioni in cui si verificano trasferimenti lungo la catena di trattamento.

2.1.1 Identificazione dei soggetti della catena di trattamento

21. Per quanto riguarda la questione se, in sostanza, il titolare del trattamento debba identificare tutti i sub-responsabili del trattamento del responsabile del trattamento, i relativi sub-responsabili del trattamento ecc. lungo l'intera catena di trattamento o soltanto la prima linea di sub-responsabili del trattamento cui fa ricorso il responsabile del trattamento, l'EDPB rileva, in primo luogo, che «*[s]ebbene la catena [di trattamento] possa essere alquanto lunga, il titolare del trattamento mantiene un ruolo centrale nella determinazione della finalità e dei mezzi dello stesso*» ([11]).

22. Ai fini della risposta alla domanda, l'EDPB considera che i termini «identificare» e «informazioni sull'identità» si riferiscano al nome, all'indirizzo, alla persona di contatto (nome, posizione, dati di contatto) del responsabile del trattamento e alla descrizione del trattamento (compresa una chiara delimitazione delle responsabilità nel caso in cui diversi sub-responsabili del trattamento siano autorizzati) ([12]).

23. Per quanto riguarda la scelta dei responsabili del trattamento, i titolari del trattamento dovrebbero essere in grado di determinare efficacemente le finalità e i mezzi del trattamento a norma dell'articolo 4, punto 7, del GDPR. A tale proposito, la determinazione dei destinatari (compresi i responsabili del trattamento) è considerata un «mezzo essenziale» del trattamento, in merito al quale il titolare del trattamento decide ([13]).

([10]) Tale questione è distinta e separata da qualsiasi altro obbligo del titolare del trattamento [o dei (sub-)responsabili del trattamento] di assicurare il rispetto del GDPR, ad esempio del principio di liceità, dell'articolo 32 o degli obblighi di cui al il capo V del GDPR. Il titolare del trattamento può essere responsabile del trattamento di sua titolarità che non è conforme a tali disposizioni del GDPR anche se ha adempiuto gli obblighi di verifica dei propri (sub-)responsabili del trattamento in conformità dell'articolo 28, paragrafo 1, del GDPR indicati nel presente parere. Inoltre, il presente parere non considera la responsabilità del titolare del trattamento per quanto riguarda il rispetto delle disposizioni del GDPR diverse dall'articolo 24, paragrafo 1, e dall'articolo 28, paragrafi 1 e 2, del GDPR.

([11]) Linee guida 07/2020 dell'EDPB, paragrafo 152.

([12]) Ciò rispecchia le informazioni necessarie per l'identificazione dei responsabili del trattamento di cui all'allegato IV delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea [decisione di esecuzione (UE) 2021/915 della Commissione, del 4 giugno 2021] e all'allegato III delle clausole contrattuali tipo della Commissione europea per i trasferimenti internazionali [decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021].

([13]) Linee guida 07/2020 dell'EDPB, paragrafo 40.

24. A tal fine, rispetto al ricorso a **ulteriori responsabili del trattamento** da parte del primo responsabile del trattamento, è necessaria la previa autorizzazione scritta, specifica o generale, del titolare del trattamento ai sensi dell'articolo 28, paragrafo 2, del GDPR. Le linee guida 07/2020 dell'EDPB chiariscono che gli obblighi specifici previsti dall'articolo 28, paragrafo 2, «*scaturiscono laddove un (sub-)responsabile del trattamento intenda coinvolgere un altro soggetto, aggiungendo in tal modo un altro anello alla catena, affidandogli attività che richiedono il trattamento di dati personali*» ([14]).

25. Qualora il titolare del trattamento decida di accettare determinati sub-responsabili, al momento della firma del contratto è opportuno inserire nello stesso o in un suo allegato un elenco dei sub-responsabili del trattamento approvati. L'elenco dovrebbe quindi essere tenuto aggiornato, conformemente all'autorizzazione generale o specifica concessa dal titolare del trattamento ([15]).

26. Per quanto riguarda il ricorso a sub-responsabili del trattamento, il GDPR prevede la possibilità di un'autorizzazione generale o specifica. **In caso di autorizzazione specifica**, il titolare del trattamento dovrebbe specificare per iscritto quale sub-responsabile del trattamento è autorizzato nonché la specifica attività di trattamento e il momento a cui fa riferimento ([16]). Qualora la richiesta di un'autorizzazione specifica da parte del responsabile del trattamento non riceva risposta entro il termine stabilito, la si considera respinta ([17]).

27. **In caso di autorizzazione generale**, il responsabile del trattamento dovrebbe fornire al titolare del trattamento la possibilità di approvare un elenco di sub-responsabili del trattamento al momento della firma dell'autorizzazione generale e la possibilità, compreso un periodo di tempo sufficiente, di opporsi a eventuali modifiche successive dei sub-responsabili del trattamento ([18]). Il comitato ricorda che dovrebbe essere il primo **responsabile del trattamento a fornire proattivamente determinate informazioni** al titolare del trattamento e che «*il dovere del responsabile di informare il titolare di qualsivoglia modifica relativa a sub-responsabili del trattamento implica che il responsabile del trattamento comunichi o segnali **attivamente** tali modifiche al titolare*» ([19]).

([14]) Il paragrafo 151 delle linee guida 07/2020 dell'EDPB recita: «*Le attività di trattamento dei dati sono spesso svolte da un gran numero di soggetti e le catene di esternalizzazione diventano sempre più complesse. Il GDPR introduce obblighi specifici che scaturiscono laddove un (sub-)responsabile del trattamento intenda coinvolgere un altro soggetto, aggiungendo in tal modo un altro anello alla catena, affidandogli attività che richiedono il trattamento di dati personali. L'analisi volta a stabilire se il prestatore di servizi agisca in qualità di sub-responsabile dovrebbe essere effettuata in linea con quanto sopra detto sul concetto di responsabile del trattamento*».

([15]) Linee guida 07/2020 dell'EDPB, paragrafo 154.

([16]) Linee guida 07/2020 dell'EDPB, paragrafi 153 e 155. Ai sensi della clausola 7.7, opzione 1, delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea, l'elenco dei sub-responsabili del trattamento specificamente autorizzati dal titolare del trattamento dovrebbe figurare nell'allegato IV, che dovrebbe essere tenuto aggiornato.

([17]) Linee guida 07/2020 dell'EDPB, paragrafo 155.

([18]) Cfr. anche le linee guida 07/2020 dell'EDPB, paragrafo 156: «*[i]n alternativa, il titolare del trattamento può fornire la propria autorizzazione generale all'uso di sub-responsabili (nel contratto, compreso un elenco di tali sub-responsabili in allegato) [...]*». Pertinente in questo contesto è anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR). Ai sensi della clausola 7.7, opzione 2, delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea, il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato e informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento in anticipo.

([19]) Linee guida 07/2020 dell'EDPB, paragrafo 128 (enfasi aggiunta). Cfr. anche la nota 14.

28. Ciò significa che le informazioni relative all'identificazione di tutti i sub-responsabili del responsabile del trattamento dovrebbero essere facilmente accessibili al titolare del trattamento. L'identificazione di tali soggetti è particolarmente importante affinché il titolare del trattamento possa avere il controllo sulle attività di trattamento di sua responsabilità e possa essere ritenuto responsabile in caso di violazione del GDPR.

29. Il responsabile del trattamento dovrebbe pertanto fornire tutte le informazioni sulle modalità di esecuzione dell'attività di trattamento per conto del titolare del trattamento, comprese le informazioni sul sub-responsabile del trattamento cui si fa ricorso ([20]) e una descrizione del trattamento affidato al sub-responsabile ([21]).

30. Altri motivi giuridici giustificano la necessità che il titolare del trattamento identifichi tutti i responsabili e i sub-responsabili. I responsabili del trattamento a cui i dati vengono comunicati o trasferiti sono considerati «destinatari» ([22]).

- Al fine di rispettare i requisiti di trasparenza di cui all'articolo 13, paragrafo 1, lettera e), e all'articolo 14, paragrafo 1, lettera e), del GDPR, i titolari del trattamento dovrebbero informare gli interessati in merito ai destinatari o alle categorie di destinatari dei dati, essendo il più possibile specifici e concreti ([23]). Le informazioni sulle «categorie di destinatari» devono essere incluse anche nei registri delle attività di trattamento [articolo 30, paragrafo 1, lettera d)].

- L'articolo 15 del GDPR prevede il diritto di accesso, tra l'altro, alle informazioni sui destinatari o sulle categorie di destinatari a cui i dati personali sono stati o saranno comunicati ([24]). La Corte di giustizia ha chiarito che tale disposizione implica l'obbligo per il titolare del trattamento di fornire all'interessato l'identità stessa dei destinatari ([25]). Al di fuori del tipo di casi in cui il titolare del trattamento può indicare

([20]) Linee guida 7/2020 dell'EDPB, paragrafo 143.
([21]) Cfr. ad esempio l'allegato IV delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea e l'allegato II delle clausole contrattuali tipo per i trasferimenti internazionali della Commissione europea.
([22]) Articolo 4, paragrafo 9, del GDPR; linee guida del gruppo dell'articolo 29 sulla trasparenza ai sensi del regolamento (UE) 2016/679, adottate il 29 novembre 2017, da ultimo riviste e adottate l'11 aprile 2018, WP260 rev. 01, approvate dall'EDPB (in prosieguo «linee guida sulla trasparenza del gruppo dell'articolo 29»), pag. 37.
([23]) Linee guida del gruppo dell'articolo 29 sulla trasparenza, pag. 39 («*Conformemente al principio di correttezza, i titolari del trattamento devono fornire sui destinatari le informazioni più pregnanti per gli interessati. In pratica, si tratterà in genere dei nomi dei destinatari, in maniera tale che gli interessati sappiano con precisione chi è in possesso dei dati personali che li riguardano. Se i titolari del trattamento optano per fornire le categorie dei destinatari, le informazioni dovrebbero essere il più specifiche possibile e indicare il tipo (ad es. facendo riferimento alle attività svolte), l'ambito di attività, il settore, il comparto e la sede dei destinatari*»); linee guida 1/2022 dell'EDPB sui diritti degli interessati - Diritto di accesso, versione 2.1, adottate il 28 marzo 2023 [in prosieguo «linee guida 1/2022 dell'EDPB (diritto di accesso)»], paragrafo 117 («*già ai sensi degli articoli 13 e 14 GDPR le informazioni sui destinatari o le categorie di destinatari dovrebbero essere il più possibile concrete nel rispetto dei principi di trasparenza e correttezza*»); cfr. sentenza della Corte di giustizia del 12 gennaio 2023, *RW contro Österreichische Post AG*, C-154/21, punto 25; conclusioni dell'avvocato generale nella causa C-154/21, punto 36 («*[gli] articoli 13 e 14 del RGPD [...] stabiliscono l'obbligo per il titolare del trattamento di fornire all'interessato le informazioni relative alle categorie di destinatari o ai destinatari concreti dei dati personali che lo riguardano, qualora questi ultimi siano raccolti presso l'interessato o non siano ottenuti presso l'interessato*»).
([24]) Articolo 5, paragrafo 1, lettera c), del GDPR. Linee guida 1/2022 dell'EDPB (diritto di accesso), paragrafi 116-117.
([25]) Sentenza della Corte di giustizia del 12 gennaio 2023, *RW contro Österreichische Post AG*, C-154/21, punto 51: «*l'articolo 15, paragrafo 1, lettera c), del RGPD deve essere interpretato nel senso che il diritto di accesso*

all'interessato solo le categorie di destinatari, in linea di principio dovrebbe essere sempre possibile per il titolare del trattamento recuperare i nomi dei destinatari e fornire le informazioni necessarie agli interessati senza indebito ritardo.

- L'articolo 19 del GDPR prevede che il titolare del trattamento comunichi a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. La Corte di giustizia ha chiarito che la seconda frase dell'articolo 19 conferisce espressamente all'interessato il diritto di essere informato dei destinatari concreti ([26]).

31. Sebbene ciò non sia esplicito in queste disposizioni, il comitato ritiene che, ai fini dell'articolo 28, paragrafi 1 e 2, del GDPR, i titolari del trattamento dovrebbero avere prontamente a disposizione in qualsiasi momento le informazioni sull'identità di tutti i responsabili del trattamento, i sub-responsabili del trattamento ecc. ([27]), in modo da poter adempiere al meglio i loro obblighi ai sensi delle disposizioni di cui sopra. Tale disponibilità è inoltre necessaria affinché i titolari del trattamento possano raccogliere e valutare tutte le informazioni necessarie per soddisfare i requisiti previsti dal GDPR, anche in modo da poter rispondere alle richieste di accesso ai sensi dell'articolo 15 del GDPR senza indebito ritardo e reagire rapidamente a violazioni dei dati che si verifichino lungo la catena di trattamento. Ciò si applicherebbe indipendentemente dal rischio associato all'attività di trattamento.

32. A tal fine, il responsabile del trattamento dovrebbe fornire proattivamente ([28]) al titolare del trattamento tutte le informazioni sull'identità di tutti i responsabili del trattamento, i sub-responsabili del trattamento ecc. che eseguono il trattamento per conto del titolare del trattamento e dovrebbe mantenere aggiornate in ogni momento tali informazioni relative a tutti i sub-responsabili del trattamento coinvolti. Il titolare del trattamento e il responsabile del trattamento possono includere nel contratto ulteriori dettagli circa le modalità e il formato con cui il responsabile del trattamento deve fornire tali informazioni, in quanto il titolare del trattamento può decidere di richiedere un formato specifico che gli consenta di recuperare e organizzare più facilmente le informazioni.

---

dell'interessato ai dati personali che lo riguardano, previsto da tale disposizione, implica, qualora tali dati siano stati o saranno comunicati a destinatari, l'obbligo per il titolare del trattamento di fornire a detto interessato l'identità stessa di tali destinatari, a meno che non sia impossibile identificare detti destinatari o che il suddetto titolare del trattamento non dimostri che le richieste di accesso dell'interessato sono manifestamente infondate o eccessive, ai sensi dell'articolo 12, paragrafo 5, del RGPD, nel qual caso il titolare del trattamento può indicare a detto interessato unicamente le categorie di destinatari di cui trattasi».

La Corte ha riconosciuto che l'interessato può anche «*scegliere di limitarsi a richiedere informazioni riguardanti le categorie di destinatari*». Sentenza della Corte di giustizia del 12 gennaio 2023, *RW contro Österreichische Post AG*, C-154/21, punto 43.

Linee guida 1/2022 dell'EDPB (diritto di accesso), paragrafo 117.

([26]) Sentenza della Corte di giustizia del 12 gennaio 2023, *RW contro Österreichische Post AG*, C-154/21, punto 41.

([27]) Tali informazioni sono necessarie affinché il titolare del trattamento possa adempiere i propri obblighi anche nel caso in cui la catena di sub-trattamento sia interrotta perché un (sub-)responsabile del trattamento è irraggiungibile, non disponibile o insolvente e un altro (sub-)responsabile del trattamento debba essere contattato.

([28]) Al fine di rispettare l'articolo 28, paragrafo 2, del GDPR, per consentire al titolare del trattamento di decidere in merito all'aggiunta di sub-responsabili del trattamento, e di rispettare l'articolo 28, paragrafo 1, del GDPR, per consentire al titolare del trattamento di verificare se i (sub-)responsabili del trattamento presentino garanzie sufficienti per attuare le misure tecniche e organizzative.

2.1.2 Verifica e documentazione, da parte del titolare del trattamento, dell'adeguatezza delle garanzie presentate da tutti i responsabili del trattamento nella catena del trattamento

33. Le domande 1.1.b.i, 1.1.b.iii e 1.3 mirano a chiarire in che misura e con quale livello di dettaglio il titolare del trattamento dovrebbe verificare e documentare l'adeguatezza delle garanzie presentate da tutti i responsabili del trattamento nella catena di trattamento e in quale misura gli obblighi di cui all'articolo 28, paragrafi 1 e 2, del GDPR, in combinato disposto con l'articolo 5, paragrafo 2, e l'articolo 24 del GDPR, variano a seconda del rischio associato all'attività di trattamento. Nel merito di tali domande, il comitato evidenzia i seguenti elementi.

34. L'articolo 5, paragrafo 2, del GDPR sancisce il principio di responsabilizzazione, in base al quale il responsabile del trattamento è competente per il rispetto dei principi di protezione dei dati di cui all'articolo 5, paragrafo 1, del GDPR e in grado di comprovarlo. L'articolo 5, paragrafo 2, del GDPR si applica a tutti i principi generali elencati nell'articolo 5, paragrafo 1, del GDPR.

35. L'articolo 24, paragrafo 1, del GDPR include l'obbligo del titolare del trattamento di dimostrare che il trattamento è effettuato conformemente al GDPR, ma sviluppa ulteriormente una delle funzioni a cui si applica il principio di responsabilizzazione: l'attuazione di «misure tecniche e organizzative adeguate» ([29]). L'articolo 24, paragrafo 1, del GDPR rileva la pertinenza ai fini dell'applicazione del concetto di «rischio» ([30]), che è uno dei criteri che il titolare del trattamento deve prendere in considerazione per valutare l'adeguatezza di tali misure ([31]). L'articolo 24, paragrafo 1, del GDPR aggiunge inoltre che dette misure devono essere riesaminate e aggiornate qualora necessario.

([29]) Sentenza della Corte di giustizia del 25 gennaio 2024, *BL contro MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, punto 36: «*L'articolo 24 del RGPD prevede un obbligo generale, gravante sul titolare del trattamento di dati personali, di attuare misure tecniche e organizzative adeguate per garantire che detto trattamento sia effettuato conformemente a tale regolamento, e per poterlo dimostrare* ».

([30]) Il considerando 75 del GDPR elenca alcuni esempi di rischi: «*il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo*»; il considerando 76 specifica: «*[l]a probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*». Come sintetizzato dalla Corte di giustizia, «*secondo il considerando 76 di tale regolamento, la probabilità e la gravità del rischio dipendono dalle specificità del trattamento in questione e tale rischio dovrebbe essere oggetto di una valutazione obiettiva*» (sentenza della Corte di giustizia del 14 dicembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punto 36).

([31]) Come affermato dalla Corte di giustizia, «*[l']articolo 24 elenca, al suo paragrafo 1, un certo numero di criteri da prendere in considerazione per valutare l'adeguatezza di siffatte misure, vale a dire la natura, l'ambito di applicazione, il contesto e le finalità del trattamento nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*», sentenza del 14 dicembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punto 25. Nella stessa sentenza, la Corte di giustizia ha precisato che «*[l']adeguatezza di siffatte misure deve essere valutata in concreto, esaminando se tali misure siano state attuate da detto responsabile (sic) tenendo conto dei diversi criteri previsti [...] e delle esigenze di protezione dei dati specificamente inerenti al trattamento di cui trattasi nonché ai rischi indotti da quest'ultimo*», punto 30; richiamato anche nella sentenza del 25 gennaio 2024, *BL contro MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, punto 38: «*[d]al testo degli articoli 24 e 32 del RGPD risulta quindi che l'adeguatezza delle misure attuate dal titolare del trattamento deve essere valutata in concreto, tenuto conto dei diversi criteri previsti da tali articoli e delle esigenze di protezione dei dati specificamente inerenti al trattamento di cui trattasi nonché ai rischi indotti da quest'ultimo, e ciò a maggior ragione in quanto il titolare del trattamento deve essere in grado di dimostrare*

36. Come affermato dalla Corte di giustizia, «*l'articolo 5, paragrafo 2, e l'articolo 24 del RGPD impongono obblighi generali di responsabilità e di conformità ai titolari del trattamento di dati personali. In particolare, tali disposizioni impongono ai titolari del trattamento di adottare le misure adeguate dirette a prevenire le eventuali violazioni delle norme previste dal RGPD a garanzia del diritto alla protezione dei dati» ([32]).*

37. Il principio di responsabilizzazione riguarda il titolare del trattamento, anche quando ha fatto ricorso a responsabili o sub-responsabili per eseguire il trattamento di dati personali per suo conto.

38. Ai sensi dell'articolo 28, paragrafo 1, del GDPR, qualora un titolare del trattamento incarichi un responsabile del trattamento di effettuare un trattamento di dati personali per suo conto, il titolare del trattamento deve avvalersi esclusivamente di un responsabile del trattamento che fornisca «*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti*» del GDPR «*e garantisca la tutela dei diritti dell'interessato*» ([33]). Come indicato nelle linee guida 07/2020 dell'EDPB, il principio di responsabilizzazione si riflette anche nell'articolo 28 del GDPR ([34]).

39. A tale proposito, l'EDPB rileva che, ai fini della valutazione della conformità all'articolo 24, paragrafo 1, e all'articolo 28, paragrafo 1, del GDPR, le autorità di controllo dovrebbero considerare che **il ricorso a responsabili del trattamento non dovrebbe abbassare il livello di protezione dei diritti degli interessati** rispetto a una situazione in cui il trattamento è effettuato direttamente dal titolare del trattamento. Ciò vale per il ricorso al primo responsabile del trattamento, ma anche per il ricorso a ulteriori responsabili lungo la catena di trattamento, ad esempio sub-responsabili e sub-sub-responsabili del trattamento. L'articolo 24, paragrafo 1, e l'articolo 28, paragrafo 1, del GDPR dovrebbero essere interpretati nel senso che il titolare del trattamento è tenuto ad assicurare che nella catena di trattamento siano coinvolti solo responsabili del trattamento, sub-responsabili del trattamento, sub-sub-responsabili del trattamento (ecc.) che presentino «garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate». Inoltre, il titolare del trattamento dovrebbe essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui al GDPR ([35]). Queste considerazioni sono valide anche se la catena di trattamento è lunga e complessa e coinvolge differenti responsabili del trattamento, sub-responsabili del trattamento ecc. in diverse fasi delle attività di trattamento. Il titolare del trattamento dovrebbe esercitare la dovuta diligenza nella selezione e nella supervisione dei responsabili del trattamento.

40. Per quanto riguarda la scelta del **primo responsabile del trattamento**, il titolare del trattamento dovrebbe verificare caso per caso l'adeguatezza delle garanzie presentate, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche, sulla base del tipo di trattamento affidato al responsabile del trattamento ([36]). A norma dell'articolo 28, paragrafo 5, del GDPR, l'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo

---

la conformità di dette misure a tale regolamento, possibilità di cui sarebbe privato se fosse ammessa una presunzione assoluta». Va osservato che l'analisi della Corte di giustizia riguarda anche l'articolo 32 del GDPR.

([32]) Sentenza della Corte di giustizia del 27 ottobre 2022, *Proximus NV contro Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, punto 81. Cfr. anche le linee guida 07/2020 dell'EDPB, paragrafo 9.

([33]) Linee guida 07/2020 dell'EDPB, paragrafo 94.

([34]) Linee guida 07/2020 dell'EDPB, paragrafo 8.

([35]) Linee guida 07/2020 dell'EDPB, paragrafo 94.

([36]) Linee guida 07/2020 dell'EDPB, paragrafo 96.

di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare garanzie sufficienti.

41. Come indicato in precedenza dall'EDPB, il titolare del trattamento dovrebbe tenere conto di diversi elementi al momento di verificare le garanzie presentate dai responsabili del trattamento ([37]) e spesso sarà necessario uno scambio di documentazione pertinente ([38]). In ogni caso «*[l]e garanzie «presentate» dal responsabile del trattamento sono quelle che il responsabile del trattamento è in grado di dimostrare in modo soddisfacente al titolare del trattamento , essendo queste le uniche che possono essere effettivamente prese in considerazione da detto titolare nel valutare l'adempimento dei suoi obblighi*» ([39]). Né l'articolo 28, paragrafo 1, del GDPR né i precedenti documenti dell'EDPB forniscono un elenco esaustivo dei documenti o delle azioni che il responsabile del trattamento dovrebbe mostrare o dimostrare, poiché ciò dipende in grande misura dalle circostanze specifiche del trattamento ([40]). Ad esempio, il titolare del trattamento può scegliere di redigere un questionario da utilizzare come strumento per raccogliere informazioni dal responsabile del trattamento al fine di verificare le garanzie pertinenti, richiedere la documentazione pertinente, basarsi su informazioni e/o certificazioni pubblicamente disponibili o su relazioni di audit preparate da terzi affidabili e/o effettuare audit in loco.

42. L'EDPB ha già specificato che l'obbligo di ricorrere unicamente a responsabili del trattamento «che presentino garanzie sufficienti», di cui all'articolo 28, paragrafo 1, del GDPR, è un obbligo permanente e che il titolare del trattamento, a intervalli adeguati, dovrebbe verificare le garanzie offerte dal responsabile del trattamento ([41]).

43. Alla luce della domanda 1.3 sollevata dall'autorità di controllo danese nella sua richiesta in merito al rischio associato al trattamento, l'EDPB sottolinea che il concetto di rischio svolge un ruolo importante in varie disposizioni del GDPR, in particolare quelle relative al capo IV del GDPR ([42]).

44. È importante rilevare che il riferimento al «rischio» di cui all'articolo 24, paragrafo 1, e al considerando 74 del GDPR non deve essere interpretato nel senso che il titolare del trattamento può prescindere o discostarsi dagli obblighi previsti dal GDPR per il semplice fatto di considerare «basso» il rischio per i diritti e le libertà degli interessati. L'obbligo di mettere in atto «misure tecniche e organizzative adeguate» per garantire la conformità al GDPR, in linea con l'articolo 24, paragrafo 1, del GDPR, si

([37]) Linee guida 07/2020 dell'EDPB, paragrafi 97-98 (che fanno riferimento alle conoscenze specialistiche, all'affidabilità e alle risorse del responsabile del trattamento, nonché alla reputazione del responsabile del trattamento sul mercato e all'adesione a un codice di condotta o a un meccanismo di certificazione approvato).
([38]) Linee guida 07/2020 dell'EDPB, paragrafo 95 (in cui ci citano alcuni esempi: politica in materia di privacy, condizioni di erogazione del servizio, registro delle attività di trattamento, meccanismi di gestione dei log, politica in materia di sicurezza delle informazioni, relazioni di audit esterni sulla protezione dei dati e certificazioni internazionali riconosciute, come la serie ISO 27000).
([39]) Linee guida 07/2020 dell'EDPB, paragrafo 95.
([40]) Linee guida 07/2020 dell'EDPB, paragrafo 96 («*La valutazione della sufficienza delle garanzie da parte del titolare del trattamento è una forma di valutazione del rischio che dipenderà in larga misura dal tipo di trattamento affidato al responsabile e va effettuata caso per caso, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche. Di conseguenza, l'EDPB non può fornire un elenco esaustivo dei documenti o delle attività che il responsabile del trattamento è tenuto a presentare o a dimostrare in un dato caso, in quanto ciò dipende in larga misura dalle circostanze specifiche del trattamento*»).
([41]) Linee guida 07/2020 dell'EDPB, paragrafo 99: «*anche mediante attività di revisione e ispezioni, se del caso*».
([42]) Il termine «rischio» è menzionato negli articoli 24, 25, 27, 30, 32, 33, 34, 35, 36 e 39 del GDPR.

applica sempre, ma le misure necessarie per raggiungere questo risultato possono variare a seconda del rischio ([43]).

45. Pur non contenendo riferimenti specifici al «rischio», l'articolo 28, paragrafo 1, del GDPR implica la necessità di considerare il livello di rischio per i diritti e le libertà degli interessati. La disposizione di cui all'articolo 28, paragrafo 1, di ricorrere unicamente a responsabili del trattamento che presentino «garanzie sufficienti» per mettere in atto «misure tecniche e organizzative adeguate» dovrebbe essere interpretato nel senso che è necessario considerare la fornitura da parte dei responsabili del trattamento di garanzie sufficienti per l'attuazione di tali misure alla luce dei rischi del trattamento, in quanto, ad esempio, il livello delle misure di sicurezza da attuare dipende anche dai rischi.

46. Il rischio associato all'attività di trattamento svolge un ruolo importante nel determinare l'adeguatezza delle misure tecniche e organizzative, insieme agli altri criteri citati all'articolo 24, paragrafo 1, del GDPR ([44]). A seconda del livello di rischio associato all'attività di trattamento (ad esempio, qualora siano trattate categorie particolari di dati personali), il titolare del trattamento può definire misure tecniche e organizzative più rigorose o più ampie. Qualsiasi responsabile del trattamento dovrebbe pertanto fornire garanzie sufficienti per mettere in atto efficacemente le misure «appropriate» definite dal titolare del trattamento.

47. Il comitato ritiene che **l'*obbligo* del titolare del trattamento di verificare se i (sub-)responsabili del trattamento presentino garanzie sufficienti per attuare le misure determinate dal titolare del trattamento debba applicarsi indipendentemente dal rischio per i diritti e le libertà degli interessati.**

48. **Tuttavia, la *portata* di tale verifica varierà nella pratica a seconda della natura di tali misure organizzative e tecniche determinate dal titolare del trattamento sulla base, tra gli altri criteri, del rischio associato al trattamento.** Ad esempio, qualora le attività di trattamento presentino un rischio limitato per i diritti e le libertà degli interessati, le corrispondenti «misure appropriate» saranno meno restrittive. Pertanto, nella pratica, la portata della verifica da parte del titolare del trattamento può essere meno ampia. Per contro, qualora il trattamento in questione sia associato a rischi più elevati, il livello della verifica del titolare del trattamento può essere più alto, in termini di controllo delle garanzie sufficienti presentate dall'intera catena di trattamento, dato che le «misure appropriate» da attuare per affrontare i rischi per gli interessati sono più ampie e solide.

49. A tale riguardo, a seconda del livello di rischio associato all'attività di trattamento, il titolare del trattamento può aumentare il livello della verifica, controllando i contratti di sub-trattamento autonomamente e/o imponendo al primo responsabile del trattamento di provvedere a una verifica e a una documentazione più ampie.

50. Conformemente al principio di responsabilizzazione, qualsiasi misura considerata necessaria per il rispetto del GDPR, anche sulla base del rischio comportato dal trattamento, dovrebbe essere

([43]) Sentenza della Corte di giustizia del 14 dicembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punto 35: «*il considerando 74 del RGPD sottolinea che è importante che il titolare del trattamento sia tenuto ad attuare misure adeguate ed efficaci e sia in grado di dimostrare la conformità delle attività di trattamento con tale regolamento, compresa l'efficacia delle misure, le quali dovrebbero tener conto dei criteri, connessi alle caratteristiche del trattamento in questione e al rischio presentato da quest'ultimo, che sono altresì enunciati ai suoi articoli 24 e 32*».

([44]) L'articolo 24, paragrafo 1, tiene conto «*della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*».

adeguatamente documentata dal titolare del trattamento ([45]). Tale obbligo è facilitato, da un lato, dagli **obblighi di assistenza e di audit** imposti ai responsabili del trattamento e, dall'altro, dalle **informazioni fornite dal primo responsabile del trattamento** al titolare del trattamento prima del ricorso a ulteriori responsabili del trattamento.

51. In primo luogo, il comitato osserva che i responsabili del trattamento hanno il dovere di assistere il titolare del trattamento ai fini della conformità a determinati requisiti del GDPR [ai sensi dell'articolo 28, paragrafo 3, lettere e) e f)] ([46]). Più in generale, il responsabile del trattamento ha il dovere di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità all'articolo 28 [articolo 28, paragrafo 3, lettera h)] ([47]). Il titolare del trattamento dovrebbe essere pienamente informato in merito agli elementi del trattamento atti a dimostrare il rispetto degli obblighi di cui all'articolo 28 del GDPR e il responsabile del trattamento dovrebbe fornire tutte le informazioni sulle modalità di effettuazione dell'attività di trattamento per conto del titolare ([48]). Il contratto dovrebbe specificare la frequenza e le modalità di tale flusso di informazioni ([49]).

52. Pertanto, il titolare del trattamento può basarsi sulle informazioni fornite dal responsabile del trattamento, ai sensi dell'articolo 28, paragrafo 3, lettera h), del GDPR, per adempiere l'obbligo relativo alla documentazione delle misure adottate, a condizione che le informazioni presentate dal responsabile del trattamento dimostrino effettivamente la conformità. Poiché il responsabile del trattamento si trova in una posizione privilegiata per conoscere i dettagli del trattamento che effettua e del trattamento effettuato dai sub-responsabili, deve mettere proattivamente a disposizione del titolare del trattamento tutte le informazioni pertinenti ([50]).

([45]) Per quanto riguarda l'onere della prova del titolare del trattamento, cfr. la sentenza della Corte di giustizia del 14 dicembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punto 52: «*[d]al disposto dell'articolo 5, paragrafo 2, dell'articolo 24, paragrafo 1, e dell'articolo 32, paragrafo 1, del RGPD risulta senza ambiguità che l'onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza ai sensi dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 32 di detto regolamento incombe al titolare del trattamento in parola*»; cfr. anche la sentenza della Corte di giustizia del 25 gennaio 2024, BL contro MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, punto 42: «*[a] questo proposito, occorre sottolineare che dal combinato disposto degli articoli 5, 24 e 32 del RGPD, letti alla luce del considerando 74 di quest'ultimo, risulta che, nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento, l'onere di dimostrare che i dati personali siano trattati in modo da garantire un'adeguata sicurezza di questi ultimi, ai sensi dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 32 di tale regolamento, incombe al titolare del trattamento in questione. Una siffatta ripartizione dell'onere della prova è idonea non solo a indurre i titolari del trattamento di tali dati ad adottare le misure di sicurezza prescritte dal RGPD, ma anche a salvaguardare l'effetto utile del diritto al risarcimento previsto all'articolo 82 di tale regolamento e a rispettare le intenzioni del legislatore dell'Unione menzionate al considerando 11 di quest'ultimo*».

([46]) Cfr. le linee guida 07/2020 dell'EDPB, paragrafi 130-138.

([47]) Cfr. le linee guida 07/2020 dell'EDPB, paragrafi 143-145.

([48]) Linee guida 07/2020 dell'EDPB, paragrafo 143.

([49]) Linee guida 07/2020 dell'EDPB, paragrafo 143.

([50]) Linee guida 07/2020 dell'EDPB, paragrafo 143, che richiama l'articolo 28, paragrafo 3, lettera h): «*[a]d esempio, le sezioni pertinenti dei registri delle attività di trattamento del responsabile possono essere condivise con il titolare del trattamento. Il responsabile del trattamento dovrebbe fornire tutte le informazioni sulle modalità di effettuazione dei trattamenti svolti per conto del titolare. Tali informazioni dovrebbero includere dettagli sul funzionamento dei sistemi utilizzati, sulle misure di sicurezza, sul modo in cui sono soddisfatti i requisiti di conservazione dei dati, sull'ubicazione e sui trasferimenti dei dati, su chi vi ha accesso e su chi sono i relativi destinatari, sui sub-responsabili ecc.*». La possibilità per il titolare del trattamento di effettuare audit è inoltre specificata al paragrafo 144: «*[l]'obiettivo di dette attività di revisione è garantire che il titolare disponga di tutte le informazioni relative all'attività di trattamento svolta per suo conto e alle garanzie fornite dal responsabile del trattamento*.»

53. Quanto sopra si applica anche ai sub-responsabili del trattamento. Di fatto, i responsabili del trattamento sono tenuti a trasferire gli obblighi di assistenza lungo la catena di trattamento (articolo 28, paragrafo 4, del GDPR).

54. In secondo luogo, il **ricorso a sub-responsabili del trattamento**, come ricordato in precedenza, è possibile solo previa autorizzazione scritta del titolare del trattamento, che potrebbe essere specifica o generale. Se il titolare del trattamento sceglie di dare un'autorizzazione generale, questa «*dovrebbe essere integrata da criteri che guidino la scelta del responsabile del trattamento (ad esempio garanzie in termini di misure tecniche e organizzative, conoscenze specialistiche, affidabilità e risorse)*» ([51]).

55. Come chiarito dall'EDPB, «*[p]er effettuare la valutazione e decidere se autorizzare o meno tale ulteriore esternalizzazione, il responsabile del trattamento dovrà fornire al titolare un elenco dei sub-responsabili previsti (contenente, per ciascuno di essi: l'ubicazione, le modalità di esecuzione e la prova delle garanzie messe in atto)*» ([52]). Tali informazioni sono necessarie affinché il titolare del trattamento possa soddisfare il principio di responsabilizzazione di cui all'articolo 24 e le disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR ([53]). Per quanto riguarda i trasferimenti di dati personali al di fuori del SEE, il comitato fa riferimento alla risposta fornita di seguito alla domanda 1.2 posta dall'autorità di controllo danese.

56. Come ricordato dall'EDPB, il primo responsabile del trattamento dovrebbe assicurare di proporre sub-responsabili in grado di offrire garanzie sufficienti ([54]). La necessità per il primo responsabile del trattamento di fornire le informazioni di cui sopra dimostra che il **responsabile del trattamento ha un ruolo da svolgere nella scelta dei sub-responsabili e nella verifica delle garanzie da essi offerte e dovrebbe fornire al titolare del trattamento informazioni sufficienti**. Ciò è anche coerente con il fatto che, a prescindere dai criteri indicati dal titolare del trattamento per la scelta di ulteriori responsabili del trattamento, il primo responsabile del trattamento conserva nei confronti del titolare l'intera responsabilità per l'adempimento degli obblighi dei sub-responsabili (articolo 28, paragrafo 4, del GDPR).

57. A questo proposito, anche se, ai sensi dell'articolo 28, paragrafo 4, del GDPR, è responsabilità diretta del responsabile del trattamento che fa ricorso a un sub-responsabile assicurare che gli stessi obblighi di protezione dei dati stabiliti nel contratto iniziale tra il titolare del trattamento e il responsabile del trattamento siano imposti a tale altro responsabile, ciò non esime il titolare del trattamento dalla responsabilità di assicurare la conformità ai requisiti dell'articolo 28, paragrafo 1, e dell'articolo 24, paragrafo 1, del GDPR e di essere in grado di dimostrare tale conformità.

58. **La decisione finale in merito al ricorso a uno specifico sub-(sub-)responsabile del trattamento e la relativa responsabilità, anche per quanto riguarda la verifica dell'adeguatezza delle garanzie fornite dal (sub-)responsabile del trattamento, incombono al titolare del trattamento.** Come già ricordato, in caso di autorizzazione generica o specifica, spetta sempre al titolare del trattamento decidere se approvare il ricorso a tale sub-responsabile del trattamento o se opporvisi.

59. Nel valutare la conformità all'articolo 24, paragrafo 1, e all'articolo 28, paragrafo 1, del GDPR, le autorità di controllo dovrebbero valutare se il titolare del trattamento sia in grado di dimostrare che la verifica dell'adeguatezza delle garanzie fornite dai sub-responsabili del trattamento ha avuto luogo con soddisfazione del titolare del trattamento. Ciò implica che il titolare del trattamento può scegliere

([51]) Linee guida 07/2020 dell'EDPB, paragrafo 156.
([52]) Linee guida 07/2020 dell'EDPB, paragrafo 152.
([53]) Linee guida 07/2020 dell'EDPB, nota 69.
([54]) Linee guida 07/2020 dell'EDPB, paragrafo 159.

di basarsi sulle informazioni ricevute dal responsabile del trattamento e, se necessario, approfondirle. Ad esempio, qualora le informazioni ricevute dal titolare del trattamento appaiano incomplete, imprecise o sollevino dubbi oppure ove necessario in base alle circostanze del caso, compreso il rischio associato al trattamento, il titolare del trattamento dovrebbe chiedere ulteriori informazioni e/o verificare le informazioni ricevute e, se opportuno, completarle o correggerle.

60. Più specificamente, per i trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, il titolare del trattamento dovrebbe aumentare il livello della verifica in termini di controllo delle informazioni fornite in merito alle garanzie presentate dai diversi responsabili lungo la catena di trattamento.

2.1.3 Verifica del contratto tra il primo responsabile del trattamento e gli ulteriori responsabiliError! Bookmark not defined.

61. L'autorità di controllo danese chiede in sostanza se e in quale misura il titolare del trattamento abbia il dovere di verificare e documentare che i contratti di sub-trattamento impongono gli stessi obblighi agli ulteriori responsabili del trattamento.

62. A tale riguardo, l'articolo 28, paragrafo 4 ([55]) impone un obbligo diretto ai responsabili del trattamento. Inoltre, l'articolo 28, paragrafo 3, lettera d) richiede che il titolare del trattamento e il responsabile del trattamento «stipulino» nel loro contratto l'obbligo per il responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 4, rendendo così tale requisito un obbligo contrattuale per il responsabile del trattamento. In altri termini, **il primo responsabile del trattamento è giuridicamente e contrattualmente tenuto a trasferire gli stessi obblighi in materia di protezione dei dati nei contratti di sub-trattamento che conclude con ulteriori responsabili del trattamento**.

([55]) Articolo 28, paragrafo 4, del GDPR: «*[q]uando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento*».

63. Analogamente, gli ulteriori responsabili del trattamento saranno obbligati per contratto (dal primo responsabile del trattamento) a imporre ai rispettivi responsabili del trattamento gli stessi obblighi in materia di protezione dei dati e così via lungo la catena di trattamento ([56]). Non è necessario che il testo del contratto di sub-trattamento sia identico a quello del contratto di trattamento dei dati stipulato con il primo responsabile del trattamento ([57]).

64. Il comitato ricorda che, se un sub-responsabile del trattamento non adempie i propri obblighi, la responsabilità ultima per l'adempimento degli obblighi di tale altro sub-responsabile del trattamento ricade sul titolare del trattamento. Tuttavia, il primo responsabile del trattamento rimarrà responsabile nei confronti del titolare del trattamento, che potrà pertanto far valere un diritto contrattuale nei confronti del primo responsabile del trattamento qualora quest'ultimo non trasferisca gli stessi obblighi in materia di protezione dei dati nei contratti di sub-trattamento.

65. I responsabili del trattamento hanno il dovere di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità all'articolo 28, paragrafo 3, lettera h), del GDPR. Pertanto, su richiesta del titolare del trattamento, il primo responsabile del trattamento dovrà fornire i contratti di sub-trattamento tra il primo responsabile del trattamento e gli ulteriori responsabili del trattamento.

66. A questo proposito, le clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento ([58]) e le clausole contrattuali tipo per il trasferimento internazionale ([59]) della

([56]) Nel parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, l'EDPB e il GEPD hanno sottolineato che la disposizione di cui all'articolo 28, paragrafo 4, del GDPR deve essere presa in considerazione dalle parti in un rapporto tra responsabili del trattamento (paragrafo 66).

([57]) Linee guida 07/2020 dell'EDPB, paragrafo 160: «*[l]'imposizione dei «medesimi» obblighi dovrebbe essere interpretata in senso funzionale piuttosto che formale: non è necessario che il contratto contenga esattamente la stessa formulazione impiegata nel contratto tra il titolare e il responsabile del trattamento; tuttavia dovrebbe garantire che, nella sostanza, gli obblighi siano identici*». L'EDPB osserva inoltre che, laddove due responsabili del trattamento si basino sul modulo tre (da responsabile del trattamento a responsabile del trattamento) delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, una garanzia supplementare è fornita dal primo responsabile del trattamento. Ai sensi della clausola 8.1.d delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, l'esportatore dei dati (il primo responsabile del trattamento) garantisce di aver imposto all'importatore dei dati (sub-responsabile del trattamento) gli stessi obblighi in materia di protezione dei dati previsti dal contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri tra il titolare del trattamento e l'esportatore dei dati.

([58]) La sezione 7, clausola 7.7, lettera c), relativa al ricorso a sub-responsabili del trattamento, delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea dispone quanto segue: «*[s]u richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia*». Decisione di esecuzione (UE) 2021/915 della Commissione, del 4 giugno 2021, relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 («clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento»).

([59]) La clausola 9, modulo due (da titolare del trattamento a responsabile del trattamento), lettera c) delle clausole contrattuali tipo della Commissione europea per il trasferimento internazionale, prevede quanto segue: «*[s]u richiesta dell'esportatore, l'importatore gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, l'importatore può espungere informazioni dal contratto prima di trasmetterne una copia*». Inoltre, ai sensi del modulo tre (da responsabile del trattamento a responsabile del

Commissione europea prevedono per il titolare del trattamento la possibilità di richiedere una copia del contratto di sub-trattamento tra il primo responsabile del trattamento e gli ulteriori responsabili del trattamento. Tale possibilità è prevista anche da tre clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento adottate dalle autorità di controllo ([60]). Questa possibilità è un'espressione del diritto di revisione del titolare del trattamento ai sensi dell'articolo 28, paragrafo 3, lettera h), del GDPR. Su richiesta del titolare del trattamento, il responsabile del trattamento dovrebbe fornire tale copia.

67. Tuttavia, l'EDPB osserva che le clausole contrattuali tipo non disciplinano se un titolare del trattamento *debba* richiedere tale copia al fine di rispettare l'articolo 28, paragrafo 1, del GDPR.

68. In tale ottica, il fatto che il titolare del trattamento scelga o meno di richiedere tale copia non può determinare la responsabilità del titolare del trattamento. In ogni caso, anche il responsabile del trattamento è soggetto a obblighi giuridici e contrattuali in base ai quali deve imporre gli stessi obblighi in materia di protezione dei dati contenuti nel contratto iniziale.

69. Ciò detto, il **titolare del trattamento non ha il dovere di richiedere sistematicamente i contratti di sub-trattamento per verificare se gli obblighi di protezione dei dati previsti nel contratto iniziale siano stati trasferiti lungo la catena di trattamento**. Il titolare del trattamento dovrebbe valutare, caso per caso, se richiedere una copia di tali contratti o esaminarli in qualsiasi momento sia necessario per poter dimostrare la conformità alla luce del principio di responsabilizzazione. Nell'ambito dell'esercizio del diritto di revisione ai sensi dell'articolo 28, paragrafo 3, lettera h), il titolare del trattamento dovrebbe disporre di un processo per effettuare azioni di revisione al fine di controllare, mediante verifiche a campione, che i contratti con i suoi sub-responsabili contengano i necessari obblighi in materia di protezione dei dati.

70. La necessità di richiedere una copia del contratto di sub-trattamento dipende quindi dalle circostanze di specie. Ad esempio, in presenza di dubbi sulla conformità del responsabile del trattamento o del sub-responsabile del trattamento ai requisiti di cui all'articolo 28, paragrafi 1 e 4, o su richiesta dell'autorità di controllo, il titolare del trattamento dovrebbe richiedere il contratto per esaminarlo (ad esempio, nel caso in cui l'ulteriore responsabile del trattamento sia interessato da una violazione dei dati o nel caso di altre informazioni pubblicamente disponibili o di altre informazioni a disposizione del titolare del trattamento), ad esempio alcuni modelli del contratto di trattamento dei dati del sub-responsabile del trattamento potrebbero non rispettare le disposizioni di cui all'articolo 28, paragrafo 3, del GDPR.

71. Per garantire il rispetto dell'articolo 28, paragrafo 1, alla luce del principio di responsabilizzazione, una copia dei contratti di sub-trattamento può aiutare il titolare del trattamento a dimostrare che i responsabili e i sub-responsabili del trattamento presentano garanzie sufficienti, compreso il fatto che il responsabile del trattamento rispetta l'articolo 28, paragrafo 4, del GDPR.L'EDPB osserva che un

---

trattamento), «*[s]u richiesta dell'esportatore o del titolare del trattamento, l'importatore fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, l'importatore può espungere informazioni dal contratto prima di trasmetterne una copia*». Decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (clausole contrattuali tipo della Commissione europea per il trasferimento internazionale).

([60]) Clausole contrattuali tipo dell'autorità di controllo danese ai fini della conformità con l'articolo 28 del GDPR, in particolare la clausola 7.5; clausole contrattuali tipo dell'autorità di controllo lituana ai fini della conformità con l'articolo 28 del GDPR, in particolare la clausola 18; clausole contrattuali tipo dell'autorità di controllo slovena ai fini della conformità con l'articolo 28 del GDPR, in particolare la clausola 6.5.

titolare del trattamento potrebbe non essere in grado di valutare se le garanzie presentate in relazione a un sub-responsabile del trattamento siano sufficienti o meno senza aver consultato e valutato il contenuto del contratto di sub-trattamento. Sebbene le garanzie possano essere previste per iscritto nel contratto, le clausole contrattuali non possono, di per sé, dimostrare che le garanzie sufficienti siano effettivamente applicate dalle parti del contratto.

2.2 Interpretazione dell'articolo 28, paragrafo 1, del GDPR in combinato disposto con l'articolo 44 del GDPR (trasferimenti nella catena di trattamento - domande 1.2 e 1.3)

72. La domanda 1.2 richiede chiarimenti per i casi di trasferimenti o trasferimenti successivi da un (sub-)responsabile del trattamento a un altro (sub-)responsabile del trattamento, in particolare riguardo alla misura in cui il titolare del trattamento, nell'ambito dell'obbligo ai sensi dell'articolo 28, paragrafo 1, del GDPR, in combinato disposto con l'articolo 44 del GDPR, dovrebbe valutare la documentazione fornita dai (sub-)responsabili del trattamento per determinare che il livello di protezione dei dati personali non è compromesso dai trasferimenti iniziali o successivi.

73. La domanda 1.3 richiede chiarimenti sulla questione se la portata degli obblighi sanciti dall'articolo 28, paragrafo 1, del GDPR, in combinato disposto con l'articolo 5, paragrafo 2, e l'articolo 24 del GDPR, di cui alla risposta alla domanda 1.2, vari a seconda del rischio associato all'attività di trattamento. In caso di risposta affermativa, l'autorità di controllo danese chiede quale sia la portata di tali obblighi per le attività di trattamento «a basso rischio» e «ad alto rischio».

Chiarimenti introduttivi

74. A fini di chiarezza, si presentano alcuni chiarimenti introduttivi relativi a tali domande nel contesto del presente parere.

75. In primo luogo, l'EDPB interpreta il termine «trasferimento» nel significato di cui alle linee guida 5/2021 dell'EDPB sull'interazione tra l'articolo 3 e il capo V del GDPR ([61]) [in prosieguo «linee guida 5/2021 dell'EDPB (interazione)»], che rimandano anche alle linee guida 3/2018 dell'EDPB sull'ambito di applicazione territoriale del RGPD ([62]). Come evidenziato in precedenza dall'EDPB, l'accesso remoto da un paese terzo costituisce un trasferimento se soddisfa i criteri stabiliti nelle linee guida 5/2021 dell'EDPB (interazione) ([63]). In ogni caso, l'esistenza di un trasferimento innesca l'applicazione del capo V del GDPR.

76. In secondo luogo, poiché la domanda 1.2 si riferisce a una situazione in cui un (sub-)responsabile del trattamento effettua un trasferimento iniziale o successivo a un altro (sub-)responsabile, il titolare del trattamento non è l'esportatore di dati; quest'ultimo è invece un responsabile del trattamento, che trasferisce i dati personali a un altro responsabile lungo la catena per conto del titolare del trattamento e non a un titolare del trattamento distinto. Sono pertanto esclusi i dati personali trasferiti a titolari del trattamento distinti, compresi gli organi giurisdizionali o le autorità amministrative di paesi terzi. Pertanto, l'interpretazione dell'articolo 48 del GDPR non rientra nell'ambito di queste domande.

77. In terzo luogo, l'EDPB osserva che la domanda 1.2 si riferisce ai trasferimenti che avvengono lungo la catena di trattamento conformemente all'istruzione documentata del titolare del trattamento a norma dell'articolo 28, paragrafo 3, lettera a), del GDPR. È opportuno sottolineare che spetta al titolare del trattamento decidere se un trasferimento di dati personali al di fuori del SEE sia possibile nell'ambito delle attività di trattamento affidate ai (sub-)responsabili del trattamento. Il responsabile del trattamento dovrebbe astenersi dall'eseguire qualsiasi trasferimento iniziale o successivo se non è istruito in tal senso dal titolare del trattamento ([64]). L'istruzione documentata del titolare del trattamento in relazione ai trasferimenti iniziali o successivi di dati personali deve essere trasmessa lungo la catena di trattamento ([65]).

78. In quarto luogo, l'EDPB chiarisce che il concetto di rischio di cui alla domanda 1.3 dovrebbe essere inteso come rischio per i diritti e le libertà degli interessati i cui dati personali sono trattati, ai sensi dei considerando 75 e 76 del GDPR (come già indicato al paragrafo 35).

La responsabilità del titolare del trattamento sussiste anche se i (sub-)responsabili del trattamento effettuano i trasferimenti iniziali o successivi.

([61]) Linee guida 5/2021 dell'EDPB sull'interazione tra l'applicazione dell'articolo 3 e le disposizioni in materia di trasferimenti internazionali di cui al capo V GDPR, versione 2.0, adottate il 14 febbraio 2023, in cui il paragrafo 9 stabilisce i tre criteri cumulativi per qualificare un'operazione di trattamento come trasferimento e, più in generale, la sezione 2 specifica tali criteri.
([62]) Paragrafo 12 delle linee guida 5/2021 dell'EDPB (interazione), che richiama le linee guida 3/2018 dell'EDPB sull'ambito di applicazione territoriale del RGPD, versione 2.1, adottate il 12 novembre 2019 (con rettifica del 7 gennaio 2020), pag. 5 e sezioni da 1 a 3. Cfr. in particolare la lettera «d) Responsabile del trattamento non stabilito nell'Unione» della sezione 2.
([63]) Linee guida 5/2021 dell'EDPB (interazione), paragrafo 16.
([64]) Articolo 29 del GDPR. Come ricordato dall'EDPB, «*[i]l contratto dovrebbe specificare i requisiti per i trasferimenti verso paesi terzi o organizzazioni internazionali tenendo conto delle disposizioni di cui al capo V del GDPR*» (linee guida 07/2020 dell'EDPB, paragrafo 119). Ad esempio, il titolare del trattamento può scegliere di vietare i trasferimenti o di autorizzarli solo verso paesi specifici.
([65]) Articolo 60, paragrafo 4, del GDPR.

79. Per quanto riguarda il merito della richiesta, l'EDPB ha già specificato che «*[...] si verificherà un trasferimento in una situazione in cui, su istruzione del proprio titolare del trattamento, un responsabile del trattamento invii dati (a norma dell'articolo 3, paragrafo 1, o dell'articolo 3, paragrafo 2, per uno dei trattamenti di cui sopra) a un altro responsabile del trattamento o anche a un titolare del trattamento situato in un paese terzo. In questi casi il responsabile del trattamento funge da esportatore di dati per conto del titolare del trattamento e deve garantire, secondo le istruzioni di quest'ultimo, il rispetto delle disposizioni del capo V per il trasferimento in questione, inclusa l'adeguatezza dello strumento di trasferimento utilizzato. Dal momento che il trasferimento è un'attività di trattamento svolta per suo conto,* ***il titolare del trattamento è anch'esso responsabile e potrebbe rispondere ai sensi del capo V; deve inoltre assicurarsi che il responsabile del trattamento presenti garanzie sufficienti ai sensi dell'articolo 28***» ([66]).

80. In altri termini, nel caso di un trasferimento, anche se non effettuato direttamente dal titolare del trattamento, ma per suo conto da un responsabile del trattamento, il titolare del trattamento rimane soggetto agli obblighi derivanti sia dall'articolo 44 del GDPR che dall'articolo 28, paragrafo 1, del GDPR ([67]) ([68]).

Responsabilità derivante dall'articolo 44 del GDPR

81. Gli obblighi di cui all'articolo 44 del GDPR ([69]) riguardano sia i responsabili del trattamento (che, nel contesto del parere, fungono da esportatori di dati) sia i titolari del trattamento ([70]). Sia i responsabili del trattamento sia i titolari del trattamento dovrebbero pertanto assicurare che il livello di protezione dei dati personali non sia pregiudicato dal trasferimento iniziale o successivo, a prescindere all'origine del trasferimento ([71]). Ad esempio, sia i titolari del trattamento sia i responsabili del trattamento, in linea di principio, rimangono responsabili ai sensi del capo V del GDPR di un trasferimento iniziale o successivo illegittimo ([72]) e pertanto potrebbero essere congiuntamente e singolarmente ritenuti responsabili in caso di violazione.

Responsabilità derivante dall'articolo 28, paragrafo 1, del GDPR

82. In base al principio di responsabilizzazione, i titolari del trattamento sono tenuti ad adottare «misure appropriate» per prevenire violazioni delle norme stabilite dal GDPR al fine di garantire il diritto alla

([66]) Linee guida 5/2021 dell'EDPB (interazione), paragrafo 19, grassetto aggiunto.
([67]) È altresì pertinente rilevare che l'articolo 28, paragrafo 1, del GDPR fa riferimento al rispetto dei requisiti del regolamento stesso e, pertanto, dovrebbe essere inteso come comprensivo delle disposizioni del capo V relative ai trasferimenti iniziali o successivi di dati personali verso paesi terzi. Ciò riguarda sia i trasferimenti iniziali che quelli successivi, cfr. l'articolo 44 del GDPR.
([68]) Ai fini della presente sezione del parere, si considerano gli obblighi derivanti dall'articolo 44 e dall'articolo 28, paragrafo 1, del GDPR, con la precisazione che il titolare del trattamento rimane soggetto a tutti gli obblighi applicabili ai titolari del trattamento a norma del GDPR.
([69]) L'articolo 44 del GDPR richiama le disposizioni del capo V del GDPR.
([70]) L'articolo 44 GDPR richiama «il titolare del trattamento e il responsabile del trattamento» ai fini del rispetto delle condizioni di cui al capo V; cfr. anche il considerando 101. Per questo motivo, le raccomandazioni 01/2020 dell'EDPB relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, versione 2.0, adottate il 18 giugno 2021 (in prosieguo «raccomandazioni 01/2020 dell'EDPB») si applicano agli «esportatori di dati» (siano essi titolari o (sub-)responsabili del trattamento che trattano dati personali).
([71]) Sentenza della Corte di giustizia del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Ltd, Maximillian Schrems* (in prosieguo «sentenza Schrems II della Corte di giustizia», causa C-311/18, ECLI:EU:C:2020:559, punto 92.
([72]) Il titolare del trattamento può chiedere al responsabile del trattamento un risarcimento corrispondente alla sua parte di responsabilità, purché siano soddisfatte le condizioni di cui all'articolo 82, paragrafo 5, del GDPR.

protezione dei dati ([73]), comprese le violazioni di cui al capo V del GDPR. Tale responsabilità si applica prima dell'inizio del trasferimento e per tutta la durata del trattamento dei dati personali trasferiti nel paese terzo.

83. Come chiarito nei precedenti paragrafi 47 e 48, l'*obbligo del titolare del trattamento* di verificare se i (sub-)responsabili del trattamento presentino garanzie sufficienti per attuare le misure determinate dal titolare del trattamento ai sensi dell'articolo 28, paragrafo 1, del GDPR ([74]) dovrebbe applicarsi indipendentemente dal rischio per i diritti e le libertà degli interessati. Tuttavia, la *portata* di tale verifica varierà nella pratica in funzione della natura delle misure tecniche e organizzative determinate dal titolare del trattamento sulla base, tra gli altri criteri, del rischio associato al trattamento ([75]). A tale riguardo, l'esistenza di un trasferimento iniziale o successivo verso paesi terzi lungo la catena di trattamento può aumentare i rischi derivanti dal trattamento ed incide pertanto sulle misure «appropriate» determinate dal titolare del trattamento ([76]).

84. Su richiesta, il titolare del trattamento, con l'assistenza del responsabile del trattamento e dei sub-responsabili del trattamento, dovrebbe essere in grado di dimostrare all'autorità di controllo competente il rispetto dei requisiti di cui all'articolo 28, paragrafo 1, del GDPR. La documentazione adeguata potrebbe basarsi, tra l'altro, sulle informazioni ricevute dai responsabili del trattamento nel contesto del ricorso a (sub-)responsabili del trattamento ([77]) (cfr. paragrafi 54-56), ma anche con l'assistenza dei responsabili del trattamento, conformemente all'articolo 28, paragrafo 3, lettera h), del GDPR (cfr. paragrafi 51 e 52).

85. Il titolare del trattamento ha inoltre bisogno di tutte le informazioni pertinenti per impartire le istruzioni necessarie al trasferimento dei dati personali verso i paesi terzi interessati e per rispettare il principio di responsabilizzazione di cui all'articolo 5, paragrafo 2, e all'articolo 24 del GDPR nonché le

([73]) Cfr. la sezione precedente sull'articolo 5, paragrafo 2, e sull'articolo 24, paragrafo 1, in combinato disposto con l'articolo 28, paragrafo 1, del GDPR.

([74]) A scanso di dubbi, è opportuno chiarire che le «misure tecniche e organizzative adeguate» di cui all'articolo 24, paragrafo 1, e all'articolo 28, paragrafo 1, del GDPR non devono essere confuse con le «misure supplementari» menzionate nelle raccomandazioni 01/2020 dell'EDPB (paragrafo 50: «*"misure supplementari" integrano per definizione le garanzie già previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD e qualsiasi altro requisito di sicurezza applicabile (per esempio misure tecniche di sicurezza) previste dal RGPD*», in riferimento al considerando 109 del GDPR e alla sentenza Schrems II della Corte di giustizia, punto 133.

([75]) Cfr. la definizione di rischio, come chiarito nei paragrafi 35 e 78.

([76]) Il considerando 116 del GDPR recita: «*[c]on i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni*».

([77]) Cfr. anche la clausola 9, lettera a), modulo tre (da responsabile del trattamento a responsabile del trattamento) delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea e il relativo allegato III; cfr. anche la clausola 9, lettera a), modulo due (da titolare del trattamento a responsabile del trattamento) e la clausola 7.7, lettera a), delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento e il relativo allegato IV «Elenco dei sub-responsabili del trattamento». Sia l'allegato II delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea sia l'allegato IV delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea devono essere compilati con le seguenti informazioni sui sub-responsabili del trattamento in caso di autorizzazione specifica del titolare del trattamento: nome, indirizzo, nome, qualifica e dati di contatto del referente e descrizione del trattamento. Inoltre, l'allegato I delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, sezione B «Descrizione del trasferimento» include quanto segue: «[p]er i trasferimenti a (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento». Analogamente, l'allegato II delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento comprende quanto segue: «[p]er il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento».

disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR ([78]). Il titolare del trattamento può opporsi o non autorizzare il ricorso a un ulteriore responsabile del trattamento ove ciò comporti un trasferimento di dati personali dal primo responsabile del trattamento (in qualità di esportatore) all'ulteriore responsabile del trattamento in questione (in qualità di importatore) sulla base delle informazioni ricevute.

86. In linea con il precedente paragrafo 58, il titolare del trattamento ha la responsabilità ultima di qualsiasi violazione dell'articolo 28, paragrafo 1, del GDPR in caso di ricorso a (sub-)responsabili del trattamento e può esserne ritenuto responsabile. L'EDPB sottolinea che le difficoltà pratiche invocate dai titolari del trattamento per quanto riguarda il controllo sul ricorso a sub-responsabili del trattamento da parte del responsabile del trattamento, che può rendere difficile per i titolari verificare le «garanzie sufficienti», in particolare rispetto ai trasferimenti verso paesi terzi, non esonerano i titolari dalle loro responsabilità nel trattamento ([79]).

87. Di seguito si descrivono esempi non esaustivi della documentazione che il titolare del trattamento dovrebbe valutare ed essere in grado di mostrare all'autorità di controllo competente (mappatura dei trasferimenti, motivo del trasferimento utilizzato e, se del caso, «valutazione dell'impatto dei trasferimenti» e misure supplementari).

Mappatura dei trasferimenti

88. Come primo passo, in caso di trasferimento dei dati personali a paesi terzi in relazione all'utilizzo di (sub-)responsabili del trattamento, il titolare del trattamento dovrebbe valutare ed essere in grado di mostrare la documentazione relativa alla mappatura del trasferimento ([80]). Il titolare del trattamento dovrebbe garantire che la mappatura sia effettuata dall'esportatore (che tratta i dati personali per suo conto), indicando quali dati personali sono trasferiti (compreso l'accesso remoto), dove e per quali finalità ([81]). Il titolare del trattamento può basarsi su tale mappatura e, se necessario, approfondirla. Ad esempio, se la mappatura ricevuta dal titolare del trattamento sembra incompleta ([82]), imprecisa o solleva dubbi, il titolare del trattamento dovrebbe chiedere ulteriori informazioni, verificarle e completarle/correggerle se necessario.

89. Il titolare del trattamento dovrebbe ricevere tali informazioni ([83]) prima che sia coinvolto un ulteriore responsabile del trattamento. Va inoltre ricordato che il titolare del trattamento è soggetto a specifici requisiti di trasparenza per quanto riguarda i trasferimenti verso paesi terzi a norma dell'articolo 13, paragrafo 1, lettera f), dell'articolo 14, paragrafo 1, lettera f), dell'articolo 15, paragrafo 1, lettera c), e dell'articolo 15, paragrafo 2, del GDPR e all'obbligo di conservare i registri delle attività di trattamento di cui all'articolo 30, paragrafo 1, lettere d) ed e), del GDPR. Al fine di soddisfare tali requisiti, il titolare

([78]) Linee guida 07/2020 dell'EDPB, paragrafo 152, nota 69.
([79]) Relazione del CEF sui servizi basati su cloud, pag. 16.
([80]) Per «mappatura» si intende il primo passo («conoscere i propri trasferimenti») delle raccomandazioni 01/2020 dell'EDPB, sezione 2.1 «Primo passo: conoscere i propri trasferimenti». Questo primo passo si applica indipendentemente dal motivo del trasferimento.
([81]) Occorre specificare che le finalità sono determinate dal titolare del trattamento, unitamente ai «mezzi essenziali» del trattamento (cfr. le linee guida 07/2020 dell'EDPB, punto 40).
([82]) Ad esempio, se la mappatura non specifica l'ubicazione dei sub-responsabili del trattamento o non menziona i trasferimenti sotto forma di accesso remoto, anche se avvengono.
([83]) Come chiarito nei paragrafi 54-56.

del trattamento dovrebbe sapere dove si trovano i sub-responsabili del trattamento e dove avvengono i trasferimenti, compreso l'accesso remoto ([84]).

Motivo del trasferimento utilizzato e, ove applicabile, «valutazione dell'impatto del trasferimento» e misure supplementari

90. Il titolare del trattamento dovrebbe valutare ed essere in grado di mostrare la documentazione relativa al motivo del trasferimento ([85]) su cui si basa l'esportatore conformemente all'istruzione del titolare ([86]). Ciò significa che il titolare del trattamento dovrebbe ricevere tali informazioni dai (sub-)responsabili del trattamento/dagli esportatori prima che i trasferimenti abbiano luogo. L'EDPB ha ricordato in tale contesto che il titolare del trattamento è soggetto a specifici requisiti di trasparenza per quanto riguarda «l'esistenza o l'assenza di una decisione di adeguatezza» ai sensi dell'articolo 45 del GDPR o le «garanzie adeguate» previste conformemente all'articolo 46 GDPR [articolo 13, paragrafo 1, lettera f), articolo 14, paragrafo 1, lettera f), e articolo 15, paragrafo 2, del GDPR ([87])].

91. La portata dell'obbligo del titolare del trattamento di valutare tale documentazione dipende dal tipo di motivo utilizzato per il trasferimento iniziale o successivo da parte dei (sub-)responsabili del trattamento (in qualità di esportatori di dati) ([88]).

92. I trasferimenti possono essere effettuati sulla base di una **decisione di adeguatezza** se, ai sensi dell'articolo 45 del GDPR, la Commissione ha deciso che un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Per valutare se il livello di protezione è adeguato, la Commissione prende in considerazione, tra gli altri criteri, le norme per il trasferimento successivo di dati personali a un altro paese terzo o a un'organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza, nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento ([89]).

93. In tale contesto, per un trasferimento effettuato da un (sub-)responsabile del trattamento (per conto del titolare del trattamento) sulla base di una decisione di adeguatezza ai sensi dell'articolo 45 del GDPR, la verifica che il titolare del trattamento deve eseguire ai sensi dell'articolo 28, paragrafo 1, del

([84]) Tale mappatura è necessaria anche quando le parti compilano gli allegati pertinenti delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea e delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea (cfr. la precedente nota 80).
([85]) Raccomandazioni 01/2020 dell'EDPB, sezione 2.2. «Secondo passo: individuare gli strumenti di trasferimento su cui fate affidamento».
([86]) Articolo 28, paragrafo 3, lettera a), del GDPR.
([87]) Linee guida 01/2022 dell'EDPB (diritto di accesso), paragrafo 122.
([88]) Conformemente all'istruzione documentata del titolare del trattamento per quanto riguarda i trasferimenti di dati personali lungo la catena di trattamento.
([89]) Cfr. l'articolo 45 del GDPR e il documento sui criteri di riferimento per l'adeguatezza del gruppo di lavoro articolo 29, adottato il 28 novembre 2017, WP 254, approvato dall'EDPB il 25 maggio 2018, pagina 7: «*[u]lteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo. Spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento*».

GDPR per accertare che il (sub-)responsabile del trattamento presenti garanzie sufficienti ai fini della conformità al capo V del GDPR dovrebbe considerare i seguenti elementi:

- se la decisione di adeguatezza sia in vigore ([90]);

- se i trasferimenti effettuati per conto del titolare del trattamento rientrino nell'ambito di applicazione di tale decisione (ad esempio, categorie di dati personali o settori rientranti nell'ambito di applicazione) ([91]).

94. Anche qualora i dati personali trasferiti da un (sub-)responsabile del trattamento (per conto del titolare del trattamento) sulla base di una decisione di adeguatezza siano oggetto di un **trasferimento successivo** da tale paese terzo, il livello di protezione delle persone fisiche garantito dal GDPR per tale trasferimento successivo non dovrebbe essere pregiudicato ([92]). A tale proposito, ai sensi dell'articolo 45, paragrafo 2, lettera a), del GDPR, la decisione di adeguatezza emessa dalla Commissione europea riguarda, tra l'altro, le norme dei paesi terzi per il trasferimento successivo. Pertanto, ai sensi dell'articolo 44 del GDPR, il titolare del trattamento non deve controllare tali requisiti autonomamente.

95. Ai fini dell'obbligo del titolare del trattamento di cui all'articolo 28, paragrafo 1, del GDPR, ciò significa che il titolare del trattamento dovrebbe garantire che il (sub-)responsabile del trattamento fornisca «garanzie sufficienti» anche in relazione ai trasferimenti successivi effettuati da un (sub-)responsabile del trattamento da un paese adeguato.

96. In assenza di una decisione di adeguatezza, i trasferimenti possono essere subordinati alla fornitura di «**garanzie adeguate**» in conformità dell'**articolo 46 del GDPR**. In tal caso, il titolare del trattamento dovrebbe valutare le garanzie adeguate messe in atto ed essere attento a qualsiasi legislazione problematica suscettibile di impedire al sub-responsabile del trattamento di rispettare gli obblighi stabiliti nel suo contratto con il primo responsabile del trattamento ([93]). Più specificamente, il titolare del trattamento dovrebbe garantire che tale «valutazione d'impatto del trasferimento» ([94]) sia effettuata, in linea con la giurisprudenza ([95]) e come chiarito nelle raccomandazioni 01/2020 dell'EDPB. La documentazione relativa alle garanzie adeguate messe in atto, alla «valutazione d'impatto del trasferimento» e alle possibili misure supplementari dovrebbe essere prodotta dal responsabile del

([90]) Raccomandazioni 01/2020 dell'EDPB, paragrafo 19: «*[s]e trasferite dati personali verso paesi terzi, regioni o settori cui si riferisce una decisione di adeguatezza della Commissione (nella misura in cui sia applicabile), non dovete adottare ulteriori misure come descritto nelle presenti raccomandazioni. Tuttavia, dovete comunque controllare se le decisioni di adeguatezza pertinenti per detti trasferimenti sono revocate o invalidate*».

([91]) Raccomandazioni 01/2020 dell'EDPB, paragrafo 19.

([92]) Cfr. l'articolo 44 del GDPR: «*[qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale,] compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo*».

([93]) A questo proposito, cfr. la sentenza Schrems II della Corte di giustizia, punti 132 e 133, in cui la Corte sottolinea la natura contrattuale delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea.

([94]) Tale valutazione è spiegata più in dettaglio nelle raccomandazioni 01/2020 dell'EDPB, terzo passo, «valutare se lo strumento di trasferimento di cui all'articolo 46 del GDPR su cui si fa affidamento è efficace alla luce di tutte le circostanze del trasferimento».

([95]) Sentenza Schrems II della Corte di giustizia, punto 134.

trattamento/dall'esportatore ([96]) [se del caso in collaborazione con il responsabile del trattamento/l'importatore ([97])]. Il titolare del trattamento può basarsi sulla valutazione preparata dal (sub-)responsabile del trattamento e, se necessario, approfondirla. Ad esempio, qualora la valutazione ricevuta dal titolare del trattamento sembri incompleta, imprecisa o sollevi dubbi, il titolare del trattamento dovrebbe chiedere informazioni aggiuntive, verificarle e completarle/correggerle se necessario, tenendo presente che la valutazione dovrebbe essere in linea con le raccomandazioni 01/2020 dell'EDPB e i passi ivi indicati ([98]). Ciò include l'individuazione di leggi e prassi pertinenti alla luce di tutte le circostanze del trasferimento ([99]) e l'individuazione di misure supplementari appropriate, se necessario ([100]). A tale riguardo, il titolare del trattamento dovrebbe considerare in particolare se l'esportatore di dati, ossia il responsabile o il sub-responsabile del trattamento, abbia valutato se vi siano elementi nel diritto e/o nelle prassi vigenti nel paese terzo che possano incidere sull'efficacia delle garanzie adeguate del motivo del trasferimento su cui l'esportatore fa affidamento ([101]), soprattutto a causa della legislazione e delle prassi che disciplinano l'accesso ai dati personali trasferiti da parte delle autorità pubbliche del paese terzo ([102]).

97. Inoltre, come nel caso dei trasferimenti basati su una decisione di adeguatezza (articolo 45 del GDPR, cfr. i precedenti paragrafi 94 e 95), qualora i dati personali siano trasferiti da un (sub-)responsabile del trattamento sulla base di garanzie adeguate ai sensi dell'articolo 46 del GDPR, il titolare del trattamento, ai sensi dell'articolo 28, paragrafo 1, del GDPR, è anche tenuto ad assicurarsi che il (sub-)responsabile del trattamento presenti garanzie sufficienti per quanto riguarda i **trasferimenti successivi**. Le garanzie adeguate ai sensi dell'articolo 46 del GDPR includono di solito disposizioni atte a stabilire le norme che disciplineranno qualsiasi trasferimento successivo ([103]). Ciò significa che i

([96]) Raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del RGPD), adottate il 20 giugno 2023, versione 2.1, paragrafo 10: «[...] *è ad esempio responsabilità di ciascun esportatore di dati valutare caso per caso, per ciascun trasferimento, se sia necessario attuare misure supplementari al fine di fornire un livello di protezione sostanzialmente equivalente a quello previsto dal RGPD*».

([97]) Nella sentenza Schrems II, punto 134, la Corte di giustizia ha osservato che tale esercizio di verifica può essere effettuato in collaborazione con l'importatore, se del caso. Cfr. anche le raccomandazioni 01/2020 dell'EDPB, sezione 4.

([98]) Cfr. in particolare «Terzo passo: valutare se lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento è efficace alla luce di tutte le circostanze del trasferimento», «Quarto passo: adozione di misure supplementari» e «Sesto passo: rivalutare a intervalli appropriati», come chiarito nelle raccomandazioni 01/2020 dell'EDPB.

([99]) Sentenza Schrems II della Corte di giustizia, punto 126. Cfr. anche le raccomandazioni 01/2020 dell'EDPB, sezione 2.3., «Terzo passo: valutare se lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento è efficace alla luce di tutte le circostanze del trasferimento» e, in particolare, il paragrafo 33. Nella sentenza Schrems II, paragrafo 134, la Corte di giustizia ha osservato che tale esercizio di verifica può essere effettuato in collaborazione con l'importatore, se del caso (cfr. anche le raccomandazioni 01/2020 dell'EDPB, paragrafo 30).

([100]) Sulla base della giurisprudenza incombe, anzitutto, al titolare del trattamento o al responsabile del trattamento verificare, caso per caso, e, eventualmente, in collaborazione con il destinatario dei dati, se il diritto del paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole (sentenza Schrems II della Corte di giustizia, punto 134). Cfr. anche le raccomandazioni 01/2020 dell'EDPB, sezione 2.4, «Quarto passo: adozione di misure supplementari».

([101]) Cfr. le raccomandazioni 01/2020 dell'EDPB, sezione 2.3 («terzo passo»).

([102]) Cfr. le raccomandazioni 01/2020 dell'EDPB, paragrafo 41 e seguenti.

([103]) Cfr. ad esempio, le clausola 8.7 (modulo uno) e, rispettivamente, 8.8 (modulo due e modulo tre) delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea [decisione di esecuzione (UE) 2021/914 della Commissione] del 4 giugno 2021.

titolari del trattamento non devono verificare se tali norme in sé siano in linea con i requisiti di cui al capo V del GDPR. Tuttavia, i titolari del trattamento dovrebbero essere in grado di presentare la documentazione relativa a tali trasferimenti successivi. Ciò significa che il titolare del trattamento dovrebbe ricevere queste informazioni dai (sub-)responsabili del trattamento / dagli esportatori, così da poter dimostrare che gli importatori rispettano effettivamente i requisiti per i trasferimenti successivi stabiliti nello strumento delle garanzie adeguate.

2.3 Interpretazione dell'articolo 28, paragrafo 3, lettera a), del GDPR (domanda 2)

98. Per garantire una ripartizione trasparente delle responsabilità generali sia internamente (tra titolari del trattamento e responsabili del trattamento) sia esternamente nei confronti degli interessati e delle autorità di regolamentazione, ai sensi dell'articolo 28, paragrafo 3, del GDPR, i trattamenti di dati personali da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri ([104]) tra il titolare del trattamento e il responsabile del trattamento. In conformità dell'articolo 28, paragrafo 3, del GDPR, il contratto prevede, in particolare, che il responsabile del trattamento «*tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*». Inoltre tale disposizione sancisce che «*in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico*».

99. La richiesta riguarda l'esistenza di contratti che prevedono l'impegno a trattare dati personali solo su istruzione del titolare del trattamento «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» (omettendo il riferimento al diritto dell'Unione o degli Stati membri). A tale riguardo, sono state sottoposte all'EDPB diverse domande, trattate insieme nella sezione seguente:

> 2 Un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri ai sensi dell'articolo 28, paragrafo 3, del GDPR deve contenere l'eccezione di cui all'articolo 28, paragrafo 3, lettera a), «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» (alla lettera o in termini molto simili) per essere conforme al GDPR?
>
> 2a In caso di risposta negativa alla domanda 2, se un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri amplia l'eccezione di cui all'articolo 28, paragrafo 3, lettera a), del GDPR per includere anche il diritto di un paese terzo (ad esempio, «salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico»), ciò costituisce di per sé una violazione dell'articolo 28, paragrafo 3, lettera a), del GDPR?

100. Le linee guida 07/2020 dell'EDPB richiamano «*l'importanza di negoziare e di redigere con attenzione gli accordi di trattamento dei dati*» in relazione a qualsiasi requisito del diritto dell'Unione o dello Stato membro a cui l'incaricato del trattamento è soggetto ([105]). In merito ai contenuti, le linee guida 07/2020 dell'EDPB rilevano che un contratto «*tra il titolare e il responsabile del trattamento deve rispettare i requisiti di cui all'articolo 28 del GDPR, al fine di garantire che il responsabile tratti i dati personali in conformità con lo stesso GDPR. Qualsivoglia accordo di questo tipo dovrebbe tenere conto delle responsabilità specifiche dei titolari e dei responsabili del trattamento. Sebbene l'articolo 28*

([104]) In prosieguo il termine «**contratto**» sarà utilizzato nell'accezione di «contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri».
([105]) Linee guida 07/2020 dell'EDPB, paragrafo 121.

preveda un elenco di elementi che devono essere contemplati in ogni contratto che disciplini il rapporto tra titolari e responsabili del trattamento, esso lascia margini di negoziato tra le parti di tali contratti» ([106]). Il margine di negoziazione è limitato dai requisiti di cui all'articolo 28, paragrafo 3, del GDPR.

([106]) Linee guida 07/2020 dell'EDPB, paragrafo 109.

101. In primo luogo, l'impegno del responsabile del trattamento a trattare i dati personali su istruzione documentata del titolare del trattamento è un elemento fondamentale del contratto.

102. Tuttavia, come riconosciuto dall'articolo 28, paragrafo 3, lettera a), del GDPR, i responsabili del trattamento possono legittimamente trattare dati personali, non su istruzione documentata del titolare del trattamento, al fine di adempiere agli obblighi giuridici previsti dal diritto dell'Unione o degli Stati membri (in prosieguo «**obbligo giuridico a norma del diritto UE/SM**»). La stessa disposizione impone anche l'impegno del responsabile del trattamento a informare con anticipo il titolare del trattamento dell'eventuale obbligo giuridico, a norma del diritto UE/SM, di trattare/trasferire dati personali a un paese terzo o a un'organizzazione internazionale, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico. Tale impegno è esplicitamente incluso con una formulazione molto simile a quella dell'articolo 28, paragrafo 3, lettera a), del GDPR nelle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea ([107]) e in altre clausole contrattuali tipo, in particolare quelle adottate dalle autorità di controllo danese ([108]), slovena ([109]) e lituana ([110]) ai fini della conformità con l'articolo 28 del GDPR.

103. Oltre all'obbligo di effettuare il trattamento solo su istruzione documentata del titolare del trattamento, l'articolo 28, paragrafo 3, lettera a), del GDPR contiene quindi tre elementi principali: a) una norma che disciplina le situazioni in cui un requisito giuridico obbliga il responsabile del trattamento a effettuare un trattamento di dati personali non basato sull'istruzione del titolare del

([107]) Cfr. in particolare le clausole 7.1., lettera a), e 7.8, lettera a):
- clausola 7.1., lettera a): «*[i]l responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate*» (enfasi aggiunta). Nel parere congiunto sul progetto di clausole contrattuali tipo della Commissione, l'EDPB e il GEPD hanno raccomandato di includere il testo completo dell'articolo 28, paragrafo 3, lettera a) (aggiungendo così un riferimento al dovere del responsabile del trattamento di informare il titolare del trattamento in merito all'obbligo giuridico) al fine di migliorare la coerenza. Parere congiunto 1/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento per le materie di cui all'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 e all'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725, paragrafo 38. Il testo «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» era già presente nel progetto di clausole contrattuali tipo;
- clausola 7.8., lettera a): «*[q]ualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725*». Per quanto riguarda la clausola 7.8, lettera a), l'EDPB e il GEPD hanno raccomandato l'inclusione di un riferimento alla possibilità per il responsabile del trattamento di effettuare trasferimenti sulla base di un requisito specifico ai sensi del diritto dell'Unione o dello Stato membro cui il responsabile del trattamento è soggetto, che inizialmente non era specificato nel progetto di clausole contrattuali tipo. Allegato 2 del parere congiunto 1/2021 dell'EDPB-EDPS, osservazioni sulla clausola 7.7, lettera a).
([108]) Clausole contrattuali tipo dell'autorità di controllo danese ai fini della conformità con l'articolo 28 del GDPR, in particolare le clausole 4.1 e 8.2. Nel parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), l'EDPB ha raccomandato di includere il testo dell'articolo 28, paragrafo 3, lettera a), al fine di garantire la certezza del diritto.
([109]) Clausole contrattuali tipo dell'autorità di controllo slovena ai fini della conformità con l'articolo 28 del GDPR, in particolare le clausole 3.1 e 7.2.
([110]) Clausole contrattuali tipo dell'autorità di controllo lituana ai fini della conformità con l'articolo 28 del GDPR, in particolare le clausole 4.1, 22 e 23.

trattamento, quindi non per conto del titolare del trattamento, b) la necessità per il responsabile del trattamento di informare il titolare del trattamento ([111]) e c) il riferimento a tale requisito giuridico come derivante dal diritto dell'Unione o degli Stati membri.

104. In questo contesto, l'EDPB ricorda che, come principio generale, i contratti non possono prevalere sul diritto. Ciò significa che l'inclusione della clausola di cui all'articolo 28, paragrafo 3, lettera a), del GDPR («*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*») in un contratto non può impedire l'applicazione di requisiti giuridici in aggiunta ai requisiti contrattuali o, in alcuni casi, in contrasto con essi. Inoltre, conformemente al principio generale secondo cui un contratto non crea obblighi nei confronti di terzi, un contratto non può vincolare, ad esempio, le autorità pubbliche di uno Stato membro o di un paese terzo ([112]).

105. Tutti i contratti tra un titolare del trattamento e un responsabile del trattamento devono considerare i casi in cui il responsabile del trattamento può essere obbligato dalla legislazione a trattare dati personali secondo modalità diverse da quelle indicate dal titolare del trattamento. Inoltre, un altro elemento fondamentale che deve essere incluso nel contratto è l'obbligo del responsabile del trattamento di informare il titolare del trattamento prima di effettuare un trattamento non basato sulla sua istruzione ([113]).

106. Per i dati personali trattati al di fuori del SEE, il riferimento al diritto dell'Unione o degli Stati membri può non essere molto significativo, dato che un responsabile del trattamento al di fuori del SEE sarà soggetto solo in via eccezionale a obblighi giuridici dell'Unione o degli Stati membri. A tale proposito, l'EDPB osserva che le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, che sono destinate a soddisfare, oltre ai requisiti dell'articolo 46, paragrafo 1, e dell'articolo 46, paragrafo 2, lettera d), del GDPR, anche i requisiti dell'articolo 28, paragrafi 3 e 4, del GDPR ([114]), non contengono un testo simile a quello della clausola «salvo che» di cui all'articolo 28, paragrafo 3, lettera a), del GDPR. Tuttavia, l'obbligo di trattare dati personali solo su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri, è già indirettamente trattato dalla clausola 8.1 delle clausole contrattuali tipo per il trasferimento

([111]) L'articolo 28, paragrafo 3, lettera a), del GDPR prevede che, qualora il diritto dell'Unione o dello Stato membro imponga al responsabile del trattamento di trattare dati personali, «*il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico*».

([112]) Per questo motivo le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea contengono diverse garanzie che impongono all'esportatore e all'importatore di valutare i requisiti obbligatori previsti dal diritto di un paese terzo prima di trasferire i dati, per garantire che non vadano oltre quanto necessario in una società democratica [clausola 14, lettere da a) a d)], richiedendo all'importatore di notificare l'esportatore in caso di modifiche e a quest'ultimo di agire di conseguenza [clausola 14, lettere e) ed f)] e imponendo all'importatore obblighi in caso di accesso da parte di autorità pubbliche (clausola 15). Cfr. la sentenza Schrems II della Corte di giustizia, punti 125 e 141.

([113]) Nel parere 18/2021 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo lituana (articolo 28, paragrafo 8, del GDPR), l'EDPB ha raccomandato di includere l'ultimo elemento dell'articolo 28, paragrafo 3, lettera a), nelle clausole contrattuali tipo (ossia l'obbligo per il responsabile del trattamento di informare il titolare del trattamento in merito alla disposizione giuridica applicabile), parere 18/2021 dell'EDPB, paragrafo 19.

([114]) Cfr. il considerando 9 delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea: «*[q]ualora il trattamento comporti trasferimenti di dati da titolari del trattamento soggetti al regolamento (UE) 2016/679 a responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, o da responsabili del trattamento soggetti al regolamento (UE) 2016/679 a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, le clausole contrattuali tipo figuranti nell'allegato della presente decisione dovrebbero consentire di soddisfare anche i requisiti di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679*».

internazionale della Commissione europea ([115]). Inoltre, ciò non significa che l'obbligo di informazione di cui all'articolo 28, paragrafo 3, lettera a), del GDPR non sia trattato, considerando che le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea prevedono esplicitamente la necessità che l'importatore di dati informi l'esportatore di dati qualora non sia in grado di eseguire l'istruzione del titolare del trattamento ([116]). Di conseguenza, l'obbligo del responsabile del trattamento di informare il titolare del trattamento qualora si applichi un obbligo giuridico di trattamento (sia esso risultante dal diritto dell'UE o di uno Stato membro o dal diritto di un paese terzo) deriva dalle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea senza l'utilizzo della formulazione esatta «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» di cui all'articolo 28, paragrafo 3, lettera a), del GDPR [elemento c) di cui sopra].

107. Ciò è in linea con l'obiettivo dell'articolo 28, paragrafo 3, lettera a), del GDPR di garantire che il titolare del trattamento sia informato nel caso in cui il responsabile del trattamento sia tenuto per legge a trattare dati personali secondo modalità diverse da quelle indicate dal titolare del trattamento.

108. Alla luce dell'analisi di cui sopra, l'EDPB ritiene che l'inclusione, in un contratto tra il titolare del trattamento e il responsabile del trattamento ([117]), dell'eccezione di cui all'articolo 28, paragrafo 3, lettera a), GDPR, «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*» (alla lettera o in termini molto simili) sia vivamente raccomandata, ma non strettamente necessaria ai fini del rispetto dell'articolo 28, paragrafo 3, lettera a), del GDPR. Tale parere non pregiudica la necessità di un obbligo contrattuale di informare il titolare del trattamento nel caso in cui il responsabile del trattamento sia tenuto per legge a trattare dati personali secondo

([115]) La clausola 8 sulle garanzie di protezione dei dati (modulo due: trasferimento da titolare del trattamento a responsabile del trattamento) afferma alla sezione 8.1 - Istruzioni:
«*a) L'importatore tratta i dati personali soltanto su istruzione documentata dell'esportatore. L'esportatore può impartire tali istruzioni per tutta la durata del contratto.*
b) L'importatore informa immediatamente l'esportatore qualora non sia in grado di seguire tali istruzioni».
Analogamente, al modulo tre (trasferimento da responsabile del trattamento a responsabile del trattamento), la clausola 8 sulle garanzie in materia di protezione dei dati recita alla sezione 8.1 - Istruzioni:
«*a) L'esportatore informa l'importatore del fatto che agisce in qualità di responsabile del trattamento seguendo le istruzioni del o dei titolari del trattamento, che mette a disposizione dell'importatore prima del trattamento.*
b) L'importatore tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, quale comunicatagli dall'esportatore, e su qualunque istruzione documentata aggiuntiva dell'esportatore. Tali istruzioni aggiuntive non devono essere in contrasto con le istruzioni del titolare del trattamento. Il titolare del trattamento o l'esportatore può impartire ulteriori istruzioni documentate in merito al trattamento dei dati per tutta la durata del contratto.
c) L'importatore informa immediatamente l'esportatore qualora non sia in grado di seguire tali istruzioni. Qualora l'importatore non sia in grado di seguire le istruzioni del titolare del trattamento, l'esportatore ne dà immediatamente notifica al titolare del trattamento».

([116]) Oltre alla clausola 8.1 (cfr. la nota precedente), la clausola 14 afferma alla sezione 14.e: «*L'importatore accetta di informare prontamente l'esportatore se, dopo aver accettato le presenti clausole e per la durata del contratto, ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla lettera a), anche a seguito di una modifica della legislazione del paese terzo o di una misura (ad esempio una richiesta di comunicazione) che indichi un'applicazione pratica di tale legislazione che non è conforme ai requisiti di cui alla lettera a). [Per il modulo 3: L'esportatore trasmette la notifica al titolare del trattamento.]»*

([117]) In particolare, se il titolare del trattamento e il responsabile del trattamento fanno affidamento sul proprio contratto di trattamento, anziché sulle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento della Commissione europea, sulle clausole contrattuali tipo adottate dalle autorità di controllo ai fini della conformità all'articolo 28 del GDPR o sulle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea. Cfr. anche il considerando 109 e l'articolo 28, paragrafo 6, del regolamento (UE) 2016/679.

modalità diverse da quelle indicate dal titolare del trattamento, come previsto dall'articolo 28, paragrafo 3, lettera a), del GDPR. Se è chiaro che i requisiti giuridici dell'UE o degli Stati membri sono pertinenti per il trattamento, l'utilizzo del testo di cui all'articolo 28, paragrafo 3, lettera a), del GDPR contribuirebbe a dimostrare la conformità.

109. L'EDPB passa ora a valutare se un contratto che includa un'eccezione più ampia riguardante anche il diritto di un paese terzo, ad esempio un'eccezione all'obbligo di trattare i dati personali solo su istruzione documentata del titolare del trattamento «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*», costituisca di per sé una violazione dell'articolo 28, paragrafo 3, lettera a), del GDPR.

110. Tale formulazione, se non accompagnata da ulteriori specificazioni, può comprendere due situazioni distinte, che dovrebbero essere analizzate separatamente alla luce del contesto giuridico:

- il requisito giuridico previsto o l'ordine vincolante deriva dal diritto dell'Unione o degli Stati membri (SEE);
- il requisito giuridico previsto o l'ordine vincolante deriva da leggi diverse da quelle dell'Unione o degli Stati membri (SEE).

111. La prima situazione rientra nelle disposizioni esplicite di cui all'articolo 28, paragrafo 3, lettera a), del GDPR, che stabiliscono l'obbligo contrattuale del responsabile del trattamento di eseguire il trattamento soltanto su istruzione documentata del titolare del trattamento «*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*», a prescindere dal fatto che il trattamento di dati personali avvenga all'interno o all'esterno del SEE.

112. Il diritto dell'UE, compreso il GDPR, e le disposizioni giuridiche degli Stati membri fanno parte della stessa tradizione costituzionale del GDPR, che sancisce la protezione delle persone fisiche in relazione al trattamento dei dati personali come diritto fondamentale, ai sensi dell'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («**TFUE**») e dell'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («**Carta**») ([118]).

113. Qualora le parti possano dimostrare, sulla base di altri elementi del contratto / dei contratti, che soltanto questa prima situazione è contemplata dal testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*», allora tale testo non ha un impatto sulle garanzie di cui all'articolo 28, paragrafo 3, lettera a), del GDPR.

114. In taluni casi (seconda situazione) il contratto / i contratti delle parti andranno oltre questa prima situazione e la formulazione «*il diritto o un ordine vincolante di un organismo pubblico*» comprenderà pertanto requisiti giuridici/ordini vincolanti derivanti da leggi diverse da quelle dell'Unione o degli Stati membri (SEE).

115. L'EDPB osserva che i requisiti per il trattamento dei dati sulla base di leggi diverse da quelle dell'Unione o degli Stati membri (SEE) non condividono di per sé la tradizione costituzionale e non possono essere automaticamente considerati allo stesso modo di quelli previsti dall'ordinamento giuridico dell'UE (alla luce dell'articolo 44 del GDPR). A tale proposito, l'EDPB ricorda che, ai sensi dell'articolo 6 del GDPR, i termini «obbligo giuridico», «interesse pubblico» e «autorità ufficiale» si riferiscono al diritto dell'Unione o degli Stati membri ([119]). Analogamente, l'EDPB osserva che l'articolo 29 del GDPR sul trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento prevede quanto segue: «*[i]l responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*» (enfasi aggiunta).

116. Nel contesto dei trasferimenti, è prevedibile che vi siano requisiti giuridici derivanti anche da leggi diverse dal diritto dell'Unione o degli Stati membri. Quando si verificano trasferimenti, l'EDPB ricorda

([118]) Il considerando 1 del GDPR richiama l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») e l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta»). Ai sensi dell'articolo 52, paragrafo 1, della Carta «*[e]ventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*».

([119]) Ai sensi dell'articolo 6, paragrafo 3, del GDPR, se la base giuridica su cui si fonda il trattamento è un «obbligo legale» [articolo 6, paragrafo 1, lettera c), del GDPR] o «un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» [articolo 6, paragrafo 1, lettera e), del GDPR], ciò si riferisce alle disposizioni del diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. In riferimento all'articolo 6 del GDPR, il considerando 40 del GDPR spiega che quando la base giuridica del trattamento è prevista per legge, ciò significa «*dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente regolamento*». L'articolo 49, paragrafo 4, del GDPR stabilisce che solo l'interesse pubblico riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento può comportare l'applicazione di tale deroga.

che il capo V del GDPR si applica in aggiunta all'articolo 28 del GDPR. L'EDPB ritiene che, per quanto riguarda i dati personali trattati al di fuori del SEE, l'articolo 28, paragrafo 3, lettera a), del GDPR non impedisca, in linea di principio, l'inclusione nel contratto di disposizioni relative ai requisiti di legge dei paesi terzi per il trattamento dei dati personali trasferiti. Tali disposizioni possono essere incluse in particolare per assicurare la conformità al capo V del GDPR. Tuttavia, è molto improbabile che la semplice inclusione del testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo governativo*» sia sufficiente.

117. In tale contesto, l'EDPB osserva che le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea considerano specificamente le «Leggi e prassi locali che incidono sul rispetto delle clausole» alla clausola 14 e gli «Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche» alla clausola 15. Prima di firmare le clausole contrattuali tipo, le parti devono valutare se esistono leggi e prassi locali importanti per il rispetto delle clausole (clausola 14 delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea). La clausola 14 impone alle parti di garantire di non essere a conoscenza di leggi e prassi del paese terzo in cui ha sede l'importatore che gli impediscano di rispettare gli obblighi che gli incombono a norma delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, a seguito di una valutazione, da parte dell'importatore, di tali leggi e prassi. Inoltre, impone all'importatore di informare prontamente l'esportatore di qualsiasi modifica, nel qual caso l'esportatore individua le misure adeguate per far fronte alla situazione o, come previsto dalla clausola 14, può sospendere il trasferimento e persino di risolvere il contratto. La clausola 15 impone alcuni obblighi all'importatore di dati in caso di accesso da parte di autorità pubbliche di paesi terzi. Stabilisce una serie di misure che l'importatore di dati deve adottare quando si trova di fronte all'accesso da parte di autorità pubbliche di paesi terzi (su richiesta o direttamente), con l'obiettivo di assicurare (in ultima analisi) che il titolare del trattamento sia informato. Oltre all'obbligo di informare l'esportatore di dati, l'importatore ha, tra l'altro, l'obbligo di riesaminare la legittimità della richiesta di accesso e di documentare tale valutazione giuridica, nonché l'obbligo di contestare la richiesta in determinati casi. L'esportatore dei dati (in consultazione con il titolare del trattamento, qualora l'esportatore dei dati non sia il titolare del trattamento) sarà quindi in grado di adottare le misure necessarie, tra cui l'eventuale sospensione del trasferimento o la risoluzione delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea. La conformità al GDPR di qualsiasi trasferimento (successivo) alle autorità pubbliche di paesi terzi dipenderà da un'analisi caso per caso (tra l'altro dalla base giuridica, dalla titolarità del controllo e dalla conformità al capo V del GDPR). Ai sensi del modulo 3 delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea (da responsabile del trattamento a responsabile del trattamento), l'importatore/responsabile del trattamento ha l'obbligo di mettere la valutazione giuridica a disposizione dell'esportatore. A questo proposito, l'EDPB richiama anche i precedenti paragrafi 88-89 e 106.

118. Inoltre, ai sensi delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, sia l'esportatore che l'importatore sono tenuti ad accertare che il diritto del paese terzo di destinazione consenta all'importatore di rispettare le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea prima di trasferire dati personali a tale paese terzo ([120]). Se il responsabile del trattamento esporta dati personali per conto del titolare del trattamento, tale obbligo incombe anche al titolare del trattamento (cfr. anche il precedente paragrafo 79 e seguenti).

119. Analogamente, anche le raccomandazioni relative alle norme vincolanti d'impresa per i titolari del trattamento (BCR-C) e i criteri di riferimento per le norme vincolanti d'impresa per i responsabili del

([120]) Sentenza *Schrems II* della Corte di giustizia, punto 141. Cfr. anche le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea, clausola 14, lettere da a) a d).

trattamento (BCR-P) stabiliscono una serie di obblighi nel caso in cui un membro delle BCR sia soggetto a un conflitto tra la legislazione locale e le BCR ([121]) e/o riceva una richiesta di divulgazione da parte di un'autorità incaricata dell'applicazione della legge o di un servizio di sicurezza pubblico ([122]). Più specificamente, le raccomandazioni 1/2022 dell'EDPB ([123]) indicano che le norme vincolanti d'impresa per i titolari del trattamento (BCR-C) dovrebbero contenere clausole relative alle leggi e alle prassi locali che possono incidere sul rispetto delle BCR-C (sezione 5.4.1), nonché agli obblighi dell'importatore di dati in caso di richieste di accesso da parte delle amministrazioni pubbliche (sezione 5.4.2). Le BCR-C possono fungere da meccanismo di trasferimento per i trasferimenti ai responsabili del trattamento all'interno del gruppo.

120. Nei casi in cui i trasferimenti sono soggetti a decisioni di adeguatezza, la legislazione riguardante «*accesso delle autorità pubbliche ai dati personali, così come l'attuazione di tale legislazione*» è uno degli elementi di cui la Commissione europea deve tenere conto nel valutare l'adeguatezza del livello di protezione, ai sensi dell'articolo 45, paragrafo 2, lettera a), del GDPR ([124]).

121. Ciò che accomuna le decisioni sull'adeguatezza ([125]), le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea ([126]) e le raccomandazioni e i criteri di riferimento per le norme vincolanti d'impresa ([127]) è il presupposto che la legislazione e le prassi di un paese terzo che

([121]) Sezione 5.4.1 «Legislazione e prassi locali che incidono sul rispetto delle BCR-C», raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del RGPD). Sezione 6.3 «La necessità di trasparenza nei casi in cui la legislazione nazionale impedisce al gruppo di rispettare le BCR» del documento di lavoro del gruppo di lavoro articolo 29 che istituisce una tabella contenente gli elementi e i principi per le norme vincolanti d'impresa per i responsabili del trattamento, WP 257 rev. 01, approvato dall'EDPB il 25 maggio 2018.

([122]) Sezione 5.4.2 «Obblighi dell'importatore di dati in caso di richieste di accesso da parte delle amministrazioni pubbliche», raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del RGPD); cfr. anche sezione 6.3 «La necessità di trasparenza nei casi in cui la legislazione nazionale impedisce al gruppo di rispettare le BCR» del documento di lavoro del gruppo di lavoro articolo 29 che istituisce una tabella contenente gli elementi e i principi per le norme vincolanti d'impresa per i responsabili del trattamento, WP 257 rev. 01.

([123]) Raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del RGPD).

([124]) La Corte di giustizia ha considerato questo elemento nelle sentenze Schrems I e Schrems II. Sentenza della Corte di giustizia del 6 ottobre 2015 *Maximillian Schrems/Data Protection Commissioner* (in prosieguo «sentenza Schrems I della Corte di giustizia»), causa C-362/14, ECLI:EU:C:2015:650, paragrafo 91 e seguenti. Sentenza Schrems II della CGUE, paragrafi 141, 174-177, 187-189.

([125]) Cfr. l'articolo 45, paragrafo 2, lettera a), GDPR, ai sensi del quale la Commissione prende in considerazione «*lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento*». Cfr. anche i Criteri di riferimento per l'adeguatezza del gruppo di lavoro articolo 29 WP 254 rev.01, adottati il 6 febbraio 2018, approvati dall'EDPB il 25 maggio 2018. Il concetto di «livello di protezione adeguato» è stato ulteriormente sviluppato dalla Corte di giustizia nelle sentenze Schrems I (paragrafi 73 e 74) e Schrems II (paragrafo 94).

([126]) Clausola 14, lettera a), delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea.

([127]) Ciò è esplicito nelle raccomandazioni 1/2022 dell'EDPB (raccomandazioni BCR-C), versione 2.1, sezioni 5.4.1 e 5.4.2. La stessa interpretazione è implicitamente alla base della sezione 6.3 «La necessità di trasparenza nei

rispettano l'essenza dei diritti e delle libertà fondamentali sanciti dal TFUE, dalla Carta e dal GDPR e che non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi elencati all'articolo 23, paragrafo 1, del GDPR, non comprometteranno il livello di protezione garantito dal GDPR ([128]). Per questo motivo, le clausole contrattuali tipo per il trasferimento internazionale della Commissione europea ([129]) e le raccomandazioni e i criteri di riferimento per le norme vincolanti d'impresa ([130]) prevedono disposizioni che attribuiscono conseguenze diverse alla legislazione e alle prassi a seconda che pregiudichino o meno il livello di protezione garantito dal GDPR. Anche i contratti ad hoc basati sull'articolo 46, paragrafo 3, lettera a), del GDPR dovrebbero contenere disposizioni analoghe ([131]).

122. Da quanto precede emerge chiaramente che, quando la legislazione del paese terzo impone al responsabile del trattamento di trattare i dati personali secondo modalità diverse da quelle indicate dal titolare del trattamento, il livello di protezione sancito dal GDPR sarà rispettato solo se tale legislazione soddisfa le succitate condizioni. In ogni caso, il responsabile del trattamento dovrebbe attuare misure supplementari nel caso in cui dette condizioni non siano soddisfatte e il contratto dovrebbe garantire il rispetto di tali.

123. Anche quando tratta dati personali all'interno del SEE, il responsabile del trattamento può comunque dover tener conto della legislazione di un paese terzo in talune circostanze. L'EDPB evidenzia che l'aggiunta nel contratto di un riferimento alla legislazione di un paese terzo non esonera il responsabile del trattamento dagli obblighi previsti dal GDPR.

124. Alla luce dell'analisi di cui sopra, l'EDPB ritiene che l'inclusione di un testo simile a «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» sia una prerogativa della libertà contrattuale delle parti e non violi di per sé l'articolo 28, paragrafo 3, lettera a), del GDPR. Ciò non pregiudica l'obbligo di rispettare il GDPR ogniqualvolta siano trattati dati personali. Inoltre, tale clausola non esonera il titolare del trattamento e il responsabile del trattamento dall'adempimento dei loro obblighi ai sensi del GDPR, in particolare per quanto riguarda le informazioni da fornire al titolare del trattamento e, se del caso, le condizioni per i trasferimenti internazionali dei dati personali trattati per conto del titolare del trattamento ([132]).

---

casi in cui la legislazione nazionale impedisce al gruppo di rispettare le BCR» del documento di lavoro del gruppo di lavoro «Articolo 29» del documento di lavoro del gruppo di lavoro articolo 29 che istituisce una tabella contenente gli elementi e i principi per le norme vincolanti d'impresa per i responsabili del trattamento, WP 257 rev.01, approvato dall'EDPB il 25 maggio 2018.

([128]) Raccomandazioni 01/2020 dell'EDPB relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, versione 2.0, paragrafo 38, e raccomandazioni 02/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza, paragrafi 22 e 24.

([129]) Clausola 14 delle clausole contrattuali tipo per il trasferimento internazionale della Commissione europea.

([130]) Cfr. nota 127.

([131]) Raccomandazioni 01/2020 dell'EDPB relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, versione 2.0, paragrafo 66.

([132]) In particolare, l'obbligo del titolare del trattamento di garantire che, per quanto riguarda il trattamento al di fuori del SEE, solo la legislazione di un paese terzo che assicura un livello di protezione sostanzialmente equivalente richieda il trattamento da parte del responsabile del trattamento. Cfr. anche i precedenti paragrafi 116-122.

125. Infine, la richiesta contiene una domanda integrativa:

> In caso di risposta negativa alla domanda 2a, tale eccezione estesa dovrebbe invece essere interpretata come un'istruzione documentata del titolare del trattamento ai sensi dell'articolo 28, paragrafo 3, lettera a), del GDPR?

126. Alla luce della risposta sopra formulata, l'EDPB ritiene che la questione rimanente sia se le parti possano sostenere che il testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» (alla lettera o in termini molto simili) all'interno del contratto sia da interpretare come istruzione documentata da parte del titolare del trattamento ai sensi dell'articolo 28, paragrafo 3, lettera a), del GDPR.

127. L'EDPB considera innanzitutto se tale argomento sia sostenibile qualora l'obbligo legale o l'ordine vincolante derivi dal diritto dell'Unione o degli Stati membri (SEE).

128. L'EDPB osserva che il concetto di «istruzione» di cui all'articolo 28, paragrafo 3, lettera a), del GDPR si riferisce specificamente alla definizione da parte del titolare del trattamento del tipo di trattamento che il responsabile del trattamento deve effettuare per suo conto e delle relative modalità ([133]). Qualsiasi disposizione che il titolare del trattamento includa nel contratto con il fornitore di servizi / il responsabile del trattamento che non consista in una richiesta di effettuare un trattamento dei dati personali per conto del titolare del trattamento non è un'istruzione ai sensi dell'articolo 28, paragrafo 3, lettera a), del GDPR. Inoltre, l'istruzione del titolare del trattamento dovrebbe essere sufficientemente precisa per contemplare un trattamento specifico di dati personali, cosa che non avviene con il testo in questione Il titolare del trattamento sarebbe (dovrebbe essere) sempre altresì in grado (e legalmente obbligato nella misura in cui un'istruzione di trattare dati personali per suo conto violi il GDPR) di ritirare tale istruzione. Il responsabile del trattamento dovrebbe quindi conformarsi al ritiro dell'istruzione da parte del titolare del trattamento e interrompere il trattamento.

129. Dando istruzioni al responsabile del trattamento, il titolare del trattamento mette in pratica la sua determinazione delle finalità e dei mezzi del trattamento dei dati, in particolare esercitando un'influenza sugli elementi chiave del trattamento ([134]). In linea di principio, l'influenza del titolare del trattamento sul trattamento dei dati personali cessa laddove il diritto dell'UE o degli Stati membri imponga al responsabile del trattamento di effettuare un trattamento di dati personali che il titolare del trattamento non è in grado di controllare o interrompere ([135]). Sebbene il titolare del trattamento possa ricordare al responsabile del trattamento di rispettare il diritto dell'UE o degli Stati membri, ciò non può essere inteso come un'istruzione ai sensi dell'articolo 28, paragrafo 3, lettera a), del GDPR ([136]). Lo stesso GDPR riconosce questo stato di cose, specificamente precisando che il responsabile del trattamento deve trattare dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento [articolo 28, paragrafo 3, lettera a), del GDPR], e deve informare

([133]) Linee guida 07/2020 dell'EDPB, paragrafo 116.
([134]) Linee guida 07/2020 dell'EDPB, paragrafo 20.
([135]) A tale riguardo, la situazione potrebbe allora essere quella prevista dall'articolo 4, paragrafo 7, del GDPR, ai sensi del quale, quando le finalità e i mezzi del trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri Cfr. la sentenza della Corte di giustizia dell'11 gennaio 2024, *Stato belga (Données traitées par un journal officiel)*, causa C-231/22, ECLI:EU:C:2024:7, punti 28-30, 35 e 39; linee guida 07/2020 dell'EDPB, paragrafi 22-24.
([136]) Piuttosto, tale richiamo sarà considerato come una messa in atto da parte del titolare del trattamento di garanzie contrattuali per assicurare che il trattamento per suo conto sia conforme a tutti i requisiti del GDPR e garantisca la protezione dei diritti dell'interessato.

immediatamente il titolare del trattamento qualora un'istruzione violi il GDPR (articolo 28, paragrafo 3, ultimo comma, del GDPR).

130. L'EDPB ritiene che il suddetto ragionamento si applichi anche qualora l'obbligo legale o l'ordine vincolante derivi dal diritto di un paese terzo. In tale situazione, il diritto in questione limita l'influenza che il titolare del trattamento può esercitare sul trattamento dei dati.

131. In aggiunta a quanto precede, una clausola in base alla quale un responsabile del trattamento si impegna a trattare i dati personali solo su istruzione documentata del titolare del trattamento «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» indica di per sé che il trattamento su istruzione del titolare del trattamento è la regola, mentre l'eccezione esiste precisamente per il trattamento non su istruzione del titolare del trattamento (come dimostra l'espressione «salvo che»). Inoltre, spetta sempre al responsabile del trattamento decidere se ottemperare all'obbligo legale o all'ordine vincolante a cui è soggetto o se affrontare le conseguenze legali di una mancata ottemperanza.

132. Su tale base, l'EDPB conclude che il testo «*salvo che lo richieda il diritto o un ordine vincolante di un organismo pubblico*» (alla lettera o in termini molto simili) non può essere interpretato come istruzione documentata del titolare del trattamento. Il titolare del trattamento rimane responsabile qualora non abbia assicurato che i dati personali fossero trattati dal (sub-)responsabile del trattamento soltanto su sua istruzione documentata. Tuttavia, ciò non è applicabile se il trattamento è imposto dal diritto dell'UE o degli Stati membri, o per il trattamento al di fuori del SEE, dalla legislazione di un paese terzo a cui il (sub-)responsabile del trattamento è soggetto e tale legislazione assicura livello di protezione sostanzialmente equivalente.

Per il comitato europeo per la protezione dei dati

Presidente

(Anu Talus)