# Parere 14/2026 sull'approvazione dei criteri di certificazione Europrivacy da parte del comitato come sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, GDPR

Adottato il 15 aprile 2026

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

# Indice

**Il comitato europeo per la protezione dei dati**

visti l'articolo 63, l'articolo 64, paragrafo 2, e l'articolo 42 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 appresso "GDPR"),

visto l'accordo sullo Spazio economico europeo (in appresso "SEE"), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione n. 154/2018 del Comitato misto SEE, del 6 luglio 2018[1],

visti gli articoli 10 e 22 del proprio regolamento interno,

considerando quanto segue:

1. Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati (in appresso "EDPB" o "comitato") e la Commissione europea incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati (in appresso "meccanismi di certificazione") nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento, tenendo in considerazione le esigenze specifiche delle micro, piccole e medie imprese. Inoltre l'istituzione di meccanismi di certificazione può migliorare la trasparenza e consentire agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi.
2. I criteri di certificazione sono parte integrante di un meccanismo di certificazione. Il GDPR richiede pertanto che i criteri di un meccanismo nazionale di certificazione debbano essere approvati dall'autorità di controllo competente (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b), GDPR) o, nel caso di un sigillo europeo per la protezione dei dati, dall'EDPB (articolo 42, paragrafo 5, e articolo 70, paragrafo 1, lettera o), GDPR).
3. Quando intende proporre l'approvazione di un sigillo europeo per la protezione dei dati da parte dell'EDPB a norma dell'articolo 42, paragrafo 5, GDPR, un'autorità di controllo (in appresso "AC") dovrebbe indicare l'intenzione del titolare del programma di certificazione di rendere disponibile il relativo meccanismo in tutti gli Stati membri. In questo caso, il ruolo principale dell'EDPB è garantire l'applicazione coerente del GDPR attraverso il meccanismo di coerenza di cui agli articoli da 63 a 65, GDPR. In tale contesto, conformemente all'articolo 64, paragrafo 2, GDPR, l'EDPB approva i criteri di certificazione.
4. Il presente parere mira a garantire l'applicazione coerente del GDPR anche da parte delle autorità di controllo, dei titolari del trattamento e dei responsabili del trattamento, alla luce degli elementi fondamentali che i meccanismi di certificazione sono tenuti a stabilire. In particolare, la valutazione dell'EDPB è effettuata sulla base delle "Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679" (in appresso le "linee guida") e del relativo addendum "Guida - Addendum, Valutazione dei criteri di certificazione" (in appresso "addendum"), per le quali il periodo di consultazione pubblica è scaduto il 26 maggio 2021.
5. Di conseguenza l'EDPB riconosce che ciascun meccanismo di certificazione dovrebbe essere esaminato individualmente, senza pregiudicare la valutazione di qualsiasi altro meccanismo di certificazione.
6. I meccanismi di certificazione dovrebbero consentire ai titolari del trattamento e ai responsabili del trattamento di dimostrare la conformità al GDPR. I criteri di tali meccanismi dovrebbero

[1] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".

pertanto rispecchiare adeguatamente i requisiti e i principi relativi alla protezione dei dati personali stabiliti nel GDPR e contribuire alla loro applicazione coerente.

7. Al contempo, il titolare del meccanismo di certificazione dovrebbe garantire l'allineamento e la conformità del meccanismo stesso alle norme ISO e alle pratiche di certificazione che il meccanismo incorpora o sulle quali si basa.
8. Di conseguenza le certificazioni dovrebbero apportare un valore aggiunto ai titolari e ai responsabili del trattamento, contribuendo all'attuazione di misure organizzative e tecniche standardizzate e specifiche che facilitino e migliorino in modo dimostrabile la conformità delle operazioni di trattamento al GDPR, tenendo conto dei requisiti settoriali specifici.
9. L'EDPB accoglie con favore gli sforzi compiuti dai titolari dei meccanismi di certificazione per elaborare tali meccanismi, che sono strumenti pratici e potenzialmente efficaci sotto il profilo dei costi per garantire una maggiore coerenza con il GDPR e promuovere il diritto alla vita privata e alla protezione dei dati degli interessati, aumentando la trasparenza.
10. L'EDPB ricorda che le certificazioni sono strumenti di responsabilizzazione volontari e che l'adesione a un meccanismo di certificazione non riduce la responsabilità dei titolari o dei responsabili del trattamento per quanto riguarda la conformità al GDPR, né impedisce alle autorità di controllo di esercitare le proprie funzioni e poteri ai sensi del GDPR e delle pertinenti leggi nazionali.
11. Nel presente parere l'EDPB affronta questioni quali l'ambito di applicazione, l'applicabilità e la pertinenza dei criteri in tutti gli Stati membri.
12. Il presente parere dell'EDPB si concentra esclusivamente sui criteri di certificazione. L'EDPB può richiedere informazioni di alto livello sui metodi di valutazione allo scopo di poter definire in modo approfondito la verificabilità dei criteri nel contesto del suo parere. Tuttavia ciò non comporta alcun tipo di approvazione di tali metodi di valutazione.
13. Il parere dell'EDPB è adottato ai sensi dell'articolo 64, paragrafo 2, GDPR, in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno del comitato, entro otto settimane a partire dal primo giorno lavorativo successivo alla data in cui la presidente e l'autorità di controllo competente hanno deciso che il fascicolo è completo. Su decisione della presidente, tale termine può essere prorogato di ulteriori sei settimane, a seconda della complessità della questione. Se nel proprio parere l'EDPB conclude che i criteri in questione non possono essere approvati, l'AC può presentarli nuovamente per approvazione una volta affrontate le problematiche segnalate nel parere iniziale,

**ha adottato il seguente parere:**

# 1 Sintesi dei fatti

14. Conformemente all'articolo 42, paragrafo 5, GDPR e alle linee guida, il Centro europeo per la certificazione e la privacy (*European Center for Certification and Privacy*, in appresso "titolare dello schema") ha elaborato i criteri di certificazione Europrivacy (versione 82) (in appresso "criteri di certificazione").
15. Il 29 gennaio 2026 l'autorità di controllo del Lussemburgo (in appresso "AC LU") ha presentato i criteri di certificazione Europrivacy (versione 82) all'EDPB per approvazione a norma dell'articolo 64, paragrafo 2, GDPR.

16. La decisione concernente la completezza del fascicolo è stata assunta il 31 marzo 2026.

17. L'EDPB ricorda di aver approvato i criteri di certificazione Europrivacy (versione 60) il 10 ottobre 2022 con l'emissione del parere 28/2022 sull'approvazione dei criteri di certificazione Europrivacy da parte del comitato come sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, del regolamento generale sulla protezione dei dati (RGPD) ("precedente parere dell'EDPB").

18. Il presente parere riguarda la versione modificata dei criteri di certificazione Europrivacy (versione 82). In primo luogo, il comitato osserva che in questa versione dei criteri di certificazione, attualmente sottoposta all'EDPB, l'ambito di applicazione è stato esteso ai richiedenti ai quali si applica l'articolo 3, paragrafo 2, GDPR e, a tale riguardo, è stato introdotto un criterio sul potenziale conflitto con la legislazione di un paese terzo. Inoltre il comitato osserva che alcuni dei criteri di certificazione approvati dall'EDPB nel 2022 sono stati adeguati, perfezionati e/o chiariti nella versione modificata dei criteri di certificazione Europrivacy (versione 82). Tali modifiche riguardano, in particolare: la designazione di un rappresentante nel SEE e la cooperazione nell'ambito delle richieste formulate dalle autorità di protezione dei dati competenti nel SEE; la relazione di valutazione della conformità agli obblighi nazionali ("NOCAR"), l'ulteriore trattamento, le garanzie che accompagnano il trattamento delle categorie particolari di dati personali, i diritti degli interessati, il coinvolgimento di sub-responsabili del trattamento, la gestione delle violazioni dei dati, la valutazione dei rischi per il trattamento dei dati, nonché la politica e i requisiti di sicurezza.

19. L'EDPB sottolinea che la modifica dei criteri di certificazione già approvata nel 2022 avrà effetto sulle certificazioni già rilasciate e sui processi di certificazione in corso. Pertanto è opportuno gestire in modo adeguato e trasparente il periodo di transizione tra i sigilli europei per la protezione dei dati rilasciati sulla base dei criteri di certificazione approvati con il precedente parere dell'EDPB (versione 60) e quelli rilasciati secondo i criteri di certificazione (versione 82), esaminati nel presente parere. A tale riguardo, il comitato comprende, sulla base della documentazione fornita dal titolare dello schema, che tutti i processi di certificazione in corso devono essere completati entro la fine del 2026 e che, a partire da tale data, i criteri di certificazione approvati con il precedente parere dell'EDPB (versione 60) non saranno più utilizzati per il rilascio di nuovi certificati. I certificati rilasciati finora rimarranno validi fino al termine del rispettivo periodo di validità triennale e saranno rinnovati conformemente ai criteri di certificazione (versione 82). Pertanto, dopo la fine del 2029, i criteri di certificazione approvati con il precedente parere dell'EDPB (versione 60) saranno integralmente sostituiti dai criteri di certificazione (versione 82). Inoltre le informazioni relative a tale piano di transizione saranno rese pubbliche dal titolare dello schema. Potrebbero rendersi necessari alcuni adeguamenti nell'accreditamento degli organismi di certificazione, ma il presente parere non affronta tale questione in quanto non rientra nella sfera di competenza dell'EDPB.

20. Il meccanismo di certificazione generale Europrivacy non è destinato a essere utilizzato come strumento per i trasferimenti ai sensi dell'articolo 42, paragrafo 2, e dell'articolo 46, paragrafo 2, lettera f), GDPR. Il 29 gennaio 2026 l'AC LU ha altresì sottoposto all'EDPB, per approvazione ai sensi dell'articolo 64, paragrafo 2, GDPR, un'ulteriore serie di criteri di certificazione ("The Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46"), il cui ambito di applicazione comprende i titolari del trattamento e i responsabili del trattamento ubicati al di fuori del SEE che non sono direttamente soggetti al GDPR ai sensi dell'articolo 3, paragrafo 2, GDPR, ma che trattano dati personali ricevuti da un altro titolare o responsabile del trattamento soggetto al GDPR. In merito alla summenzionata serie di criteri di certificazione destinati a essere utilizzati come strumento per i trasferimenti ai sensi dell'articolo 46, paragrafo 2, lettera f), GDPR, l'EDPB ha adottato il parere 15/2026.

# 2 Valutazione

21. L'EDPB ha condotto la propria valutazione dei criteri di certificazione ai fini della loro approvazione a norma dell'articolo 42, paragrafo 5, GDPR, conformemente alla struttura prevista nell'allegato 2 delle linee guida (in appresso "allegato") e nel relativo addendum.

22. Nel contesto del presente parere e al fine di approvare i criteri di certificazione, l'EDPB ha valutato i criteri seguenti: "Application and Target of Evaluation - Preliminary Checks and Controls" (A); "Europrivacy GDPR Core Criteria" (G); "Technological and Organisational Measures Checks and Controls" (T), forniti unitamente ai criteri di certificazione.

23. Inoltre il comitato osserva a tale riguardo che le "verifiche e i controlli contestuali complementari"[2], forniti unitamente ai criteri di certificazione approvati con il precedente parere dell'EDPB (versione 60), volti a garantire che il trattamento dei dati ricompreso nell'oggetto della valutazione sia conforme ai requisiti specifici settoriali e tecnologici[3], non sono stati approvati dall'EDPB nel precedente parere e che tali "verifiche e controlli contestuali complementari" non sono più presenti nella documentazione aggiornata fornita nel contesto del presente parere.

24. Il comitato osserva, come precisato nelle definizioni dello schema, che i riferimenti alle "autorità di protezione dei dati competenti" all'interno dello schema devono intendersi come autorità di protezione dei dati nel SEE[4].

25. Per quanto riguarda le definizioni di diritto di un paese terzo, il comitato ritiene che queste facciano riferimento alla legge applicabile al richiedente e/o ai dati personali trattati nell'oggetto della valutazione, nella misura in cui tale legge non imponga restrizioni ai diritti in materia di protezione dei dati che vadano oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi elencati all'articolo 23, paragrafo 1, GDPR, sia proporzionata all'obiettivo perseguito, rispetti l'essenza del diritto alla protezione dei dati e preveda misure specifiche a tutela dei diritti e degli interessi fondamentali degli interessati.

## 2.1 Ambito di applicazione del meccanismo di certificazione e oggetto della valutazione

26. L'EDPB ricorda[5] che il meccanismo di certificazione Europrivacy è uno schema generale in quanto riguarda un'ampia gamma di trattamenti diversi effettuati da titolari e responsabili del trattamento in vari settori di attività.

27. Il comitato accoglie con favore il fatto che, nella documentazione relativa all'ambito di applicazione di tale meccanismo di certificazione fornita da AC LU, lo schema Europrivacy modificato si applichi ai: **i)** titolari e responsabili del trattamento stabiliti nell'Unione europea (UE) o nello Spazio economico europeo (SEE); **ii)** titolari e responsabili del trattamento stabiliti al di fuori del SEE che sono soggetti al GDPR ai sensi dell'articolo 3, paragrafo 2, GDPR in quanto offrono beni o servizi a interessati nel SEE oppure monitorano il comportamento degli

[2] L'EDPB non ha approvato le "verifiche e i controlli contestuali complementari" nel suo precedente parere.
[3] Precedente parere dell'EDPB, punti 7 e 8.
[4] Cfr. la definizione prevista dai criteri Europrivacy per l'"autorità di controllo competente": "*"Autorità di protezione dei dati competente" si riferisce alle autorità di protezione dei dati nel SEE. In generale, indica le autorità nazionali di protezione dei dati che hanno competenza a far rispettare la conformità dei dati personali trattati dall'oggetto della valutazione. Nel caso di una certificazione ai sensi del GDPR rilasciata a un importatore di dati a norma dell'articolo 46 GDPR, l'autorità di protezione dei dati competente è quella dell'esportatore di dati nel SEE, fatta eccezione per la presentazione di un reclamo, per la quale è competente qualsiasi autorità nel SEE*".
[5] Precedente parere dell'EDPB, punto 6.

interessati nel SEE[6]. L'applicabilità dei criteri è definita in funzione del ruolo e delle responsabilità del richiedente.

28. Per quanto riguarda i richiedenti ai sensi dell'articolo 3, paragrafo 2, GDPR stabiliti in un paese terzo non soggetti a una decisione di adeguatezza che ricomprenda l'oggetto della valutazione, il criterio A.2.1.6 definisce le condizioni da soddisfare nella definizione di tale oggetto nel corso del riesame della domanda di certificazione. In particolare, prima di prendere in considerazione un audit di certificazione, esso richiede all'organismo di certificazione di verificare che il richiedente sia in grado di dimostrare che il diritto e la prassi nazionali del paese terzo non ostacolano la conformità del richiedente ai requisiti di certificazione. In caso contrario, il processo di certificazione si interromperà nella fase di presentazione della domanda.

29. Il comitato osserva che un titolare del trattamento può sottoporre al processo di certificazione Europrivacy un oggetto della valutazione soggetto a contitolarità del trattamento (criterio A.2.1.5). Nel caso in cui l'oggetto della valutazione sia soggetto a contitolarità del trattamento, il comitato desidera sottolineare che l'organismo di certificazione accreditato dovrà condurre attentamente il processo di certificazione per garantire che l'oggetto della valutazione sia significativo e che il richiedente sia pienamente responsabile della sua conformità a tutti gli obblighi previsti dal GDPR che il meccanismo di certificazione mira a dimostrare. Di conseguenza l'accordo concluso tra il richiedente e gli altri contitolari del trattamento coinvolti nell'oggetto della valutazione per quanto riguarda le rispettive responsabilità per l'osservanza degli obblighi di cui al GDPR potrebbe, a seconda del contesto delle attività di trattamento dell'oggetto della valutazione, impedire al richiedente di soddisfare i criteri di certificazione.

## 2.2 Trattamenti

30. Come osservato dall'EDPB nel suo precedente parere, i criteri di certificazione riguardano le componenti pertinenti dei trattamenti (dati, sistemi e processi) per quanto riguarda l'ambito di applicazione generale dello schema di certificazione. In particolare, i criteri di certificazione consentono di individuare categorie particolari di dati quali definite all'articolo 9 GDPR (sezione G.2 dei criteri "Trattamento di dati speciali").

## 2.3 Liceità del trattamento

31. Come affermato dall'EDPB nel precedente parere sui criteri di certificazione già approvati (versione 60), i criteri richiedono di verificare la liceità di ogni singolo trattamento nell'oggetto della valutazione e di verificare l'osservanza dei requisiti applicabili alla base giuridica ai sensi dell'articolo 6 GDPR (sezione G.1 dei criteri "Ammissibilità del trattamento dei dati"). In particolare, il comitato accoglie con favore il fatto che i criteri di certificazione aggiornati richiedano che il consenso degli interessati copra ciascuna finalità per cui il trattamento è effettuato e che la revoca del consenso non debba comportare alcun pregiudizio per l'interessato.

32. Inoltre, come osservato nel precedente parere dell'EDPB, i criteri di certificazione richiedono di verificare i requisiti specifici delle condizioni alle quali, ai sensi dell'articolo 9, paragrafo 2, GDPR, è consentito il trattamento di categorie particolari di dati personali (sezione G.2.1 dei criteri "Trattamento di dati speciali") e di prevedere limitazioni e garanzie aggiuntive per i diritti e le libertà dell'interessato. I criteri di certificazione richiedono altresì la verifica dei requisiti

[6] Cfr. Linee-guida dell'EDPB sull'ambito di applicazione territoriale del RGPD (articolo 3), versione 2.1, adottate il 12 novembre 2019, sezione 2.

delle condizioni di cui all'articolo 10 GDPR per il trattamento dei dati personali relativi a condanne penali e reati (sezione G.2.2 dei criteri), se del caso. A tale riguardo, il comitato accoglie con favore il fatto che i criteri di certificazione aggiornati (criterio G.2.1.3 sulle garanzie aggiuntive per il trattamento di categorie particolari di dati personali) richiedano altresì che il richiedente disponga di limitazioni e garanzie aggiuntive, adattate alla natura specifica dei dati e ai corrispondenti rischi, qualora il trattamento riguardi categorie particolari di dati personali.

33. Inoltre, per quanto riguarda i richiedenti di cui all'articolo 3, paragrafo 2, GDPR stabiliti in un paese terzo non soggetti a una decisione di adeguatezza che copra l'oggetto della valutazione, i criteri di certificazione aggiornati impongono al richiedente di fornire una relazione redatta da un esperto giuridico che attesti che la legislazione e la prassi nazionali del paese terzo non ostacolino l'adempimento degli obblighi in materia di protezione dei dati previsti dal GDPR. Analogamente, la valutazione deve accertare che la legislazione nazionale del paese terzo non imponga limitazioni ai diritti in materia di protezione dei dati che vadano oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi elencati all'articolo 23, paragrafo 1, GDPR, sia proporzionata all'obiettivo perseguito, rispetti l'essenza del diritto alla protezione dei dati e preveda misure specifiche a tutela dei diritti e degli interessi fondamentali degli interessati. La valutazione deve inoltre essere riesaminata ogniqualvolta modifiche normative o organizzative possano ostacolare il rispetto dei criteri o incidere sull'oggetto della valutazione o sui diritti degli interessati, e l'organismo di certificazione dovrebbe esserne informato (criterio G.1.1.5).

34. In tale contesto, i criteri di certificazione aggiornati chiariscono negli orientamenti che "qualora un richiedente sia stabilito al di fuori del SEE e benefici di una decisione di adeguatezza pertinente per il trattamento effettuato nell'oggetto della valutazione, il rispetto di tale requisito può essere dimostrato mediante una relazione semplificata". Secondo tali criteri, la relazione in questione avrebbe dovuto verificare se la decisione di adeguatezza è in vigore e documentare i motivi per cui l'oggetto della valutazione rientra nell'ambito di applicazione della decisione di adeguatezza (criterio G.1.1.5, lettera F).

## 2.4 Principi del trattamento di dati

35. L'EDPB ricorda che i criteri di certificazione tengono debitamente conto dei principi di protezione dei dati di cui all'articolo 5 GDPR. In particolare, i criteri di certificazione aggiornati ampliano e illustrano ulteriormente il principio di limitazione delle finalità, includendo un criterio specifico che richiede di dimostrare che i dati personali non sono ulteriormente trattati in modo incompatibile con tali finalità, che qualsiasi ulteriore trattamento dovrebbe essere separatamente valutato come lecito e che è condotta e debitamente documentata una valutazione della compatibilità delle finalità per l'ulteriore trattamento dei dati (criterio G.1.1.6).

## 2.5 Obblighi generali dei titolari e dei responsabili del trattamento

36. L'EDPB ricorda che i criteri di certificazione[7] riflettono gli obblighi del titolare del trattamento previsti dall'articolo 24 GDPR (sezione G.4 "Responsabilità del titolare del trattamento") e richiedono la valutazione degli accordi contrattuali conclusi tra il responsabile e il titolare del

[7] Precedente parere dell'EDPB, punto 16.

trattamento conformemente all'articolo 28 GDPR (sezione G.5 dei criteri "Responsabili o sub-responsabili del trattamento").

37. Inoltre il comitato accoglie con favore l'integrazione per cui i criteri di certificazione impongono al richiedente, a norma dell'articolo 3, paragrafo 2, GDPR, di designare un ufficio o un rappresentante nel SEE a norma dell'articolo 27 GDPR, i cui dati di contatto sono disponibili sul sito web del richiedente (criterio G.4.1.4). Il comitato prende atto di tali criteri di certificazione e ricorda che non sempre si tratta di un obbligo imperativo per i titolari del trattamento e per i responsabili del trattamento ai sensi del GDPR; pertanto occorre tenere presenti le condizioni di cui all'articolo 27 GDPR.

38. Inoltre l'EDPB osserva, come dichiarato nel precedente parere, che i criteri di certificazione impongono a tutti i richiedenti di nominare un responsabile della protezione dei dati (RPD) anche nel caso in cui il richiedente non sia tenuto a designarne uno ai sensi dell'articolo 37 GDPR. I criteri verificano che il responsabile della protezione dei dati soddisfi i requisiti di cui agli articoli da 37 a 39 (sezione G.9 dei criteri "Responsabile della protezione dei dati").

39. Analogamente, i criteri di certificazione richiedono di verificare il contenuto dei registri delle attività di trattamento conformemente all'articolo 30 GDPR (sezione G.5.3 dei criteri "Registri delle attività di trattamento"). A tale riguardo, il comitato accoglie con favore il fatto che, per i richiedenti di cui all'articolo 3, paragrafo 2, GDPR, i criteri di certificazione aggiornati richiedano loro di cooperare nell'ambito delle richieste formulate dalle autorità di protezione dei dati competenti nel SEE e di mettere a loro disposizione, su richiesta, il registro delle attività di trattamento (criterio G.5.3.5).

40. Nella stessa ottica, l'EDPB osserva che alcuni criteri di certificazione aggiuntivi sono stati introdotti in relazione al ricorso a sub-responsabili del trattamento per i richiedenti che agiscono in qualità di titolari o di responsabili del trattamento (sezione G.5.1.2 "Ricorso a sub-responsabili del trattamento"). Tale distinzione consente di rispecchiare meglio la separazione dei ruoli e delle responsabilità tra i soggetti della catena del trattamento.

## 2.6 Diritti degli interessati

41. Come indicato nel suo precedente parere, l'EDPB ricorda che i criteri di certificazione tengono adeguatamente conto del diritto all'informazione dell'interessato conformemente al capo III GDPR e richiedono l'attuazione delle apposite misure[8]. I criteri di certificazione richiedono inoltre l'adozione di misure che prevedano la possibilità di intervenire nel trattamento al fine di garantire i diritti degli interessati e consentire rettifiche, cancellazioni o limitazioni (sezione G.3 dei criteri "Diritti degli interessati").

42. Inoltre l'EDPB accoglie con favore i miglioramenti apportati ai criteri di certificazione per quanto riguarda le informazioni da fornire agli interessati (sezione G 3.2 "Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato" e sezione G.3.3 "Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato"), le modalità di comunicazione agli interessati[9] e per l'esercizio dei loro diritti[10] (sezione G 3.1 "Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti degli interessati"),

[8] Precedente parere dell'EDPB, punto 19.

[9] Ad esempio, il criterio G.3.1.1 relativo all'obbligo di informare in un linguaggio chiaro approfondisce ulteriormente le informazioni sul trattamento dei dati fornite dal richiedente all'interessato, che ora includono che i) dovrebbero essere fornite per iscritto o con altri mezzi, ii) dovrebbero essere disponibili nella lingua o nelle lingue ufficiali del richiedente e iii) dovrebbero essere disponibili nella lingua degli interessati cui sono destinate.

[10] Ad esempio, il criterio G.3.1.3 relativo alla garanzia di una corretta gestione e registrazione dei diritti degli interessati prevede ora che il richiedente disponga di una procedura o di un meccanismo atti anche a confermare all'interessato la ricezione della richiesta e a conservare registrazioni anche delle richieste dell'interessato con la data di ricevimento.

nonché il diritto di accesso (sezione G 3.4 "Diritto di accesso dell'interessato"), di cancellazione (sezione G.3.6 "Diritto alla cancellazione ("diritto all'oblio")"), di limitazione del trattamento (criterio G 3.7.1 "Diritto di limitazione del trattamento"), l'obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (criterio G.3.8.2 "Obbligo di informare gli interessati in merito ai destinatari, se richiesto"), il diritto di opposizione (sezione G.3.10 "Diritto di opposizione") e il diritto di non essere sottoposto a un processo decisionale individuale automatizzato, compresa la profilazione (sezione G.3.11 "Diritto di non essere sottoposto a un processo decisionale individuale automatizzato, compresa la profilazione").

## 2.7 Rischi per i diritti e le libertà

43. L'EDPB ha già affermato nel suo precedente parere che i criteri di certificazione richiedono di valutare il rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati rientrante nell'oggetto della valutazione conformemente all'articolo 35 GDPR (sezione G.8 dei criteri "Obbligo di valutare se sia necessaria una valutazione dell'impatto sulla protezione dei dati")[11].

44. L'EDPB accoglie con favore le modifiche apportate ai criteri di certificazione al fine di prevedere che "il richiedente abbia valutato, con una metodologia replicabile, i rischi presentati dal trattamento che possono incidere sui diritti e sulle libertà delle persone fisiche" (sezione G.6.2.4 "Valutazione dei rischi per il trattamento dei dati").

45. Inoltre l'EDPB accoglie con favore le ulteriori integrazioni e i dettagli introdotti dai criteri di certificazione. Ad esempio, l'EDPB prende atto dell'integrazione apportata al processo di valutazione dell'impatto sulla protezione dei dati per quanto riguarda le situazioni in cui il richiedente non è tenuto a effettuare tale valutazione (sezione G.8.2.1 "Requisiti del processo di valutazione dell'impatto sulla protezione dei dati").

## 2.8 Misure tecniche e organizzative a garanzia della protezione

46. Come osservato nel precedente parere dell'EDPB, i criteri di certificazione richiedono l'applicazione di misure tecniche e organizzative che garantiscano la riservatezza, l'integrità e la disponibilità dei trattamenti. I criteri richiedono inoltre l'applicazione di misure tecniche per attuare la protezione dei dati fin dalla progettazione e per impostazione predefinita conformemente agli articoli 25 e 32 GDPR (sezione G.6 dei criteri "Protezione dei dati fin dalla progettazione e per impostazione predefinita, e sicurezza del trattamento", sezione G.6.2 dei criteri "Sicurezza del trattamento" e sezione sui criteri T)[12]. A tale riguardo, il comitato accoglie con favore il fatto che i criteri di certificazione modificati approfondiscano ulteriormente (sezione G.6.1.2 "Minimizzazione dei dati per impostazione predefinita") le norme e le procedure che il richiedente deve applicare al fine di soddisfare tali criteri.

47. Come sottolineato nel precedente parere dell'EDPB, i criteri di certificazione richiedono l'applicazione di misure volte a garantire il corretto e tempestivo assolvimento degli obblighi di notifica di violazioni dei dati personali conformemente agli articoli 33 e 34 GDPR (sezione G.7 dei criteri "Gestione delle violazioni dei dati").

[11] Precedente parere dell'EDPB, punto 20.
[12] Precedente parere dell'EDPB, punto 21.

48. A tale riguardo, il comitato osserva che i criteri di certificazione sono stati ulteriormente migliorati ed elaborati. Più segnatamente, i criteri di certificazione comprendono ora un elenco più dettagliato (sezione G.7.1.1 "Obbligo di documentare le violazioni dei dati") delle informazioni che il richiedente deve documentare in caso di violazione dei dati (ad esempio le categorie di dati personali che sono o possono essere interessate, il numero approssimativo di interessati che sono o possono essere interessati; le categorie e il numero approssimativo di registrazioni di dati personali che riguardano o possono riguardare la violazione, le probabili conseguenze della violazione dei dati personali).

### 2.9 Criteri finalizzati a dimostrare l'esistenza di garanzie adeguate per il trasferimento dei dati personali

49. Come affermato dal comitato nel suo precedente parere, i criteri di certificazione richiedono l'individuazione di tutti i trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali coinvolti nell'oggetto della valutazione, nonché di motivare la scelta operata per quanto riguarda il meccanismo di trasferimento dei dati al fine di offrire garanzie adeguate, conformemente al capo V GDPR (sezione G.10 "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali").

50. L'EDPB riconosce che, per i richiedenti di cui all'articolo 3, paragrafo 2, GDPR, tali criteri di certificazione si applicheranno sia in caso di trasferimento di dati personali previsti nell'oggetto della valutazione verso soggetti stabiliti nello stesso paese terzo in cui si trova il richiedente, sia verso soggetti in un paese terzo diverso.

51. Inoltre il comitato accoglie con favore il fatto che i criteri di certificazione relativi ai trasferimenti di dati personali siano stati ulteriormente elaborati e definiscano più chiaramente gli obblighi del richiedente a tale riguardo (sezione G.10.1 "Obblighi generali per i trasferimenti internazionali di dati personali verso paesi terzi o organizzazioni internazionali").

## 3 Criteri aggiuntivi per il sigillo europeo di protezione dei dati

52. Ai sensi delle linee guida, la valutazione deve esaminare se "i criteri sono in grado di tener conto della legislazione in materia di protezione dei dati o dei relativi scenari di tutti gli Stati membri". Come affermato nel precedente parere dell'EDPB, la sezione G.1.1.3 dei criteri di certificazione impone al richiedente di fornire tale valutazione in una relazione di valutazione della conformità agli obblighi nazionali (NOCAR). Tale relazione deve comprendere una valutazione degli obblighi nazionali applicabili all'oggetto della valutazione e documentare le misure adottate dal richiedente per conformarsi alle norme applicabili ed eventualmente le azioni correttive in corso. Il richiedente non deve utilizzare l'elenco dei principali requisiti nazionali complementari fornito per ciascun paese dal titolare dello schema alla stregua di un elenco esaustivo degli obblighi nazionali pertinenti con riguardo all'oggetto della valutazione. L'elenco indicativo dei requisiti minimi per le verifiche e i controlli complementari fornito dal titolare dello schema non costituisce un criterio di certificazione ricadente nell'ambito del presente parere.

53. Il comitato accoglie con favore gli adeguamenti apportati alla NOCAR nei criteri aggiornati (sezione G.1.1.3 "Valutazione della conformità agli obblighi nazionali"). In particolare, è ora precisato che il richiedente dovrebbe documentare in una relazione di valutazione della conformità agli obblighi nazionali (NOCAR) la valutazione effettuata sulla conformità del trattamento dei dati "*agli obblighi nazionali complementari del SEE relativi alla protezione dei*

*dati personali applicabili al richiedente*". Nello specifico, la NOCAR dovrebbe contenere, tra l'altro, una chiara identificazione dell'oggetto della valutazione sottoposto a valutazione, l'elenco degli obblighi nazionali complementari del SEE individuati in materia di protezione dei dati applicabili all'oggetto della valutazione, nonché la valutazione della conformità dell'oggetto della valutazione agli obblighi nazionali complementari del SEE individuati in materia di protezione dei dati. Il comitato ritiene che, qualora il richiedente sia stabilito al di fuori del SEE e sia soggetto all'articolo 3, paragrafo 2, GDPR, gli obblighi nazionali del SEE in materia di protezione dei dati applicabili all'oggetto della valutazione debbano essere determinati sulla base dell'ubicazione degli interessati ai quali il richiedente offre beni o servizi o il cui comportamento è oggetto di monitoraggio.

# 4 Conclusioni/Raccomandazioni

54. In conclusione, l'EDPB ritiene che i criteri di certificazione Europrivacy siano allineati con il GDPR e li approva conformemente a quanto previsto dall'articolo 70, paragrafo 1, lettera o), GDPR, il che risulta in una certificazione comune (sigillo europeo per la protezione dei dati).

55. L'EDPB ritiene che i criteri di certificazione costituiscano parte integrante del meccanismo di certificazione e inserirà il meccanismo di certificazione Europrivacy nel registro pubblico dei meccanismi di certificazione e dei sigilli e marchi di protezione dei dati; inoltre renderà pubblici i criteri a norma dell'articolo 42, paragrafo 8, GDPR.

# 5 Osservazioni finali

56. L'autorità di controllo del Lussemburgo è destinataria del presente parere, che sarà reso pubblico ai sensi dell'articolo 64, paragrafo 5, lettera b), GDPR.

Per il comitato europeo per la protezione dei dati

La presidente

Anu Talus