Parere del comitato (articolo 64)

Parere 27/2024 sull'approvazione dei criteri di certificazione «Brand Compliance» 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)

Adottato il 2 dicembre 2024

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

INDICE

1 SINTESI DEI FATTI 4
2 VALUTAZIONE 5
3 CRITERI AGGIUNTIVI PER IL SIGILLO EUROPEO DI PROTEZIONE DEI DATI 8
4 CONCLUSIONI / RACCOMANDAZIONI 8
5 OSSERVAZIONI FINALI 8

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 «RGPD»),

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 l'articolo 10 e l'articolo 22 del proprio regolamento interno.

(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 al livello dell'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 RGPD dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento, tenendo in considerazione le esigenze specifiche delle micro, piccole e medie imprese ([2]). 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 ([3]).

(2) I criteri di certificazione sono parte integrante di un meccanismo di certificazione. Il RGPD richiede pertanto che i criteri di un meccanismo di certificazione debbano essere approvati dall'autorità di controllo competente (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b), del RGPD) 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), del RGPD].

(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, del RGPD, 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 RGPD attraverso il meccanismo di coerenza di cui agli articoli da 63 a 65 del RGPD. In tale contesto, conformemente all'articolo 64, paragrafo 2, del RGPD, l'EDPB approva i criteri di certificazione.

(4) Il presente parere mira a garantire l'applicazione coerente del RGPD 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 devono sviluppare. 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» (in appresso le «linee guida») e del relativo addendum «Guida – Addendum, Valutazione dei criteri di certificazione» (in appresso «addendum»).

([1]) Nel presente parere, con il termine «Stati membri» si intendono gli «Stati membri del SEE».
([2]) Articolo 42, paragrafo 1, del RGPD.
([3]) Considerando 100 del RGPD.

(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 RGPD. I criteri di tali meccanismi dovrebbero pertanto rispecchiare adeguatamente i requisiti e i principi relativi alla protezione dei dati personali stabiliti nel RGPD e contribuire alla loro applicazione coerente.

(7) Al tempo stesso, il titolare del programma dovrebbe garantire l'allineamento e la conformità del meccanismo di certificazione alle norme ISO e alle pratiche di certificazione incluse o basate su di esse.

(8) Di conseguenza, le certificazioni dovrebbero apportare un valore aggiunto ai titolari del trattamento 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 RGPD, tenendo conto dei requisiti settoriali specifici.

(9) L'EDPB accoglie con favore gli sforzi compiuti dai titolari dei programmi per elaborare meccanismi di certificazione, che sono strumenti pratici e potenzialmente efficaci sotto il profilo dei costi per garantire una maggiore coerenza con il RGPD e promuovere il diritto alla vita privata e alla protezione dei dati degli interessati, aumentando la trasparenza.

(10) L'EDPB rammenta che le certificazioni sono strumenti di responsabilità volontari e che l'adesione a un meccanismo di certificazione non riduce la responsabilità dei titolari del trattamento o dei responsabili del trattamento per quanto riguarda la conformità al RGPD, né impedisce alle autorità di controllo di esercitare le proprie funzioni e poteri ai sensi del RGPD 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 si concentra sui criteri di certificazione. Nel caso in cui l'EDPB richieda informazioni di alto livello sui metodi di valutazione per poter valutare attentamente la verificabilità dei criteri nel contesto del suo parere, quest'ultimo non comprende alcun tipo di approvazione di tali metodi di valutazione.

(13) Il parere dell'EDPB è adottato ai sensi dell'articolo 64, paragrafo 2, del RGPD 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 ripresentare i criteri per approvazione qualora siano trattate le problematiche espresse nel parere iniziale dell'EDPB.

HA ADOTTATO IL SEGUENTE PARERE:

1 SINTESI DEI FATTI

1. In conformità con l'articolo 42, paragrafo 5, RGPD e le linee guida, il progetto «Norme e criteri di certificazione ai sensi del RGPD, BC 5701:2024, versione 0.7» (in appresso «progetto di criteri di certificazione», «criteri di certificazione» o «criteri») è stato redatto da Brand Compliance B.V., un'entità giuridica nei Paesi Bassi (in appresso «proprietario del sistema»), e sottoposto all'Autoriteit Persoonsgegevens, l'Autorità di controllo competente dei Paesi Bassi (in appresso «AC NL»).

2. L'autorità di controllo della Germania (in appresso «AC DE») ha presentato i criteri di certificazione all'EDPB per l'approvazione a norma dell'articolo 64, paragrafo 2, del RGPD il 26 settembre 2024. La decisione concernente la completezza del fascicolo è stata resa il 12 novembre 2024.

3. Il meccanismo di certificazione «Brand Compliance» non è una certificazione ai sensi dell'articolo 46, paragrafo 2, lettera f), del RGPD intesa per i trasferimenti internazionali di dati personali e pertanto non fornisce garanzie adeguate nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali ai sensi dell'articolo 46, paragrafo 2, lettera f). Infatti, qualsiasi trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale ha luogo solo se sono rispettate le disposizioni del capo V del RGPD.

2 VALUTAZIONE

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

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

5. Il meccanismo di certificazione «Brand Compliance» contiene criteri di certificazione per la certificazione delle operazioni di trattamento effettuate su dati personali da titolari o responsabili del trattamento stabiliti nell'Unione europea (UE) o nello Spazio economico europeo (SEE).

6. I criteri principali di questo meccanismo di certificazione sono suddivisi in sei serie di requisiti, vale a dire: contesto del trattamento dei dati, compresa la conformità alla legislazione dell'UE o degli Stati membri (set 1), Condizioni quadro organizzative (set 2), Fondamenti delle attività di trattamento, compresi i principi relativi al trattamento dei dati personali (set 3), Protezione tecnica e organizzativa (set 4), Esecuzione operativa, compresi i diritti degli interessati (set 5) e Sistema di gestione (set 6).

7. I richiedenti la certificazione nell'ambito di questo sistema devono essere titolari o responsabili del trattamento. Sono compresi i responsabili del trattamento che sono incaricati direttamente del trattamento dei dati personali da parte di un titolare del trattamento ai sensi dell'articolo 4, paragrafo 7, del RGPD, nonché i sub-responsabili del trattamento. Le operazioni di trattamento effettuate (in parte) in qualità di sub-trattamento saranno certificate nella capacità organizzativa di un responsabile del trattamento.

8. Il comitato osserva che il meccanismo di certificazione non può essere utilizzato per certificare le operazioni di trattamento in cui due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi ai sensi dell'articolo 26, paragrafo 1, RGPD (contitolari del trattamento). Il meccanismo di certificazione non può essere utilizzato per certificare le operazioni di trattamento dei dati da un'organizzazione situata al di fuori dell'UE o del SEE. Inoltre, il meccanismo di certificazione non può essere utilizzato come strumento di trasferimento ai sensi dell'articolo 42, paragrafo 2, e dell'articolo 46, paragrafo 2, lettera f), del RGPD.

2.2 Operazioni di trattamento

9. Il meccanismo di certificazione può essere applicato al trattamento dei dati personali indipendentemente dal tipo e dalle dimensioni dell'organizzazione e dalla natura dei prodotti o dei servizi forniti. Pertanto, l'ambito di applicazione del meccanismo di certificazione non è limitato a determinati tipi di operazioni di trattamento e consente la certificazione di qualsiasi operazione di trattamento da parte di un responsabile del trattamento o di un incaricato del trattamento. Pertanto, è di fondamentale importanza che i requisiti metodologici siano rispettati, in quanto questo è l'unico modo per garantire un'applicazione uniforme dei criteri di certificazione e un livello di test comparabile tra le diverse procedure di certificazione. L'obiettivo è garantire la comparabilità e la riproducibilità delle certificazioni rilasciate e dei loro risultati.

2.3 Liceità del trattamento

10. I criteri richiedono di esaminare se le operazioni di trattamento di un responsabile del trattamento sono conformi alle disposizioni dell'articolo 6 (sezione 6.1.2 dei criteri) e, ove applicabile, dell'articolo 9 (sezione 6.1.2.h dei criteri), nonché dell'articolo 10 del RGPD (sezione 6.1.2.i dei criteri). Sebbene il rispetto del principio di liceità del trattamento sia un obbligo del responsabile del trattamento, un incaricato del trattamento deve comunque attenersi a requisiti specifici in questo contesto (sezione 6.2 dei criteri). Tali requisiti mirano in particolare a garantire che l'autorizzazione per il trattamento dei dati sia legittimamente derivata dal titolare del trattamento e che il responsabile del trattamento assista il titolare del trattamento nel conformarsi al RGPD, compreso il principio di liceità.

2.4 Principi del trattamento di dati

11. I criteri stabiliscono requisiti specifici per la valutazione di tutti i principi relativi al trattamento dei dati personali ai sensi dell'articolo 5 del RGPD (sezione 6 dei criteri). Per quanto riguarda i requisiti per i responsabili del trattamento, in questo contesto devono essere valutati criteri separati (sezione 6.2 dei criteri). Come già detto, l'obiettivo principale dei requisiti per gli incaricati del trattamento è quello di supportare il responsabile del trattamento nell'attuazione della conformità ai principi.

2.5 Obblighi generali dei titolari e dei responsabili del trattamento

12. I criteri riflettono sul rapporto tra titolari del trattamento e responsabili del trattamento. In particolare, i criteri stabiliscono l'obbligo per i responsabili del trattamento e gli incaricati del trattamento di rispettare i requisiti relativi all'esternalizzazione delle attività di trattamento, che comprendono, tra l'altro, l'osservanza delle disposizioni di cui all'articolo 28, paragrafo 3, RGPD (sezione 8.5 dei criteri). Per quanto riguarda i responsabili del trattamento, essi devono anche soddisfare i requisiti specifici per il trattamento sotto l'autorità di un titolare del trattamento (sezione 8.6 dei criteri). Inoltre, sono stabiliti ulteriori requisiti per tenere conto delle circostanze del sub-trattamento [sezione 6.2, lettera e), e in particolare sezione 8.6, lettera g), dei criteri].

13. I criteri verificano il contenuto dei registri delle attività di trattamento conformemente all'articolo 30, RGPD (sezione 5.4 dei criteri). In tale contesto, viene operata una distinzione tra il contenuto richiesto di un registro delle attività di trattamento per i titolari del trattamento e i responsabili del trattamento, in linea con l'articolo 30, paragrafi 1 e 2, RGPD.

14. I criteri impongono ai richiedenti di nominare un responsabile della protezione dei dati a norma dell'articolo 37, RGPD. Inoltre, i criteri garantiscono che siano soddisfatti i requisiti di cui agli articoli da 37 a 39 del RGPD (sezione 5.3.2 dei criteri).

15. In relazione al principio di responsabilità ai sensi dell'articolo 5, paragrafo 2, e dell'articolo 24, RGPD, vengono stabiliti i requisiti per l'organizzazione dei meccanismi di protezione dei dati e di segnalazione (sezione 5.1 e 5.3 dei criteri), nonché per l'attuazione delle politiche di protezione dei dati (sezione 5.2 dei criteri).

2.6 Diritti degli interessati

16. I criteri forniscono requisiti adeguati per i diritti degli interessati conformemente al capo III del RGPD. In primo luogo, vengono affrontati i requisiti di trasparenza dell'informazione, della comunicazione e delle modalità di esercizio dei diritti degli interessati, seguiti da un esame dettagliato dei rispettivi diritti degli interessati (sezione 8.4 dei criteri). Per quanto riguarda i requisiti per gli incaricati del trattamento, sono previste disposizioni specifiche per gli obblighi di assistenza (sezione 8.4.11 dei criteri).

2.7 Rischi per i diritti e le libertà

17. I criteri prevedono che il responsabile del trattamento sia consapevole dei possibili rischi per i diritti e le libertà delle persone fisiche per il trattamento dei dati di cui all'oggetto della valutazione. Se il trattamento dei dati personali rischia di comportare un rischio elevato per i diritti e le libertà delle persone fisiche, diversi criteri garantiscono che il richiedente dimostri che i requisiti di cui all'articolo 35, RGPD sono soddisfatti (sezione 7.3 dei criteri). Inoltre, sono previsti requisiti specifici per gli obblighi di assistenza degli incaricati del trattamento ai sensi dell'articolo 35, RGPD.

2.8 Misure tecniche e organizzative a garanzia della protezione

18. I criteri richiedono l'applicazione di misure tecniche e organizzative basate su uno standard di sicurezza delle informazioni che garantisca la riservatezza, l'integrità e l'esattezza dei dati personali trattati e la resilienza del sistema di trattamento. I criteri prevedono inoltre l'applicazione di misure tecniche per attuare la protezione dei dati fin dalla progettazione e per impostazione predefinita conformemente all'articolo 25 e all'articolo 25, RGPD (sezione 7.4 dei criteri). I criteri stabiliscono requisiti specifici per i titolari del trattamento per quanto riguarda la valutazione della notifica di una violazione dei dati personali all'autorità di controllo e, se necessario, la comunicazione di tale violazione all'interessato conformemente agli articoli 33 e 34, RGPD (sezione 8.8 dei criteri). In questo contesto, vengono anche delineati obblighi specifici per gli incaricati del trattamento, in particolare per quanto riguarda l'identificazione di una violazione dei dati personali e la comunicazione con il responsabile del trattamento (sezioni 8.8.1 e 8.8.4 dei criteri).

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

19. I criteri prevedono l'individuazione di tutti i trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali coinvolti nell'oggetto della valutazione e la giustificazione della scelta operata per quanto riguarda il meccanismo di trasferimento dei dati che prevede garanzie adeguate, conformemente al capo V del RGPD (sezione 8.7 dei criteri). I criteri prevedono una procedura di valutazione dei trasferimenti previsti, come il controllo della loro legittimità.

3 CRITERI AGGIUNTIVI PER IL SIGILLO EUROPEO DI PROTEZIONE DEI DATI

20. Ai sensi delle linee guida, la valutazione comprende la questione 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». La sezione 4.3 dei criteri impone al richiedente di rispettare la pertinente normativa nazionale e settoriale applicabile in materia di protezione dei dati. L'organizzazione individua, analizza e documenta in modo corretto e completo le pertinenti disposizioni legislative e regolamentari degli Stati membri o settoriali applicabili al trattamento dei dati personali all'interno dell'oggetto della valutazione. La documentazione deve identificare la persona, o le persone, responsabili della stesura del quadro giuridico nazionale o settoriale rilevante per l'oggetto della valutazione e le loro competenze giuridiche. Inoltre, il comitato è consapevole del fatto che l'adeguatezza dell'individuazione e dell'elaborazione di tale quadro giuridico è determinata dall'organismo di certificazione.

4 CONCLUSIONI / RACCOMANDAZIONI

21. In conclusione, l'EDPB ritiene che i criteri di certificazione «Brand Compliance» siano coerenti con il regolamento generale sulla protezione dei dati e li approva conformemente al compito del Comitato definito all'articolo 70, paragrafo 1, lettera o), RGPD, con conseguente certificazione comune (sigillo europeo per la protezione dei dati).

22. L'EDPB registrerà il meccanismo di certificazione «Norme e criteri di certificazione ai sensi del RGPD, BC 5701:2024, versione 0.7» nel registro pubblico dei meccanismi di certificazione e dei sigilli e marchi per la protezione dei dati ai sensi dell'articolo 42, paragrafo 8.

5 OSSERVAZIONI FINALI

23. L'AC NL è destinataria del presente parere, che sarà reso pubblico ai sensi dell'articolo 64, paragrafo 5, lettera b), RGPD.

Per il Comitato europeo per la protezione dei dati

La presidente
Anu Talus