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)

Adottato il 10 ottobre 2022

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 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 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 (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.

([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 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 RGPD, 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 RGPD 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 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 natura generale sui metodi di valutazione allo scopo di definire la verificabilità dei criteri nel contesto del suo parere, 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, 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 presentarli nuovamente per approvazione una volta affrontate le problematiche segnalate nel parere iniziale.

HA ADOTTATO IL SEGUENTE PARERE:

SINTESI DEI FATTI

1. Conformemente all'articolo 42, paragrafo 5, del RGPD e alle linee guida, i criteri Europrivacy v.60 (in appresso «progetto di criteri di certificazione», «criteri di certificazione» o «criteri») sono stati elaborati dal Centro europeo per la certificazione e la privacy (European Center for Certification and Privacy, in appresso il «titolare dello schema»).

2. L'autorità di controllo del Lussemburgo (in appresso «AC LU») ha presentato i criteri di certificazione Europrivacy all'EDPB per approvazione a norma dell'articolo 64, paragrafo 2, del RGPD il 28 settembre 2022. La decisione concernente la completezza del fascicolo è stata assunta il 28 settembre 2022.

3. Il meccanismo di certificazione Europrivacy non è una certificazione ai sensi dell'articolo 46, paragrafo 2, lettera f), del RGPD intesa per i trasferimenti internazionali di dati personali; pertanto, esso 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.

5. L'EDPB osserva che le indicazioni attuative e i mezzi di verifica proposti dal titolare dello schema per il meccanismo di certificazione non sono uniformemente coerenti con riguardo all'intero catalogo dei criteri. Ad esempio, la sezione T.2.3.2 prevede l'esistenza di norme, politiche, procedure o meccanismi per individuare e segnalare le intrusioni (quali un sistema di rilevamento delle intrusioni che monitora il traffico di rete per rilevare attività sospette e segnala quando una tale attività viene scoperta), mentre i mezzi di verifica proposti menzionano attività di ispezione e test di penetrazione (richiesti nella sezione T.2.3.1). Sebbene tali incoerenze non rientrino nell'ambito della sua valutazione, l'EDPB sottolinea che esse possono costituire un ostacolo all'accreditamento dell'organismo di certificazione, a meno che non siano rettificate dal titolare dello schema.

2.1 Ambito di applicazione del meccanismo di certificazione e oggetto della valutazione (ToE)

6. 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. I principali criteri di questo meccanismo di certificazione sono costituiti da «criteri fondamentali» e da «verifiche e controlli delle misure tecnologiche e organizzative» poste in essere per garantire la sicurezza dei dati personali trattati. Una serie dei criteri relativi a «verifiche e controlli delle misure tecnologiche e organizzative» è applicabile solo se l'oggetto della valutazione (in appresso «ToE») comprende categorie particolari di dati, dati relativi a reati o dati personali di un minore.

7. Inoltre, tra i criteri figurano anche «verifiche e controlli contestuali complementari» volti a garantire che il trattamento dei dati ricompreso nel ToE sia conforme ai requisiti specifici settoriali e tecnologici. Una matrice informativa fornita dal titolare dello schema descrive a quali categorie di trattamenti si applica ciascuna serie di criteri relativi a «verifiche e controlli contestuali complementari».

8. L'EDPB accoglie con favore schemi generali di certificazione che includono criteri specifici in grado di consentirne la scalabilità e l'applicabilità rispetto a specifici trattamenti o settori di attività. Tuttavia, l'EDPB desidera anche chiarire che, nel contesto di uno schema generale, non è richiesta la completezza dei criteri relativi a specifici trattamenti e, pertanto, tale elemento non è stato oggetto

di valutazione nel presente parere. Inoltre, l'EDPB ricorda che il titolare dello schema e gli organismi di certificazione accreditati devono tenere conto dei documenti relativi a specifiche attività di trattamento pubblicati dallo stesso EDPB.

9. I criteri applicabili alla specificazione del ToE sono definiti al punto A.2.1.1. Lo schema Europrivacy specifica le regole applicabili al processo che il richiedente e l'organismo di certificazione devono seguire per definire il ToE (10.2 – Attività preliminari alla certificazione).

10. Nella documentazione relativa all'ambito di applicazione del meccanismo di certificazione fornita dall'AC LU, il Comitato rileva che lo schema Europrivacy si applica ai titolari e ai responsabili del trattamento stabiliti nell'Unione europea (UE) o nello Spazio economico europeo (SEE). L'applicabilità dei criteri è definita in funzione del ruolo e delle responsabilità del richiedente.

11. Il Comitato osserva che un titolare del trattamento può sottoporre al processo di certificazione Europrivacy un ToE soggetto a contitolarità del trattamento (criteri A.2.7.1). Nel caso in cui il ToE 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 il ToE sia significativo e che il richiedente sia pienamente responsabile della sua conformità a tutti gli obblighi previsti dal RGPD che il meccanismo di certificazione mira a dimostrare. Di conseguenza, l'accordo concluso tra il richiedente e gli altri contitolari del trattamento coinvolti nel ToE per quanto riguarda le rispettive responsabilità per l'osservanza degli obblighi di cui al RGPD ([4]) potrebbe – a seconda del contesto delle attività di trattamento del ToE – impedire al richiedente di soddisfare i criteri di certificazione.

12. Il Comitato osserva che il trattamento di dati genetici è escluso dall'ambito di applicazione del meccanismo di certificazione Europrivacy. Di conseguenza, la valutazione dei criteri effettuata dal Comitato non riguarda l'idoneità dei criteri riferiti a un ToE che includa tale trattamento di dati.

2.2 Trattamenti

13. Per quanto riguarda l'ambito di applicazione generale del meccanismo di certificazione, i criteri riguardano le componenti pertinenti dei trattamenti (dati, sistemi e processi). In particolare, i criteri consentono di individuare categorie particolari di dati quali definite all'articolo 9 del RGPD (sezione G.2 dei criteri – Trattamento di dati speciali).

2.3 Liceità del trattamento

14. I criteri richiedono di verificare la liceità di ogni singolo trattamento nel ToE e di verificare l'osservanza dei requisiti applicabili alla base giuridica ai sensi dell'articolo 6 del RGPD (sezione G.1 dei criteri – Ammissibilità del trattamento dei dati).

2.4 Principi del trattamento di dati

15. I criteri tengono debitamente conto dei principi di protezione dei dati di cui all'articolo 5 del RGPD. In particolare, i criteri impongono al richiedente di dimostrare che i dati personali sono adeguati,

([4]) *La determinazione delle rispettive responsabilità deve riguardare in particolare l'esercizio dei diritti degli interessati e gli obblighi di informazione. Inoltre, la ripartizione delle responsabilità dovrebbe riguardare altri obblighi in capo al titolare del trattamento, quali i principi generali in materia di protezione dei dati, la base giuridica, le misure di sicurezza, l'obbligo di notifica di violazione dei dati, le valutazioni d'impatto sulla protezione dei dati, il ricorso a responsabili del trattamento, i trasferimenti verso paesi terzi e i contatti con gli interessati e le autorità di controllo* (Linee guida 7/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR).

pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati).

2.5 Obblighi generali dei titolari e dei responsabili del trattamento

16. I criteri riflettono gli obblighi del titolare del trattamento previsti dall'articolo 24 del RGPD (G.4 – Responsabilità del titolare del trattamento) e richiedono la valutazione degli accordi contrattuali tra il responsabile e il titolare del trattamento conformemente all'articolo 28 del RGPD (sezione G.5 dei criteri – Responsabili o sub-responsabili del trattamento).

17. I criteri 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 del RGPD. 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).

18. I criteri verificano il contenuto dei registri delle attività di trattamento conformemente all'articolo 30 del RGPD (sezione G.5.3 dei criteri – Registri delle attività di trattamento).

2.6 Diritti degli interessati

19. I criteri tengono adeguatamente conto del diritto all'informazione dell'interessato conformemente al capo III del RGPD e richiedono l'attuazione delle apposite misure. I criteri 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).

2.7 Rischi per i diritti e le libertà

20. I criteri richiedono di valutare il rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati oggetto del ToE conformemente all'articolo 35 del RGPD (sezione G.8 dei criteri – Valutazione dell'impatto sulla protezione dei dati).

2.8 Misure tecniche e organizzative a garanzia della protezione

21. I criteri 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 all'articolo 25 e all'articolo 32 del RGPD (sezione G.6 dei criteri – Sicurezza del trattamento e protezione dei dati fin dalla progettazione e sezione T.1/T.2 dei criteri – Requisiti fondamentali di sicurezza/requisiti di sicurezza ampliati).

22. I criteri richiedono l'applicazione di misure volte a garantire il corretto e tempestivo assolvimento degli obblighi di notifica di violazioni dei dati personali conformemente all'articolo 33 e all'articolo 34 del RGPD (sezione G.7 dei criteri – Gestione delle violazioni dei dati).

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

23. I criteri richiedono l'individuazione di tutti i trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali coinvolti nel ToE nonché di motivare la scelta operata per quanto riguarda il meccanismo di trasferimento dei dati prescelto al fine di offrire garanzie adeguate,

conformemente al capo V del RGPD (sezione G.10 dei criteri – Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali).

3. CRITERI AGGIUNTIVI PER IL SIGILLO EUROPEO DI PROTEZIONE DEI DATI

24. 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». La sezione G.1.1.3 dei criteri impone al richiedente di fornire tale valutazione in una relazione di valutazione della conformità agli obblighi nazionali (NOCAR). Il Comitato osserva che tale relazione deve comprendere una valutazione degli obblighi nazionali applicabili al ToE 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 al ToE. 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.

CONCLUSIONI / RACCOMANDAZIONI

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

26. L'EDPB inserirà il meccanismo di certificazione Europrivacy nel registro pubblico dei meccanismi di certificazione e dei sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 8.

OSSERVAZIONI FINALI

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

Per il Comitato europeo per la protezione dei dati

La presidente