Parere 16/2020 sul progetto di decisione dell'autorità di controllo competente della Repubblica ceca relativo all'approvazione dei requisiti per l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3 (RGPD)

Adottato il 25 maggio 2020

Adottato

Indice

Il comitato europeo per la protezione dei dati

visti l'articolo 63, l'articolo 64, paragrafo 1, lettera c), e paragrafi da 3 a 8, e l'articolo 43, paragrafo 3, 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 il «RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, 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 del 25 maggio 2018,

considerando quanto segue:

(1) Il ruolo principale del comitato è garantire l'applicazione coerente del regolamento (UE) 2016/679 (in appresso il «RGPD») in tutto lo Spazio economico europeo. In conformità dell'articolo 64, paragrafo 1, del RGPD, il comitato emette un parere ove un'autorità di controllo intenda approvare i requisiti per l'accreditamento di organismi di certificazione ai sensi dell'articolo 43. Il presente parere è quindi finalizzato a stabilire un approccio armonizzato per quanto riguarda i requisiti che saranno utilizzati da un'autorità di controllo in materia di protezione dei dati o dall'organismo nazionale di accreditamento ai fini dell'accreditamento di un organismo di certificazione. Il RGPD non impone un'unica serie di requisiti per l'accreditamento, ma promuove la coerenza. Il comitato, nei suoi pareri, si prefigge di realizzare tale obiettivo, incoraggiando innanzitutto le autorità di controllo a definire i propri requisiti per l'accreditamento seguendo la struttura di cui all'allegato delle linee guida del comitato europeo per la protezione dei dati relative all'accreditamento degli organismi di certificazione e, in secondo luogo, analizzandoli mediante un modello fornito dal comitato che consente l'analisi comparativa dei requisiti (sulla base della norma ISO 17065 e delle linee guida del comitato relative all'accreditamento degli organismi di certificazione).

(2) Ai sensi dell'articolo 43 del RGPD, le autorità di controllo competenti adottano requisiti per l'accreditamento. Esse applicano, tuttavia, il meccanismo di coerenza per creare fiducia nel meccanismo di certificazione stesso, in particolare fissando un elevato livello di requisiti.

(3) Sebbene i requisiti per l'accreditamento siano sottoposti al meccanismo di coerenza, ciò non significa che debbano essere identici. Le autorità di controllo competenti godono di un margine di discrezionalità relativamente al contesto nazionale o regionale e dovrebbero tenere conto della legislazione locale di riferimento. Il parere del comitato non si prefigge di definire un'unica serie di requisiti a livello di UE, quanto piuttosto di evitare significative incongruenze che possano, ad esempio, intaccare la fiducia nell'indipendenza o nelle competenze degli organismi di certificazione accreditati.

(4) Le «Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati [regolamento (UE) 2016/679]» (in appresso le «linee guida») e le «Linee guida 1/2018 relative alla certificazione e all'identificazione di

([1]) Nel presente parere, i riferimenti all'«Unione» sono da intendersi come riferimenti al «SEE».

criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679» serviranno da filo conduttore nel contesto del meccanismo di coerenza.

(5) Se uno Stato membro stabilisce che gli organismi di certificazione debbano essere accreditati dall'autorità di controllo, quest'ultima dovrebbe stabilire i requisiti per l'accreditamento, compresi, tra gli altri, i requisiti di cui all'articolo 43, paragrafo 2, del RGPD. Rispetto agli obblighi relativi all'accreditamento degli organismi di certificazione da parte degli organismi nazionali di accreditamento, l'articolo 43 del RGPD fornisce minori dettagli in materia di requisiti per l'accreditamento nel caso in cui sia l'autorità di controllo stessa a eseguire l'accreditamento. Al fine di contribuire a un approccio armonizzato all'accreditamento, i requisiti per l'accreditamento utilizzati dall'autorità di controllo dovrebbero basarsi sulla norma ISO/IEC 17065 ed essere integrati dai requisiti aggiuntivi stabiliti da un'autorità di controllo ai sensi dell'articolo 43, paragrafo 1, lettera b). Il comitato osserva che l'articolo 43, paragrafo 2, lettere da a) a e), del RGPD rispecchia e precisa i requisiti di cui alla norma ISO 17065, contribuendo così alla coerenza ([2]).

(6) Il parere del comitato è adottato ai sensi dell'articolo 64, paragrafo 1, lettera c), e paragrafi 3 e 8, 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, tenendo conto della complessità della questione.

HA ADOTTATO IL PRESENTE PARERE:

1 SINTESI DEI FATTI

1. L'autorità di controllo ceca ha presentato al comitato europeo per la protezione dei dati il progetto di requisiti per l'accreditamento ai sensi dell'articolo 43, paragrafo 1, lettera b). Il fascicolo è stato ritenuto completo in data 17 febbraio 2020. L'organismo nazionale di accreditamento ceco, NAB, accrediterà gli organismi di certificazione preposti a certificare applicando i criteri di certificazione del RGPD. Ciò significa che, ai fini dell'accreditamento degli organismi di certificazione, l'organismo nazionale di accreditamento della Repubblica ceca applicherà la norma ISO 17065 nonché i requisiti aggiuntivi stabiliti dall'autorità di controllo ceca, dopo che questa li avrà approvati, a seguito del parere del comitato sul progetto di tali requisiti.
2. Ai sensi dell'articolo 10, paragrafo 2, del regolamento interno del comitato, data la complessità della questione la presidente ha deciso di prorogare di ulteriori sei settimane il periodo di adozione iniziale di otto settimane.

2 VALUTAZIONE

([2]) Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati, punto 39. Disponibili all'indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_it

2.1 Analisi generale del comitato europeo per la protezione dei dati in merito al progetto di decisione

3. Il presente parere intende valutare i requisiti per l'accreditamento definiti da un'autorità di controllo, in relazione alla norma ISO 17065 o a una serie completa di requisiti, per consentire a un organismo nazionale di accreditamento o a un'autorità di controllo di accreditare, ai sensi dell'articolo 43, paragrafo 1, del RGPD, un organismo di certificazione competente per il rilascio e il rinnovo della certificazione in conformità dell'articolo 42 del RGPD. Ciò lascia impregiudicati i compiti e i poteri dell'autorità di controllo competente. Nel caso specifico, il comitato osserva che l'autorità di controllo ceca ha deciso di affidarsi al proprio organismo nazionale di accreditamento per il rilascio dell'accreditamento, avendo elaborato, in conformità delle linee guida, requisiti aggiuntivi che tale organismo dovrebbe applicare al momento del rilascio dell'accreditamento.

4. La presente valutazione dei requisiti aggiuntivi per l'accreditamento dell'autorità di controllo ceca è intesa ad analizzare gli scostamenti (aggiunte o soppressioni) rispetto alle linee guida e, in particolare, al loro allegato 1. Il parere del comitato è inoltre incentrato su tutti gli aspetti che possono influire su un approccio coerente in tema di accreditamento degli organismi di certificazione.

5. Va osservato che le linee guida relative all'accreditamento degli organismi di certificazione intendono aiutare le autorità di controllo a definire i propri requisiti per l'accreditamento. L'allegato delle linee guida di per sé non stabilisce requisiti per l'accreditamento. I requisiti per l'accreditamento degli organismi di certificazione devono pertanto essere definiti dall'autorità di controllo, in modo tale da consentire la loro applicazione pratica e coerente in funzione delle necessità del contesto in cui opera l'autorità di controllo.

6. Il comitato riconosce che, viste le loro competenze, sia opportuno lasciare libertà di manovra agli organismi nazionali di accreditamento nel definire talune disposizioni specifiche nell'ambito dei requisiti applicabili per l'accreditamento. Il comitato ritiene tuttavia necessario evidenziare che, qualora siano stabiliti requisiti aggiuntivi, essi dovrebbero essere definiti in modo tale da consentirne il riesame e l'applicazione secondo principi di praticità e coerenza, ove necessario.

7. Il comitato osserva che le norme ISO, in particolare la norma ISO 17065, sono soggette a diritti di proprietà intellettuale; pertanto, nel presente parere non si farà menzione del testo del relativo documento. Il comitato ha quindi deciso di fare riferimento a specifiche sezioni della norma ISO, se necessario, senza tuttavia riprodurre il testo.

8. Il comitato ha effettuato la propria valutazione conformemente alla struttura prevista nell'allegato 1 delle linee guida (in appresso «allegato»). Qualora il presente parere non si pronunci su una determinata sezione del progetto di requisiti per l'accreditamento elaborato dall'autorità di controllo ceca, significa che il comitato non ha alcuna osservazione da fare e non chiede alla suddetta autorità di adottare ulteriori misure in merito.

9. Il presente parere non si pronuncia sulle voci presentate dall'autorità di controllo ceca che esulano dall'ambito di applicazione dell'articolo 43, paragrafo 2, del RGPD, come i riferimenti alla legislazione nazionale. Il comitato, tuttavia, osserva che la legislazione nazionale dovrebbe conformarsi al RGPD, ove previsto.

2.2 Elementi principali contenuti nei requisiti per l'accreditamento su cui si concentra la valutazione (articolo 43, paragrafo 2, del RGPD e allegato 1 delle linee guida del comitato) al fine di un esame coerente di quanto segue:

a. rispetto di tutti i punti chiave come evidenziato dall'allegato delle linee guida e analisi di qualsiasi scostamento rispetto all'allegato;

b. indipendenza dell'organismo di certificazione;

c. conflitti di interessi dell'organismo di certificazione;

d. competenza dell'organismo di certificazione;

e. garanzie appropriate per assicurare che i criteri di certificazione in materia di RGPD siano adeguatamente applicati dall'organismo di certificazione;

f. procedure per il rilascio, il riesame periodico e la revoca delle certificazioni in materia di RGPD;

g. gestione trasparente dei reclami relativi a violazioni della certificazione.

10. Tenuto conto che:

a. l'articolo 43, paragrafo 2, del RGPD contiene un elenco di condizioni relative all'accreditamento che un organismo di certificazione deve soddisfare per essere accreditato;

b. l'articolo 43, paragrafo 3, del RGPD prevede che i requisiti per l'accreditamento degli organismi di certificazione siano approvati dall'autorità di controllo competente;

c. l'articolo 57, paragrafo 1, lettere p) e q), del RGPD impone che l'autorità di controllo competente debba definire e pubblicare i requisiti per l'accreditamento degli organismi di certificazione e possa decidere di effettuare essa stessa l'accreditamento degli organismi di certificazione;

d. l'articolo 64, paragrafo 1, lettera c), del RGPD prevede che il comitato emetta un parere laddove un'autorità di controllo intenda approvare i requisiti per l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;

e. se l'accreditamento è effettuato dall'organismo nazionale di accreditamento in conformità della norma ISO/IEC 17065/2012, devono essere applicati anche i requisiti aggiuntivi stabiliti dall'autorità di controllo competente;

f. l'allegato 1 delle linee guida relative all'accreditamento degli organismi di certificazione delinea i requisiti consigliati che un'autorità di controllo in materia di protezione dei dati è tenuta a elaborare e che si applicano durante l'accreditamento di un organismo di certificazione da parte dell'organismo nazionale di accreditamento;

il comitato è del parere che:

2.2.1 PREMESSA

11. Il comitato riconosce che le disposizioni in materia di collaborazione tra un organismo nazionale di accreditamento e la rispettiva autorità di controllo in materia di protezione dei dati non costituiscono in quanto tali un requisito per l'accreditamento degli organismi di certificazione. Per motivi di completezza e trasparenza, il comitato reputa tuttavia che tali disposizioni, laddove esistano, siano rese pubbliche nei modi ritenuti opportuni dall'autorità di controllo.

2.2.2 OSSERVAZIONI GENERALI

12. Il comitato osserva che il progetto di requisiti per l'accreditamento non è interamente conforme alla struttura di cui all'allegato 1 delle linee guida. A titolo esemplificativo, mancano le sezioni «Ambito di applicazione» e «Termini e definizioni». A tale riguardo, il comitato ritiene che la numerazione e la struttura generale del documento potrebbero essere migliorate per garantire maggiore chiarezza e consentire una valutazione più agevole dei requisiti. Allo scopo, dunque, di agevolare la valutazione, il comitato invita l'autorità di controllo ceca a conformare il progetto di requisiti per l'accreditamento alla struttura dell'allegato e ad aggiungere le sezioni mancanti, vista la particolare rilevanza della definizione dei termini usati nell'intero documento. Il comitato osserva altresì che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca fa spesso riferimento alla corrispondente sezione della norma ISO 17065 o alle corrispondenti sezioni dell'allegato, senza specificare, tuttavia, tali riferimenti. Il comitato invita pertanto l'autorità di controllo ceca a esplicitare i riferimenti alle sezioni della norma ISO 17065 e dell'allegato.

13. Il comitato osserva che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca fa spesso riferimento all'«oggetto valutato» (*evaluated object*) (ad esempio nelle sezioni 3.2.1.2.1.2.10, 3.2.1.2.6.3.1, 3.2.1.2.8.1.6.3, 3.2.1.2.10.4.1, 3.1.2.10.7.3.1, 3.1.2.10.7.3.2 e 3.2.1.2.10.10.2). Il comitato ritiene che tale termine sia utilizzato quale sinonimo di «obiettivo di valutazione» (*target of evaluation*). Il comitato invita tuttavia l'autorità di controllo ceca a utilizzare in modo coerente l'espressione «obiettivo di valutazione» per maggiore chiarezza.

14. Il comitato osserva che numerosi requisiti non sono formulati come obblighi per l'organismo di certificazione (ad esempio 3.2.1.2.2 e 3.2.1.2.3). Il comitato invita l'autorità di controllo ceca a riformulare i requisiti per rendere esplicito il loro carattere obbligatorio, ad esempio iniziando le frasi relative ai requisiti con «L'organismo di certificazione deve […]».

2.2.3 REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO

15. Per quanto riguarda l'accordo di certificazione (sezione 3.2.1.2.1.2 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca), il comitato osserva che la sottosezione 3.2.1.2.1.2.2 non contiene alcun riferimento agli «aspetti contrattuali riservati» ai quali dovrà avere accesso anche l'autorità di controllo. Il comitato raccomanda pertanto all'autorità di controllo ceca di modificare il progetto di requisiti per includervi l'obbligo di fornire all'autorità di controllo l'accesso anche agli aspetti contrattuali riservati.

16. Per quanto riguarda la sottosezione 3.2.1.2.1.2.8 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca, il comitato osserva che non è chiaro a chi saranno divulgate le informazioni. Il comitato invita pertanto l'autorità di controllo ceca a precisare chi sarà il destinatario delle informazioni. Inoltre, tali informazioni devono essere «necessarie al rilascio della certificazione»,

come previsto dalla sezione 4.1.2, punto 7, dell'allegato. Il comitato raccomanda all'autorità di controllo ceca di sostituire l'espressione «informazioni sul rilascio della certificazione» (*information about granting certification*) con «informazioni necessarie al rilascio della certificazione» (*information necessary for granting certification*).

17. Nella sottosezione 3.2.1.2.1.2.9 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca non è chiaro quale tipo di informazioni dovrebbe essere comunicato direttamente al comitato. L'articolo 42, paragrafo 8, del RGPD sancisce per il comitato l'obbligo di raccogliere in un registro, tra l'altro, tutti i meccanismi di certificazione. In tale contesto si presume che le autorità di controllo competenti trasmettano le informazioni rilevanti al comitato, il quale poi le inserisce nel registro pubblico. Il comitato raccomanda pertanto all'autorità di controllo ceca di formulare in modo più chiaro la sottosezione 3.2.1.2.1.2.9 del progetto di requisiti, in conformità dell'articolo 42, paragrafo 8, del RGPD.

18. In merito alla sottosezione 3.2.1.2.1.2.12 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca, il comitato prende atto del fatto che tale autorità abbia riformulato una parte del requisito previsto dall'allegato. L'autorità di controllo ceca ha tuttavia omesso qualsiasi riferimento [laddove applicabile] al fatto che gli accordi di certificazione «disciplinano anche [...] le conseguenze [...] che si ripercuotono sul cliente». Il comitato raccomanda quindi all'autorità di controllo ceca di aggiungere la parte mancante del requisito sopra menzionato.

19. La sottosezione 3.2.1.2.1.2.13 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca stabilisce inoltre l'obbligo di «prevedere l'impegno del richiedente di comunicare all'organismo di certificazione tutte le modifiche tali da incidere sulla conformità dell'oggetto certificato rispetto ai criteri di certificazione». Il comitato considera questa formulazione troppo generica e raccomanda all'autorità di controllo ceca di modificare il progetto di requisiti per includervi «tutte le modifiche della propria situazione di fatto o giuridica e dei propri prodotti, processi e servizi coperti dalla certificazione».

20. Per quanto riguarda l'uso dei sigilli e marchi di protezione dei dati (sezione 3.2.1.2.1.3 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca), il comitato rileva che il progetto stabilisce che l'accordo di certificazione deve prevedere «norme per l'uso dei certificati, sigilli e marchi se forniti dal titolare dello schema di certificazione». La stessa formulazione è presente nella sottosezione 3.2.1.2.1.2.14. Il comitato ritiene che tale obbligo sia già contemplato nel punto 4.1.2.2., lettera l), della norma ISO 17065 e che, pertanto, dovrebbe essere previsto in tutti gli schemi di certificazione (si veda anche il punto 4.1.3 della norma ISO 17065). Il comitato raccomanda pertanto all'autorità di controllo ceca di eliminare le sezioni sopra menzionate a fini di una maggiore chiarezza.

21. In riferimento ai requisiti per la gestione dell'imparzialità, secondo le informazioni comunicate dall'autorità di controllo ceca nel modello, le sezioni 4.2.1, lettera b), e 4.2.2 dell'allegato sono sufficientemente trattate nel punto 4.2 della norma ISO 17065. Il comitato ritiene tuttavia che tali requisiti debbano essere inclusi espressamente nei progetti di requisiti per l'accreditamento elaborati dalle autorità di controllo in conformità dell'allegato. Il comitato raccomanda pertanto all'autorità di controllo ceca di includere i requisiti mancanti concernenti la gestione dell'imparzialità previsti dall'allegato.

22. In merito al requisito di responsabilità e finanziamento (sezione 3.2.1.2.3.1 del progetto di requisiti dell'autorità di controllo ceca), il comitato invita l'autorità di controllo ceca a specificare che detta conformità sarà verificata periodicamente.

2.2.4 REQUISITI PER LE RISORSE

23. Per quanto riguarda il personale dell'organismo di certificazione (sezione 3.2.1.2.8.1.6 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca), il comitato osserva che i requisiti applicabili al personale responsabile delle valutazioni (sottosezione 3.2.1.2.8.1.6.3) comprendono «*un'esperienza professionale di cinque anni con almeno dieci audit eseguiti, svolta in attività di certificazione nello stesso ambito o in un ambito analogo [...] ovvero un'esperienza di cinque anni nella certificazione degli oggetti su cui si concentra l'organismo di certificazione*». Analogamente, i requisiti per il personale responsabile delle decisioni (sottosezione 3.2.1.2.8.1.6.4) comprendono «*un'esperienza professionale di almeno cinque anni con almeno dieci audit eseguiti, svolta in attività di certificazione nello stesso ambito o in un ambito analogo*». Il comitato ritiene che i requisiti relativi alle competenze del personale responsabile delle valutazioni e di quello responsabile delle decisioni dovrebbero essere differenziati tenendo conto della diversità dei rispettivi compiti. A tale riguardo il comitato è del parere che il personale responsabile delle valutazioni dovrebbe possedere competenze ed esperienze professionali più specializzate in materia di procedure tecniche (ad esempio audit e certificazioni), mentre il personale responsabile delle decisioni dovrebbe avere competenze ed esperienze professionali più generali e di ampia portata in materia di protezione dei dati. Ciò considerato, il comitato invita l'autorità di controllo ceca a riformulare tale sottosezione tenendo conto dei differenti requisiti sostanziali relativi alle conoscenze e/o esperienze professionali del personale responsabile delle valutazioni e di quello responsabile delle decisioni.

24. Inoltre, il comitato prende atto del fatto che il punto 3.2.1.2.9.1 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca stabilisce che non è ammessa l'esternalizzazione delle attività di certificazione. Tuttavia, il punto successivo ammette il ricorso a revisori ed esperti di valutazione esterni, purché non costituisca un'attività di certificazione. Il comitato ritiene che il progetto di requisiti per l'accreditamento dovrebbe specificare quando ciò «costituisca un'attività di certificazione», ovvero dovrebbe precisare che l'organismo di certificazione manterrà la responsabilità delle decisioni anche quando si avvale di esperti esterni. Il comitato raccomanda pertanto all'autorità di controllo ceca di modificare di conseguenza il progetto.

2.2.5 REQUISITI DI PROCESSO

25. Il comitato osserva che la sezione 3.2.1.2.10.1.1 del progetto di requisiti aggiuntivi dell'autorità di controllo ceca fa riferimento a «tutti i requisiti aggiuntivi concernenti un conflitto di interessi (7.1, punto 1)». Tuttavia, il progetto di requisiti aggiuntivi dell'autorità di controllo ceca non prevede requisiti aggiuntivi concernenti eventuali conflitti di interessi. Il comitato invita pertanto l'autorità di controllo ceca a modificare il progetto per evitare confusione.

26. In merito ai requisiti per la presentazione della domanda, il comitato osserva che la sottosezione 3.2.1.2.10.2.3 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca sembra implicare che le informazioni sui dati trasferiti debbano essere fornite nella domanda soltanto se i dati vengono trasferiti a un paese terzo o a un'organizzazione internazionale. Il comitato sottolinea, tuttavia, che la domanda deve sempre contenere una descrizione dei dati trasferiti ad altri sistemi o organizzazioni, indipendentemente dalla loro ubicazione. Il comitato invita pertanto l'autorità di controllo ceca a modificare la formulazione per evitare confusione.

27. Il comitato osserva che l'obbligo di stabilire nell'accordo di certificazione metodi di valutazione vincolanti (sezione 3.2.1.2.1.2.6 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca) non contiene alcun riferimento all'obiettivo di valutazione, come invece previsto dalla sezione 7.3, punto 1, dell'allegato delle linee guida. Il comitato invita l'autorità di controllo ceca a inserire tale riferimento a fini di chiarezza.

28. Il comitato osserva altresì che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca contempla una situazione in cui si fa ricorso a responsabili del trattamento per eseguire operazioni di trattamento dei dati, in conformità dell'allegato delle linee guida (sezione 3.2.1.2.10.2 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca). Il comitato invita l'autorità di controllo ceca a valutare se, in questo caso, sia opportuno fare riferimento anche alla presenza di contitolari del trattamento e ai loro accordi specifici.

29. Per quanto riguarda i requisiti per la valutazione (sezione 3.2.1.2.10.4 del progetto di requisiti dell'autorità di controllo ceca), il comitato osserva che i requisiti per l'accreditamento dell'autorità di controllo ceca non prevedono l'obbligo dell'organismo di certificazione di indicare dettagliatamente nel proprio meccanismo di certificazione con quali modalità saranno fornite al richiedente le informazioni di cui al punto 7.4.6 della norma ISO 17065 in merito alle non conformità a un meccanismo di certificazione. Come stabilito nell'allegato (sottosezione 7.4), dovrebbero essere definite almeno la natura e le tempistiche di tali informazioni. Il comitato raccomanda pertanto all'autorità di controllo ceca di aggiungere l'obbligo sopra menzionato.

30. Inoltre, la sottosezione 3.2.1.2.10.4.2 del progetto di requisiti dell'autorità di controllo ceca sembra limitare i metodi di valutazione all'esecuzione di test, audit o ispezioni. Il comitato ritiene che si potrebbero utilizzare anche altri metodi di valutazione, e invita pertanto l'autorità di controllo ceca a modificare il progetto per specificare che l'elenco non è esaustivo.

31. In merito alla sottosezione 3.2.1.2.10.4.4.1.4 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca, il comitato ritiene che i requisiti dovrebbero stabilire chiaramente che l'organismo di certificazione è tenuto a verificare la conformità rispetto ai criteri, e invita l'autorità di controllo ceca a modificare di conseguenza il progetto.

32. Per quanto riguarda i requisiti per il riesame (sottosezione 3.2.1.2.10.5 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca), il comitato osserva che il progetto di requisiti per l'accreditamento non fa riferimento all'obbligo di definire procedure per il rilascio e la revoca delle certificazioni. Il comitato raccomanda all'autorità di controllo ceca di modificare di conseguenza il progetto.

33. Per quanto concerne i requisiti per la documentazione riguardante la certificazione, il comitato rileva che la sezione 3.1.2.10.7.2 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca prevede che l'organismo di certificazione specifichi che il monitoraggio è una condizione per la validità della certificazione «se il monitoraggio è richiesto da uno schema di certificazione [...]». Il comitato ritiene che, in caso di certificazione in conformità del RGPD, le attività di monitoraggio sono sempre obbligatorie, e pertanto raccomanda all'autorità di controllo ceca di inserire tale obbligo.

34. Per quanto riguarda i requisiti relativi all'elenco dei prodotti certificati (sezione 3.2.1.2.10.8 del progetto di requisiti per l'accreditamento dell'autorità di controllo ceca e sezione 7.8 dell'allegato) e, in particolare, l'obbligo di informare l'autorità di controllo competente in merito ai motivi del rilascio o della revoca della certificazione richiesta, il comitato osserva che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca fa riferimento alla sezione 3.2.1.2.10.4.5. Tuttavia, la

sezione citata riguarda l'obbligo di concedere all'autorità di controllo ceca l'accesso alla documentazione riguardante la valutazione, su richiesta; diversamente, il requisito di cui alla sezione 7.8 dell'allegato delle linee guida prevede l'obbligo di informare proattivamente l'autorità di controllo in merito ai motivi del rilascio o della revoca della certificazione. Il comitato raccomanda pertanto all'autorità di controllo ceca di modificare di conseguenza il progetto.

35. In merito alle modifiche che influenzano la certificazione, il comitato osserva che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca non elenca, tra le procedure da concordarsi, i processi di approvazione da parte dell'autorità di controllo competente, citati nell'allegato delle linee guida (pagina 21). Il comitato riconosce che l'elenco di cui alla sezione 7.10 dell'allegato non è obbligatorio. Tuttavia, al fine di garantire l'uniformità, il comitato invita l'autorità di controllo ceca ad aggiungere un riferimento ai processi di approvazione da parte dell'autorità di controllo.

36. Il comitato osserva che il progetto di requisiti per l'accreditamento dell'autorità di controllo ceca non include espressamente l'obbligo per l'organismo di certificazione di accettare decisioni e ordini dell'autorità di controllo competente che gli ingiungano di revocare o non rilasciare la certificazione a un richiedente se i requisiti per la certificazione non sono più soddisfatti. Il comitato raccomanda all'autorità di controllo ceca di inserire espressamente tale obbligo nel progetto di requisiti per l'accreditamento. In riferimento alla rescissione, riduzione, sospensione o revoca della certificazione, il comitato rileva che le sezioni 3.2.1.2.10.10.2 e 3.2.1.2.10.10.3 del progetto di requisiti fanno riferimento a un «incitamento» (*instigation*). Se l'intento è quello di riferirsi a «decisioni e ordini» dell'autorità di controllo, quali previste dall'articolo 58, paragrafo 2, lettera h), del RGPD, il comitato invita l'autorità di controllo ceca a utilizzare la stessa terminologia usata dal RGPD e a fare riferimento pertanto a «decisioni e ordini».

2.2.6 SISTEMA DI GESTIONE

37. Il comitato ritiene che la sezione 3.2.1.2.11 del progetto di requisiti aggiuntivi dell'autorità di controllo ceca non preveda l'obbligo per l'organismo di certificazione di « rendere noto al pubblico in via permanente e continuativa quali certificazioni ha effettuato e su quali basi [...], nonché la durata delle certificazioni e il quadro e le condizioni a cui è subordinata la loro validità», come previsto dalla sezione 8 dell'allegato. Il comitato raccomanda pertanto all'autorità di controllo ceca di modificare il progetto di requisiti inserendovi il riferimento sopra menzionato.

3 CONCLUSIONI / RACCOMANDAZIONI

38. Il progetto di requisiti per l'accreditamento presentato dall'autorità di controllo ceca può comportare un'applicazione non coerente dell'accreditamento degli organismi di certificazione; occorre quindi introdurre le modifiche di seguito riportate.

39. Per quanto riguarda i «requisiti generali in materia di accreditamento», il comitato raccomanda all'autorità di controllo ceca di:

    1) inserire nella sezione 3.2.1.2.1.2 l'obbligo di fornire all'autorità di controllo l'accesso agli «aspetti contrattuali riservati»;

    2) sostituire nella sottosezione 3.2.1.2.1.2.8 l'espressione «informazioni sul rilascio della certificazione » (*information about granting certification*) con «informazioni necessarie al rilascio della certificazione» (*information necessary for granting certification*);

3) formulare più chiaramente la sottosezione 3.2.1.2.1.2.9, in linea con l'articolo 42, paragrafo 8, del RGPD;

4) nella sottosezione 3.2.1.2.1.2.12 aggiungere un riferimento al fatto che gli accordi di certificazione [laddove applicabile] «disciplinano anche [...] le conseguenze [...] che si ripercuotono sul cliente»;

5) modificare la sottosezione 3.2.1.2.1.2.13 per includervi «tutte le modifiche della propria situazione di fatto o giuridica e dei propri prodotti, processi e servizi coperti dalla certificazione»;

6) eliminare la sezione 3.2.1.2.1.3 e la sottosezione 3.2.1.2.1.2.14;

7) includere i requisiti mancanti concernenti la gestione dell'imparzialità previsti dall'allegato.

40. Per quanto riguarda i «requisiti per le risorse», il comitato raccomanda all'autorità di controllo ceca di:

1) modificare la sezione 3.2.1.2.9.1 per specificare quando «costituisce un'attività di certificazione», oppure precisare che l'organismo di certificazione manterrà la responsabilità delle decisioni anche quando si avvale di esperti esterni.

41. Per quanto riguarda i «requisiti di processo», il comitato raccomanda all'autorità di controllo ceca di:

1) includere nella sezione 3.2.1.2.10.4 l'obbligo per l'organismo di certificazione di indicare dettagliatamente nel proprio meccanismo di certificazione con quali modalità saranno fornite al richiedente le informazioni di cui al punto 7.4.6 della norma ISO 17065 in merito alle non conformità a un meccanismo di certificazione;

2) modificare la sezione 3.2.1.2.10.5 per fare riferimento all'obbligo di definire procedure per il rilascio e la revoca delle certificazioni;

3) modificare la sezione 3.1.2.10.7.2 per tenere conto del fatto che, in caso di certificazione in conformità del RGPD, le attività di monitoraggio sono sempre obbligatorie;

4) modificare la sezione 3.2.1.2.10.8 per tenere conto dell'obbligo per l'organismo di certificazione di informare proattivamente l'autorità di controllo in merito ai motivi del rilascio o della revoca della certificazione;

5) inserire l'obbligo per l'organismo di certificazione di accettare decisioni e ordini dell'autorità di controllo competente che gli ingiungano di revocare o non rilasciare la certificazione a un richiedente se i requisiti per la certificazione non sono più soddisfatti.

42. Per quanto riguarda il «sistema di gestione», il comitato raccomanda all'autorità di controllo ceca di:

1) inserire l'obbligo per l'organismo di certificazione di « rendere noto al pubblico in via permanente e continuativa quali certificazioni ha effettuato e su quali basi [...], nonché la durata delle certificazioni e il quadro e le condizioni a cui è subordinata la loro validità», come previsto dalla sezione 8 dell'allegato.

4 OSSERVAZIONI FINALI

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

44. Ai sensi dell'articolo 64, paragrafi 7 e 8, del RGPD, l'autorità di controllo ceca, entro due settimane dal ricevimento del parere, comunica per via elettronica al presidente se intende mantenere o modificare il progetto di elenco di requisiti. Entro lo stesso termine l'autorità di controllo invia il progetto di elenco di requisiti modificato oppure, ove non intenda conformarsi al parere del comitato, comunica le pertinenti motivazioni, in base alle quali non intende conformarsi al presente parere, in tutto o in parte.

45. L'autorità di controllo ceca comunica la decisione definitiva al comitato affinché sia inserita nel registro delle decisioni soggette al meccanismo di coerenza, ai sensi dell'articolo 70, paragrafo 1, lettera y), del RGPD.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)