Parere 15/2020 sul progetto di decisione delle autorità di controllo competenti della Germania riguardante l'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

1 SINTESI DEI FATTI 4

2 VALUTAZIONE 5

2.1 Analisi generale del comitato europeo per la protezione dei dati in merito al progetto di decisione presentato 5

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: 6

2.2.1 PREMESSA 7

2.2.2 TERMINI E DEFINIZIONI 7

2.2.3 OSSERVAZIONI GENERALI 7

2.2.4 REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO (sezione 4 del progetto di requisiti per l'accreditamento) 7

2.2.5 REQUISITI RELATIVI ALLE RISORSE (sezione 6 del progetto di requisiti per l'accreditamento) 9

2.2.6 REQUISITI DI PROCESSO (sezione 7 del progetto di requisiti per l'accreditamento) 10

2.2.7 ULTERIORI REQUISITI AGGIUNTIVI 12

3 CONCLUSIONI / RACCOMANDAZIONI 12

4 OSSERVAZIONI CONCLUSIVE 13

Il comitato europeo per la protezione dei dati

visti l'articolo 63, l'articolo 64, paragrafo 1, lettera c), 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 n. 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 di garantire l'applicazione coerente del regolamento (UE) 2016/679 (di seguito 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 per l'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, invitando innanzitutto le autorità di controllo a definire i propri requisiti per l'accreditamento seguendo la struttura di cui all'allegato 1 delle linee guida 4/2018 del comitato stesso 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 CEPD 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, non è necessario che siano identici. Le autorità di controllo competenti godono di un margine di discrezionalità relativamente al contesto nazionale o regionale e dovrebbero tenere conto della propria legislazione locale. Il parere del comitato europeo per la protezione dei dati 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 devono 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. Rispetto agli obblighi relativi all'accreditamento degli organismi di certificazione a carico degli organismi nazionali di accreditamento, l'articolo 43 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 dall'autorità di controllo stessa ai sensi dell'articolo 43, paragrafo 1, lettera b) del RGPD. Il comitato europeo per la protezione dei dati osserva che l'articolo 43, paragrafo 2, lettere da a) a e), rispecchia e specifica i requisiti di cui alla norma ISO 17065, contribuendo così alla coerenza ([2]).

(6) Ai sensi dell'articolo 64, paragrafo 1, lettera c) e dell'articolo 64, paragrafi 3 e 8, del RGPD in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno del comitato, il parere del comitato europeo per la protezione dei dati è adottato entro otto settimane a partire dal primo giorno lavorativo successivo alla data in cui il presidente e l'autorità di controllo competente hanno deciso che il fascicolo è completo. Su decisione del presidente, tale termine può essere prorogato di ulteriori sei settimane, tenendo conto della complessità della questione.

HA ADOTTATO IL PRESENTE PARERE:

1 SINTESI DEI FATTI

1. Le autorità di controllo tedesche della Federazione e dei Länder hanno 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 13 febbraio 2020. L'organismo nazionale di accreditamento della Germania, DAkkS, accrediterà gli organismi di certificazione preposti a certificare utilizzando i criteri di certificazione del RGPD. Ciò significa che, ai fini dell'accreditamento degli organismi di certificazione, l'organismo nazionale di accreditamento utilizzerà la norma ISO 17065 nonché i requisiti aggiuntivi stabiliti dalle autorità di controllo tedesche, una volta che queste li abbiano approvati a seguito del parere espresso dal comitato sul progetto di tali requisiti.

2. Ai sensi dell'articolo 10, paragrafo 2, del regolamento interno del comitato, data la complessità della questione in esame, la presidente ha deciso di estendere di ulteriori sei settimane il periodo di adozione iniziale di otto settimane.

([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 VALUTAZIONE

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

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 non pregiudica i compiti e i poteri dell'autorità di controllo competente. Nel caso di specie, il comitato osserva che le autorità di controllo tedesche hanno deciso di affidarsi all'accreditamento congiunto da parte del proprio organismo nazionale di accreditamento (DAkkS) e dell'autorità di controllo competente, per il rilascio dell'accreditamento, avendo elaborato, in conformità delle linee guida, requisiti aggiuntivi che dovrebbero essere utilizzati al momento del rilascio dell'accreditamento.

4. La presente valutazione dei requisiti aggiuntivi per l'accreditamento delle autorità di controllo tedesche 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 supportare le autorità di controllo nel 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 dalle autorità di controllo, in modo tale da consentire la loro applicazione pratica e coerente in funzione delle necessità del contesto in cui operano le autorità di controllo.

6. Il comitato riconosce che, viste le loro competenze, sia opportuno lasciare libertà di manovra agli organismi nazionali di accreditamento e alle autorità di controllo competenti, se del caso, 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 e pertanto non si farà menzione nel presente parere al testo del relativo documento. Il comitato ha quindi deciso di fare riferimento a specifiche sezioni della norma ISO, se necessario, senza tuttavia riprodurne il testo.

8. Il comitato ha, infine, 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 dalle autorità di controllo tedesche, significa che il comitato non ha alcuna osservazione da fare e non chiede alle suddette autorità di adottare ulteriori misure in merito.

9. Il presente parere non si pronuncia sulle voci presentate dalle autorità di controllo tedesche 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:

1) rispetto di tutti i punti chiave evidenziati dall'allegato delle linee guida e analisi di qualsiasi scostamento rispetto all'allegato;
2) indipendenza dell'organismo di certificazione;
3) conflitti di interessi dell'organismo di certificazione;
4) competenza dell'organismo di certificazione;
5) garanzie appropriate per assicurare che i criteri di certificazione in materia di RGPD siano adeguatamente applicati dall'organismo di certificazione;
6) procedure per il rilascio, il riesame periodico e la revoca delle certificazioni in materia di RGPD;
7) 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 stabilisce 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 relativa 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 TERMINI E DEFINIZIONI

12. Il comitato osserva che la sezione 3 («Definizioni») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche definisce quali tipologie di schemi di certificazione sono ammesse, specificando che esse devono soddisfare i requisiti della norma DIN EN ISO/IEC 17065. A questo proposito, si evidenzia che le sezioni 5.1 e 5.2 delle linee guida del comitato europeo per la protezione dei dati definiscono già chiaramente e dettagliatamente ciò che può essere oggetto di certificazione ai sensi del RGPD. Il comitato riconosce pertanto che l'intento delle autorità di controllo tedesche non è di limitare quanto indicato nelle linee guida e che le affermazioni contenute nella sezione 3 del progetto di requisiti per l'accreditamento elaborato dalle stesse devono essere considerate applicabili nel contesto di tali requisiti per l'accreditamento.

2.2.3 OSSERVAZIONI GENERALI

13. Il comitato osserva che la sezione «note generali» del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche fa riferimento all'«autorizzazione» dei criteri di certificazione da parte del comitato europeo per la protezione dei dati «conformemente all'articolo 63 e all'articolo 64, paragrafo 1, lettera c), del RGPD». Il comitato osserva che il RGPD non conferisce al comitato europeo per la protezione dei dati la competenza ad «autorizzare» i criteri di certificazione. Tuttavia, secondo i suddetti articoli, il comitato europeo per la protezione dei dati può approvare i criteri di certificazione. Il comitato raccomanda pertanto alle autorità di controllo tedesche di eliminare il riferimento all'«autorizzazione da parte del comitato europeo per la protezione dei dati», al fine di adeguare il progetto di requisiti alla formulazione del RGPD.

2.2.4 REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO (sezione 4 del progetto di requisiti per l'accreditamento)

14. Per quanto riguarda il requisito della responsabilità giuridica (sottosezione 4.1 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche), il comitato osserva che, nel documento di accompagnamento, le autorità di controllo tedesche spiegano come ci si aspetti che l'organismo di certificazione disponga di procedure aggiornate e che pertanto non sia necessario aggiungere ulteriori requisiti a tale riguardo. Tuttavia, il comitato ritiene che un'aspettativa non vincoli gli organismi di certificazione a disporre di tali procedure. Come stabilito nella sottosezione 4.1.1 dell'allegato alle linee guida, gli organismi di certificazione devono disporre di procedure aggiornate che dimostrino la conformità alle responsabilità giuridiche stabilite nei requisiti di accreditamento. Inoltre, l'organismo di certificazione deve essere in grado di fornire prove dell'esistenza di procedure e misure conformi al RGPD specificamente finalizzate al controllo e alla gestione dei dati personali dell'organizzazione cliente nel quadro del processo di certificazione. Il comitato raccomanda pertanto

alle autorità di controllo tedesche di modificare il progetto di requisiti al fine di adeguarli alle linee guida.

15. Per quanto riguarda la sottosezione 4.1.2.2 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche («accordo di certificazione»), il comitato osserva che esso non prevede l'obbligo di garantire piena trasparenza nei riguardi dell'autorità di controllo competente rispetto alla procedura di certificazione, comprese le questioni soggette a vincoli contrattuali di riservatezza. Inoltre, non vi è alcun riferimento all'obbligo del richiedente di fornire all'organismo di certificazione l'accesso alle proprie attività di trattamento. Il comitato raccomanda pertanto alle autorità di controllo tedesche di introdurre i suddetti obblighi nel progetto di requisiti.

16. Il comitato osserva che il riferimento esplicito ai compiti e ai poteri dell'autorità di controllo competente (sottosezione 4.1.2, punto 3, dell'allegato) non è incluso nella sottosezione 4.1.2.2 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche. Il comitato è del parere che tale riferimento debba essere aggiunto nel progetto di requisiti e, pertanto, raccomanda alle autorità di controllo tedesche di modificare il progetto di conseguenza.

17. Inoltre, in merito all'accordo di certificazione, il progetto di requisiti delle autorità di controllo tedesche non prevede l'obbligo di consentire all'organismo di certificazione di comunicare tutte le informazioni necessarie al rilascio della certificazione ai sensi dell'articolo 42, paragrafo 8, e dell'articolo 43, paragrafo 5, del RGPD (sottosezione 4.1.2, punto 7, dell'allegato). Anche se tale obbligo è previsto nella sezione sulla gestione del procedimento del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato ritiene che dovrebbe essere compreso nell'accordo di certificazione, al fine di rafforzarne la natura vincolante. Il comitato raccomanda pertanto alle autorità di controllo tedesche di introdurre il suddetto obbligo fra gli elementi dell'accordo di certificazione.

18. Ai sensi dell'allegato, il richiedente deve informare l'organismo di certificazione in caso di modifiche significative della propria situazione di fatto o di diritto e dei prodotti, processi e servizi interessati dalla certificazione (sottosezione 4.1.2, punto 10, dell'allegato). Tuttavia, nel progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il punto 6 della sottosezione 4.1.2.2 prevede solo l'obbligo di informare l'organismo di certificazione in caso di modifiche significative delle circostanze di fatto o di diritto, senza citare esplicitamente i prodotti, i processi e i servizi. Il comitato raccomanda alle autorità di controllo tedesche di introdurre tale riferimento, in conformità con l'allegato.

19. Per quanto riguarda la sottosezione 4.2.7 («gestione dell'imparzialità») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato raccomanda di rafforzare i criteri applicabili agli organismi di certificazione che appartengono a o sono sotto il controllo di un soggetto giuridicamente distinto, in modo da tenere in considerazione che qualsiasi tipo di relazione economica tra l'organismo di certificazione e tale soggetto, a seconda delle sue caratteristiche, può influenzare l'imparzialità delle attività di certificazione.

20. Per quanto riguarda la sottosezione 4.6 («informazioni disponibili al pubblico») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato osserva che non vi è alcun riferimento alla pubblicazione di tutte le versioni dei criteri approvati e delle procedure di certificazione. Il comitato invita pertanto le autorità di controllo tedesche a modificare il progetto di requisiti per l'accreditamento al fine di esplicitare che la pubblicazione include tutte le versioni dei criteri approvati e delle procedure di certificazione. Inoltre, il comitato osserva che il secondo paragrafo della sottosezione 4.6 afferma che «gli schemi di certificazione utilizzati dall'organismo di

certificazione i criteri approvati in conformità all'articolo 42, paragrafo 5, RGPD, che indicano la durata autorizzata di applicazione, *in generale devono essere pubblicati*». Per evitare qualsiasi ambiguità, il comitato invita le autorità di controllo tedesche a cancellare la parola «in generale» e a inserire la congiunzione «e» tra «organismo di certificazione» e «i criteri approvati».

2.2.5 REQUISITI RELATIVI ALLE RISORSE (sezione 6 del progetto di requisiti per l'accreditamento)

21. Per quanto riguarda i requisiti in materia di competenza e, in particolare, la sottosezione 6.1.2.1 («competenze delle risorse umane») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato osserva che, in merito alle conoscenze richieste nei settori elencati, non si specifica che esse devono essere pertinenti e adeguate. Al fine di garantire la coerenza con il livello di esperienza richiesto nell'allegato, il comitato raccomanda alle autorità di controllo tedesche di uniformare la formulazione alle linee guida, introducendo il requisito che le conoscenze siano pertinenti e adeguate.

22. Inoltre, il comitato osserva che i requisiti per il personale con competenze tecniche responsabile del processo decisionale prevedono almeno sette anni di esperienza professionale o cinque anni di esperienza professionale in materia di protezione tecnica dei dati, a seconda del livello di istruzione, mentre il personale responsabile delle valutazioni dovrebbe avere quattro anni di esperienza professionale o due anni di esperienza professionale in materia di protezione tecnica dei dati ed esperienza nelle procedure di prova, a seconda del livello di istruzione. Analogamente, il personale con competenze giuridiche responsabile delle decisioni deve avere almeno cinque anni di esperienza professionale nell'ambito del diritto della protezione dei dati, mentre il personale responsabile delle valutazioni deve avere almeno due anni di esperienza professionale nell'ambito del diritto della protezione dei dati e in materia di procedure di controllo. Il comitato osserva che esiste una differenza significativa, quanto al numero minimo di anni di esperienza professionale richiesti, tra il personale responsabile delle decisioni e il personale responsabile delle valutazioni. A questo proposito, il comitato ritiene che i requisiti di competenza per i responsabili delle valutazioni e i responsabili delle decisioni debbano essere definiti in base ai diversi compiti che essi svolgono, piuttosto che guardando al numero di anni di esperienza. Il comitato è del parere che il personale responsabile delle valutazioni dovrebbe possedere competenze ed esperienza professionale più specialistiche per quanto concerne le procedure tecniche (ad es. audit e certificazioni), mentre il personale responsabile delle decisioni dovrebbe avere competenze ed esperienza professionale più generali e di ampia portata in materia di protezione dei dati. Alla luce di queste considerazioni, il comitato invita le autorità di controllo tedesche a dare maggiore rilievo alle diverse conoscenze e/o esperienze sostanziali necessarie per il personale responsabile delle decisioni e per quello responsabile delle valutazioni, riducendo il divario degli anni di esperienza richiesti.

23. Inoltre, il comitato ritiene che la conoscenza dei sistemi di gestione pertinenti per il settore delle certificazioni debba essere estesa alla norma ISO/IEC 27701:2019 «Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines» e invita le autorità di controllo tedesche a introdurre tale riferimento.

24. Infine, per quanto riguarda i requisiti di formazione del personale tecnico, il comitato ritiene che l'elenco delle materie sia già adeguato alle esperienze tecniche richieste dall'allegato. Il comitato

invita pertanto le autorità di controllo tedesche a eliminare il riferimento alle «scienze naturali» dall'elenco delle materie relative alla formazione universitaria del personale tecnico.

2.2.6 REQUISITI DI PROCESSO (sezione 7 del progetto di requisiti per l'accreditamento)

25. Il comitato osserva che la sezione 7 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche usa diverse volte il termine «i suoi criteri» (ad esempio nelle sottosezioni 7.4, 7.6, 7.11 e 7.13). Al fine di evitare qualsiasi ambiguità, il comitato invita le autorità di controllo tedesche a chiarire il significato di tale termine, ad esempio aggiungendo una spiegazione nell'appendice 1 (Glossario).

26. Per quanto riguarda la sottosezione 7.1 («informazioni generali») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato osserva che non c'è alcun riferimento esplicito all'obbligo dell'organismo di certificazione di rispettare i requisiti aggiuntivi. Anche se tale obbligo potrebbe essere dedotto dal testo del progetto di requisiti, il comitato ritiene che debba essere introdotto un riferimento esplicito al suddetto obbligo. Pertanto, il comitato raccomanda alle autorità di controllo tedesche di modificare il progetto di conseguenza.

27. Il comitato osserva che il progetto di requisiti aggiuntivi delle autorità di controllo tedesche non contiene alcun riferimento all'utilizzo di un sigillo europeo per la protezione dei dati approvato, di cui alla sottosezione 7.1.2 dell'allegato. Il comitato è del parere che tale riferimento debba essere introdotto, soprattutto considerando che l'accreditamento di un organismo di certificazione che rilascia sigilli europei per la protezione dei dati potrebbe dover essere effettuato in ciascuno degli Stati membri in cui l'organismo di certificazione è stabilito ([3]). Pertanto, il comitato raccomanda alle autorità di controllo tedesche di introdurre il suddetto riferimento. Ad esempio, il progetto di requisiti potrebbe indicare quanto segue: *«L'autorità di controllo competente viene informata prima che un organismo di certificazione cominci a utilizzare in un nuovo Stato membro, attraverso una sede distaccata, un sigillo europeo per la protezione dei dati approvato».*

28. Il comitato osserva che nella sottosezione 7.2 («domanda»), il progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche prevede la situazione in cui si fa ricorso a responsabili del trattamento per effettuare operazioni di trattamento dei dati, in linea con l'allegato alle linee guida. Tuttavia, il comitato osserva che, quando si fa ricorso a responsabili del trattamento, la domanda deve contenere il pertinente contratto (o contratti) fra il titolare e il responsabile del trattamento, come indicato nell'allegato. Il comitato raccomanda pertanto alle autorità di controllo tedesche di adeguare la formulazione alle linee guida introducendo il riferimento al contratto (o contratti) fra titolare del trattamento e responsabile del trattamento. Inoltre, il comitato invita le autorità di controllo tedesche a valutare se, in questo caso, sia opportuno fare riferimento anche ai contitolari del trattamento e a loro accordi specifici.

29. Il comitato osserva che la sottosezione 7.2 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche specifica che «hanno il diritto di richiedere la certificazione il titolare del trattamento e il responsabile del trattamento». La facoltà dei responsabili del trattamento di richiedere una certificazione dipenderà dallo specifico schema di certificazione. Pertanto, al fine di evitare confusione, il comitato invita le autorità di controllo tedesche a eliminare il suddetto

([3]) A questo proposito, cfr. le linee guida 1/2018, punto 44.

riferimento oppure a chiarire che la possibilità di certificare responsabili del trattamento dipenderà dall'ambito di applicazione dello schema di certificazione.

30. Per quanto riguarda la sottosezione 7.3 («domande di valutazione») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato osserva che il progetto di requisiti indica che «i metodi di valutazione pianificati sono stabiliti da contratto [...]». Per chiarire che si tratta di un requisito, il comitato invita le autorità di controllo tedesche a riformulare il primo paragrafo, al fine di chiarire che i metodi di valutazione devono essere inclusi nell'accordo di certificazione, stabilendo quindi che «i metodi di valutazione previsti devono essere stabiliti da contratto [...]». Inoltre, il comitato invita le autorità di controllo tedesche a sostituire il riferimento alla sottosezione 7.3.1.b della norma ISO 17065 con quello alla sottosezione 7.3 della stessa, al fine di adeguare la formulazione all'allegato. Il comitato osserva anche che il quarto paragrafo fa riferimento ad adeguate competenze tecniche e giuridiche. Per maggiore chiarezza, il comitato invita le autorità di controllo tedesche ad aggiungere «in materia di protezione dei dati».

31. Il comitato osserva che la sottosezione 7.4 («metodi di valutazione») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche non prevede l'obbligo da parte dell'organismo di certificazione di descrivere metodi di valutazione sufficienti a valutare la conformità delle operazioni di trattamento ai criteri di certificazione. Il comitato raccomanda alle autorità di controllo tedesche di modificare il progetto di requisiti al fine di introdurre tale riferimento. Per esempio, si potrebbe aggiungere quanto segue: «*L'organismo di certificazione garantisce che i meccanismi utilizzati per rilasciare la certificazione descrivano metodi di valutazione sufficienti a valutare la conformità dei trattamenti ai criteri di certificazione*». Inoltre, per quanto riguarda il primo ambito da considerare nei metodi di valutazione, il comitato ritiene che la necessità e la proporzionalità debbano essere valutate anche in relazione agli interessati, se del caso. Infine, il comitato osserva che non vi è alcun riferimento alla documentazione dei metodi e dei risultati. Pertanto, il comitato invita le autorità di controllo tedesche a modificare il progetto e a introdurre esplicitamente i riferimenti di cui sopra.

32. Per quanto riguarda le certificazioni esistenti (sottosezione 7.4 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche), il comitato ritiene che il punto 4 a pag. 13 crei confusione, poiché non è chiaro quale sia il collegamento tra i periodi di validità della certificazione attuale e di quella precedente e come si concilierebbero tra loro. Inoltre, non sembra possibile mettere in discussione la validità di una certificazione precedentemente rilasciata da un diverso organismo di certificazione accreditato. In sintesi, il paragrafo trarrebbe beneficio da una maggiore chiarezza per quanto riguarda il rapporto tra i diversi elementi menzionati. Il comitato raccomanda alle autorità di controllo tedesche di modificare il progetto di requisiti, in particolare chiarendo che il periodo di validità della certificazione ai sensi del RGPD non deve essere subordinato alla validità di altri tipi di certificazioni.

33. Per quanto riguarda la sottosezione 7.5 («valutazione») del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche, il comitato invita queste ultime a cambiare il titolo della sezione in «verifica».

34. Per quanto riguarda le modifiche che incidono sulla certificazione (sottosezione 7.10 del progetto di requisiti per l'accreditamento delle autorità di controllo tedesche), il comitato osserva che il progetto di requisiti stabilisce che «il cliente è informato tempestivamente delle modifiche del quadro giuridico che lo riguardano». Tenendo presente la necessità di preservare l'imparzialità dell'organismo di certificazione, il comitato invita le autorità di controllo tedesche a riformulare la frase per chiarire che

al cliente vengono fornite, in modo tempestivo, informazioni generali sulle modifiche che potrebbero riguardarlo. Per garantire inoltre una chiara comprensione di ciò che si intende con «decisioni del comitato europeo per la protezione dei dati», il comitato invita le autorità di controllo tedesche a chiarire tale riferimento. A titolo esemplificativo, si potrebbe utilizzare l'espressione «documenti adottati dal comitato europeo per la protezione dei dati».

35. Il comitato osserva che la sottosezione 7.11 del progetto di requisiti per l'accreditamento elaborato dalle autorità di controllo tedesche («termine, limitazione, sospensione o revoca della certificazione») non prevede l'obbligo dell'organismo di certificazione di accettare decisioni e prescrizioni delle autorità di controllo tedesche che gli ingiungano di revocare o non rilasciare la certificazione a un richiedente qualora i requisiti per la certificazione non siano o non siano più soddisfatti. Il comitato raccomanda pertanto alle autorità di controllo tedesche di introdurre tale obbligo. Inoltre, il comitato invita le autorità di controllo tedesche a sostituire la parola «limitazione» con «riduzione» nel titolo della sezione, in conformità con l'allegato alle linee guida.

2.2.7 ULTERIORI REQUISITI AGGIUNTIVI

36. Per quanto riguarda la sottosezione 8.11.3 («gestione dei reclami») dei requisiti per l'accreditamento delle autorità di controllo tedesche, il comitato invita le stesse a sostituire il riferimento ai «reclami giustificati» con «reclami motivati», al fine di una maggiore chiarezza.

3 CONCLUSIONI / RACCOMANDAZIONI

37. Il progetto di requisiti per l'accreditamento presentato dalle autorità di controllo tedesche della Federazione e dei Länder può comportare un'applicazione non coerente dell'accreditamento degli organismi di certificazione; occorre quindi introdurre le modifiche di seguito riportate.

38. Per quanto riguarda le «osservazioni generali», il comitato raccomanda alle autorità di controllo tedesche di:

    1) eliminare il riferimento all'«autorizzazione da parte del comitato europeo per la protezione dei dati», al fine di adeguare il progetto di requisiti alla formulazione del RGPD.

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

    1) modificare i requisiti relativi alla responsabilità giuridica (sottosezione 4.1) per adeguarli alle linee guida;

    2) modificare la sottosezione 4.1.2.2 per introdurre, nell'accordo di certificazione, l'obbligo di garantire piena trasparenza alle autorità di controllo tedesche relativamente alla procedura di certificazione, e di fornire all'organismo di certificazione l'accesso alle attività di trattamento del richiedente;

    3) introdurre, nella sottosezione 4.1.2.2, un riferimento esplicito ai compiti e ai poteri dell'autorità di controllo competente, conformemente all'allegato;

4) introdurre, fra gli elementi dell'accordo di certificazione, l'obbligo di consentire all'organismo di certificazione di comunicare tutte le informazioni necessarie al rilascio della certificazione ai sensi dell'articolo 42, paragrafo 8, e dell'articolo 43, paragrafo 5, del RGPD;

5) introdurre un riferimento esplicito ai «prodotti, processi e servizi coperti dalla certificazione» al punto 6 della sottosezione 4.1.2.2;

6) rafforzare, nella sottosezione 4.2.7, i criteri applicabili agli organismi di certificazione che appartengono a o sono sotto il controllo di un soggetto giuridicamente distinto, in modo da tenere in considerazione che qualsiasi tipo di relazione economica tra l'organismo di certificazione e tale soggetto, a seconda delle sue caratteristiche, può influenzare l'imparzialità delle attività di certificazione.

40. Per quanto riguarda i «requisiti in materia di risorse umane», il comitato raccomanda alle autorità di controllo tedesche di:

1) adeguare la formulazione della sottosezione 6.1.2.1 alle linee guida, richiedendo che le conoscenze siano pertinenti e adeguate.

41. Per quanto riguarda i «requisiti di processo», il comitato raccomanda alle autorità di controllo tedesche di:

1) modificare la sottosezione 7.1 affinché contenga un riferimento esplicito all'obbligo dell'organismo di certificazione di rispettare i requisiti aggiuntivi;

2) introdurre un riferimento all'utilizzo di un sigillo europeo per la protezione dei dati approvato;

3) adeguare la formulazione della sottosezione 7.2 alle linee guida introducendo il riferimento al contratto (o contratti) fra titolare del trattamento e responsabile del trattamento;

4) introdurre nella sottosezione 7.4 l'obbligo dell'organismo di certificazione di descrivere metodi di valutazione sufficienti a valutare la conformità delle operazioni di trattamento ai criteri di certificazione;

5) chiarire, nella sottosezione 7.4, che il periodo di validità della certificazione ai sensi del RGPD non deve essere subordinato alla validità di altri tipi di certificazioni;

6) prevedere, nella sottosezione 7.11, l'obbligo dell'organismo di certificazione di accettare decisioni e prescrizioni delle autorità di controllo tedesche che gli ingiungano di revocare o non rilasciare la certificazione a un richiedente qualora i requisiti per la certificazione non siano più soddisfatti.

4 OSSERVAZIONI CONCLUSIVE

42. Le autorità di controllo tedesche della Federazione e dei Länder sono destinatarie del presente parere, che sarà reso pubblico ai sensi dell'articolo 64, paragrafo 5, lettera b, del RGPD.

43. Ai sensi dell'articolo 64, paragrafi 7 e 8, del RGPD, le autorità di controllo tedesche comunicano, entro due settimane dal ricevimento del parere, per via elettronica al presidente del comitato se intendono mantenere o modificare il progetto di decisione. Entro lo stesso termine le autorità di controllo trasmettono il progetto di decisione modificato oppure comunicano le motivazioni per le quali non intendono conformarsi al parere del comitato, in tutto o in parte.

44. Le autorità di controllo tedesche comunicano 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)