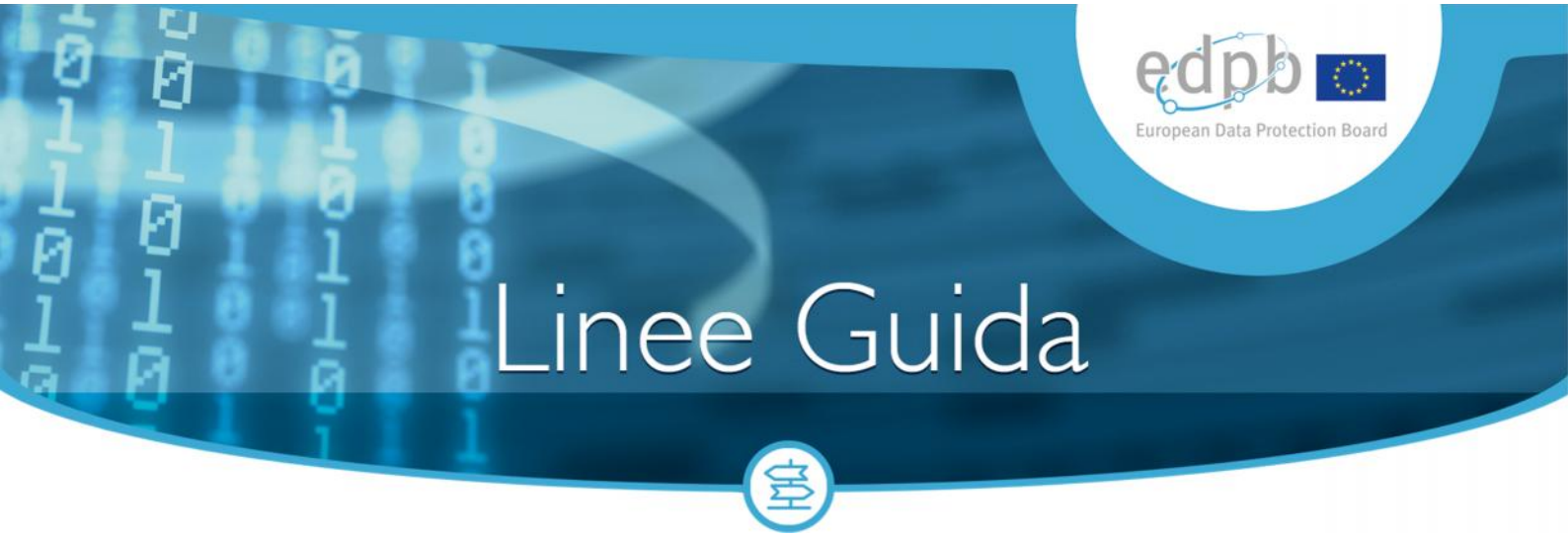

Linee-guida 4/2018 relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del regolamento generale sulla protezione dei dati (2016/679)

Adottate il 4 dicembre 2018

Sommario

Il comitato europeo per la protezione dei dati

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE 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,

HA ADOTTATO LE SEGUENTI LINEE-GUIDA

1 INTRODUZIONE

Il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) («il RGPD»), entrato in vigore il 25 maggio 2018, istituisce un quadro di conformità aggiornato per la protezione dei dati in Europa, basato sul principio di responsabilizzazione e sulla tutela di diritti fondamentali. All'interno di tale nuovo quadro, risultano essenziali diverse misure intese a facilitare la conformità alle disposizioni del RGPD. Esse includono requisiti obbligatori in circostanze specifiche (inclusa la nomina di responsabili della protezione dei dati e lo svolgimento di valutazioni d'impatto sulla protezione dei dati) nonché misure volontarie, quali codici di condotta e meccanismi di certificazione.

Nell'ambito dell'istituzione di meccanismi di certificazione e di sigilli e marchi di protezione dei dati, l'articolo 43, paragrafo 1, del RGPD impone agli Stati membri di garantire che gli organismi di certificazione che rilasciano certificazioni ai sensi dell'articolo 42, paragrafo 1, siano accreditati dall'autorità di controllo competente o dall'organismo nazionale di accreditamento, o da entrambi. 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.

Meccanismi di certificazione significativi possono migliorare la conformità al RGPD e la trasparenza per gli interessati e nelle relazioni tra imprese (B2B), ad esempio tra i titolari e i responsabili del trattamento. I titolari e i responsabili del trattamento dei dati beneficeranno di un'attestazione di terza parte che dimostra la conformità delle loro operazioni di trattamento[1].

In questo contesto, il comitato europeo per la protezione dei dati riconosce la necessità di fornire orientamenti in relazione all'accreditamento. Il valore e lo scopo peculiari dell'accreditamento consistono nell'attestazione autorevole della competenza degli organismi di certificazione, e ciò consente di creare fiducia nel meccanismo stesso di certificazione.

Le presenti linee-guida mirano a fornire indicazioni sull'interpretazione e l'attuazione delle disposizioni di cui all'articolo 43 del RGPD. In particolare, esse intendono aiutare gli Stati membri, le autorità di controllo e gli organismi nazionali di accreditamento a stabilire un quadro di riferimento coerente e

[1] Il considerando 100 del RGPD afferma che l'istituzione di meccanismi di certificazione può migliorare la trasparenza e il rispetto del regolamento e consentire agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi.

armonizzato per l'accreditamento degli organismi di certificazione che rilasciano certificazioni in conformità del RGPD.

2 AMBITO DI APPLICAZIONE DELLE LINEE-GUIDA

Le presenti Linee-guida:

- definiscono l'obiettivo dell'accreditamento nel contesto del RGPD;
- illustrano le procedure disponibili per l'accreditamento degli organismi di certificazione a norma dell'articolo 43, paragrafo 1, e individuano le questioni fondamentali da prendere in considerazione;
- forniscono un quadro di riferimento per stabilire requisiti di accreditamento aggiuntivi quando l'accreditamento è gestito dall'organismo nazionale di accreditamento; e
- forniscono un quadro di riferimento per stabilire requisiti di accreditamento quando l'accreditamento è gestito dall'autorità di controllo.

Le linee-guida non costituiscono un manuale di procedure per l'accreditamento degli organismi di certificazione a norma del RGPD, né elaborano una nuova norma tecnica per l'accreditamento degli organismi di certificazione ai fini del RGPD.

Le presenti linee-guida sono rivolte ai seguenti soggetti:

- Stati membri, che devono garantire che gli organismi di certificazione siano accreditati dall'autorità di controllo e/o dall'organismo nazionale di accreditamento;
- organismi nazionali di accreditamento, che effettuano l'accreditamento degli organismi di certificazione a norma dell'articolo 43, paragrafo 1, lettera b);
- l'autorità di controllo competente, che specifica «requisiti aggiuntivi» rispetto a quelli di cui alla norma ISO/IEC 17065/2012[2], quando l'accreditamento è effettuato dall'organismo nazionale di accreditamento a norma dell'articolo 43, paragrafo 1, lettera b);
- il comitato europeo per la protezione dei dati, quando rilascia un parere e approva i requisiti di accreditamento dell'autorità di controllo competente, a norma dell'articolo 43, paragrafo 3, dell'articolo 70, paragrafo 1, lettera p) e dell'articolo 64, paragrafo 1, lettera c);
- l'autorità di controllo competente, che precisa i requisiti di accreditamento quando l'accreditamento è effettuato dall'autorità di controllo stessa, a norma dell'articolo 43, paragrafo 1, lettera a);
- altre parti interessate, quali i soggetti che si candidano a operare da organismi di certificazione o i proprietari di schemi di certificazione che definiscano criteri e procedure di certificazione[3].

[2] Organizzazione internazionale per la standardizzazione: Valutazione della conformità - Requisiti per organismi che certificano prodotti, processi e servizi.

[3] Il proprietario di uno schema di certificazione è un'organizzazione identificabile che ha stabilito i criteri di certificazione e i requisiti in base ai quali va valutata la conformità. L'accreditamento riguarda l'organismo che effettua le valutazioni della conformità (articolo 43, paragrafo 4) sulla base dei requisiti dello schema di certificazione e rilascia i relativi certificati (ossia l'organismo di certificazione, noto anche come organismo di

Definizioni

Le seguenti definizioni mirano a promuovere un'interpretazione comune degli elementi fondamentali del processo di accreditamento. Devono essere considerate come punti di riferimento e non hanno alcuna pretesa di insindacabilità. Queste definizioni si basano sui quadri regolamentari e sulle norme esistenti, in particolare sulle disposizioni pertinenti del RGPD e della norma ISO/IEC 17065/2012.

Ai fini delle presenti linee-guida, si applicano le seguenti definizioni:

per «*accreditamento*» degli organismi di certificazione: si rimanda alla sezione 3 sull'interpretazione dell'accreditamento ai fini dell'articolo 43 del RGPD;

per «*requisiti aggiuntivi*» si intendono i requisiti stabiliti dall'autorità di controllo competente e sulla base dei quali viene eseguito l'accreditamento[4];

per «*certificazione*» si intende la valutazione e l'attestazione imparziale di terza parte[5] in merito al comprovato rispetto dei criteri di certificazione;

per «*organismo di certificazione*» si intende un organismo terzo di valutazione della conformità[6] che gestisce[7] un meccanismo di certificazione[8];

per «*schema di certificazione*» si intende un sistema di certificazione relativo a prodotti, processi e servizi specifici ai quali si applicano gli stessi requisiti specifici, norme e procedure specifiche[9];

per «*criteri*» o *criteri di certificazione* si intendono i criteri in base ai quali viene effettuata una certificazione (ossia, la valutazione della conformità)[10];

per «*organismo nazionale di accreditamento*» si intende l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento, a norma del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[11].

valutazione della conformità). L'organismo che effettua le valutazioni potrebbe essere la stessa organizzazione che ha sviluppato lo schema di certificazione e ne è proprietaria, ma potrebbero sussistere accordi in base ai quali un'organizzazione è proprietaria dello schema e un'altra (o più di una) effettua le valutazioni.

[4] Articolo 43, paragrafi 1, 3 e 6.

[5] Si noti che, secondo la norma ISO 17000, l'attestazione di terza parte (certificazione) è "applicabile a tutti gli oggetti della valutazione della conformità" (5.5) "a eccezione degli organismi di valutazione della conformità stessi, ai quali è applicabile l'accreditamento" (5.6).

[6] L'attività di valutazione della conformità di terza parte è svolta da un'organizzazione indipendente dalla persona o dall'organizzazione che fornisce l'oggetto e da interessi da utilizzatore per l'oggetto stesso, cfr. ISO 17000, 2.4.

[7] Cfr. ISO 17000, 2.5: organismo che svolge servizi di valutazione della conformità; ISO 17011: organismo che svolge servizi di valutazione della conformità e che può essere oggetto di accreditamento; ISO 17065, 3.12.

[8] Articolo 42, paragrafi 1 e 5, del RGPD.

[9] Cfr. 3.9 in combinato disposto con l'allegato B della norma ISO 17065.

[10] Cfr. articolo 42, paragrafo 5.

[11] Cfr. articolo 2, punto 11, del regolamento n. 765/2008/CE.

3 INTERPRETAZIONE DI «ACCREDITAMENTO» AI FINI DELL'ARTICOLO 43 DEL RGPD

Il RGPD non fornisce una definizione di «accreditamento». L'articolo 2, paragrafo 10, del regolamento (CE) n. 765/2008, che stabilisce requisiti generali in materia di accreditamento, definisce l'accreditamento come segue:

«attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità».

Ai sensi della norma ISO/IEC 17011

«l'accreditamento indica l'attestazione da parte di terzi recante prova formale che un determinato organismo di valutazione della conformità ha le competenze necessarie per svolgere specifiche attività di valutazione della conformità».

L'articolo 43, paragrafo 1, dispone quanto segue:

«Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:

(a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;
(b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio conformemente alla norma ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.»

Per quanto riguarda il RGPD, i requisiti di accreditamento si baseranno su:

- la norma ISO/IEC 17065/2012 e i «requisiti aggiuntivi» stabiliti dall'autorità di controllo competente ai sensi dell'articolo 43, paragrafo 1, lettera b), quando l'accreditamento è effettuato dall'organismo nazionale di accreditamento e dall'autorità di controllo, quando essa stessa effettua l'accreditamento.

In entrambi i casi, i requisiti consolidati devono includere i requisiti di cui all'articolo 43, paragrafo 2.

Il comitato europeo per la protezione dei dati riconosce che lo scopo dell'accreditamento è fornire una dichiarazione autorevole della competenza di un determinato organismo a svolgere attività di certificazione (attività di valutazione della conformità)[12]. Per accreditamento, ai sensi del RGPD, si intende quanto segue:

[12] Cfr. considerando 15 del regolamento n. 765/2008/CE.

l'attestazione[13] da parte di un organismo nazionale di accreditamento e/o di un'autorità di controllo che un organismo di certificazione[14] è qualificato a effettuare la certificazione ai sensi degli articoli 42 e 43 del RGPD, tenendo conto della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo e/o dal Comitato.

4 ACCREDITAMENTO AI SENSI DELL'ARTICOLO 43, PARAGRAFO 1, DEL RGPD

L'articolo 43, paragrafo 1, riconosce l'esistenza di diverse opzioni per l'accreditamento degli organismi di certificazione. Il RGPD impone alle autorità di controllo e agli Stati membri di definire il processo di accreditamento degli organismi di certificazione. In questa sezione sono indicate le modalità di accreditamento di cui all'articolo 43.

4.1 Ruolo degli Stati membri

L'articolo 43, paragrafo 1, impone agli Stati membri di *garantire* che gli organismi di certificazione siano accreditati, ma consente a ciascuno Stato membro di determinare a chi spetti condurre la valutazione ai fini dell'accreditamento. Sulla base dell'articolo 43, paragrafo 1, sono disponibili tre opzioni; l'accreditamento è effettuato:

(1) esclusivamente dall'autorità di controllo, sulla base dei propri requisiti;
(2) esclusivamente dall'organismo nazionale di accreditamento, designato a norma del regolamento (CE) n. 765/2008 e in conformità della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo competente; oppure
(3) sia dall'autorità di controllo che dall'organismo nazionale di accreditamento (e conformemente a tutti i requisiti di cui al precedente punto 2).

Spetta al singolo Stato membro decidere se tali attività di accreditamento dovranno essere svolte dall'organismo nazionale di accreditamento, dall'autorità di controllo o da entrambi, ma in ogni caso lo Stato membro dovrebbe garantire che siano messe a disposizione risorse idonee[15].

4.2 Interazione con il regolamento (CE) n. 765/2008

Il comitato europeo per la protezione dei dati osserva che l'articolo 2, paragrafo 11, del regolamento (CE) n. 765/2008, definisce un organismo nazionale di accreditamento come «l'*unico* organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento».

L'articolo 2, paragrafo 11, potrebbe essere considerato in conflitto con l'articolo 43, paragrafo 1, del RGPD, che consente l'accreditamento da parte di un organismo diverso dall'organismo nazionale di accreditamento dello Stato membro. Il comitato europeo per la protezione dei dati ritiene che l'intenzione del legislatore UE sia stata quella di derogare al principio generale secondo cui l'accreditamento deve essere effettuato esclusivamente da un organismo nazionale di

[13] Cfr. articolo 2, punto 10, del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.
[14] Cfr. la definizione del termine «accreditamento» ai sensi della norma ISO 17011.
[15] Cfr. articolo 4, paragrafo 9, del regolamento (CE) n. 765/2008.

accreditamento, conferendo alle autorità di controllo lo stesso potere in materia di accreditamento degli organismi di certificazione. L'articolo 43, paragrafo 1, si caratterizza pertanto come *lex specialis* rispetto all'articolo 2, paragrafo 11, del regolamento (CE) n. 765/2008.

4.3 Il ruolo dell'organismo nazionale di accreditamento

L'articolo 43, paragrafo 1, lettera b), prevede che l'organismo nazionale di accreditamento accrediti gli organismi di certificazione conformemente alla norma ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente.

Per chiarezza, il comitato europeo per la protezione dei dati sottolinea che il riferimento specifico all'articolo 43, paragrafo 1, lettera b), nel testo del paragrafo 3 dello stesso articolo, implica che «tali requisiti» siano i «requisiti aggiuntivi» stabiliti dall'autorità di controllo competente ai sensi dell'articolo 43, paragrafo 1, lettera b), e i requisiti stabiliti all'articolo 43, paragrafo 2.

Nel processo di accreditamento, gli organismi nazionali di accreditamento applicano i requisiti aggiuntivi che devono essere forniti dalle autorità di controllo.

Un organismo di certificazione che sia già accreditato sulla base della norma ISO/IEC 17065/2012 per schemi di certificazione non relativi al RGPD, e che desideri estendere l'ambito del proprio accreditamento per includere la certificazione rilasciata in conformità del RGPD dovrà soddisfare i requisiti aggiuntivi stabiliti dall'autorità di controllo se l'accreditamento è gestito dall'organismo nazionale di accreditamento. Se l'accreditamento per la certificazione ai sensi del RGPD è offerto solo dall'autorità di controllo competente, un organismo di certificazione che faccia richiesta di accreditamento dovrà soddisfare i requisiti stabiliti dalla relativa autorità di controllo.

4.4 Il ruolo dell'autorità di controllo

Il comitato europeo per la protezione dei dati osserva che l'articolo 57, paragrafo 1, lettera q), stabilisce che l'autorità di controllo *effettua* l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43 in quanto «compito dell'autorità di controllo» ai sensi dell'articolo 57; e l'articolo 58, paragrafo 3, lettera e), stabilisce che l'autorità di controllo ha il potere autorizzativo e consultivo per accreditare gli organismi di certificazione a norma dell'articolo 43. La formulazione dell'articolo 43, paragrafo 1, offre una certa flessibilità e la funzione di accreditamento dell'autorità di controllo dovrebbe essere interpretata come un compito non tassativo. La legislazione degli Stati membri potrà chiarire questo punto. Tuttavia, nel processo di accreditamento da parte di un organismo nazionale di accreditamento, l'articolo 43, paragrafo 2, lettera a), impone all'organismo di certificazione di dimostrare in modo convincente all'autorità di controllo competente la propria indipendenza e competenza in rapporto all'oggetto del meccanismo di certificazione che esso offre[16].

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 da parte degli organismi nazionali di accreditamento, l'articolo 43 fornisce minori indicazioni in materia di requisiti per l'accreditamento nel caso in cui sia l'autorità di

[16] I requisiti aggiuntivi stabiliti dall'autorità di controllo ai sensi dell'articolo 43, paragrafo 1, lettera b), dovrebbero specificare i requisiti in materia di indipendenza e di competenza. Cfr. anche allegato 1 delle presenti Linee-guida.

controllo stessa a effettuare l'accreditamento. Al fine di contribuire ad un approccio armonizzato all'accreditamento, i requisiti di accreditamento utilizzati dall'autorità di controllo dovrebbero basarsi sulla norma ISO/IEC 17065 ed essere integrati dai requisiti aggiuntivi stabiliti da tale autorità di controllo ai sensi dell'articolo 43, paragrafo 1, lettera b). Il comitato europeo per la protezione dei dati osserva che l'articolo 43, paragrafo 2, lettere da a) ad e), rispecchia e precisa i requisiti di cui alla norma ISO 17065, contribuendo così alla coerenza.

Se uno Stato membro stabilisce che gli organismi di certificazione devono essere accreditati dagli organismi nazionali di accreditamento, l'autorità di controllo dovrebbe stabilire requisiti aggiuntivi che integrano le convenzioni di accreditamento esistenti previste dal regolamento (CE) n. 765/2008 (i cui articoli da 3 a 14 riguardano l'organizzazione e il funzionamento dell'accreditamento degli organismi di valutazione della conformità) e le norme tecniche che descrivono i metodi e le procedure degli organismi di certificazione. Alla luce di ciò, il regolamento (CE) n. 765/2008 fornisce ulteriori indicazioni: l'articolo 2, paragrafo 10, definisce l'accreditamento e fa riferimento a «norme armonizzate» e a «ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali». Ne consegue che i requisiti aggiuntivi stabiliti dall'autorità di controllo dovrebbero includere requisiti specifici ed essere incentrati sull'agevolazione della valutazione, tra l'altro, dell'indipendenza e del livello di competenza in materia di protezione dei dati degli organismi di certificazione - ad esempio la loro capacità di valutare e certificare le operazioni di trattamento dei dati personali da parte dei titolari e dei responsabili del trattamento ai sensi dell'articolo 42, paragrafo 1. Ciò include le competenze richieste per i programmi settoriali e per quanto riguarda la tutela dei diritti e delle libertà fondamentali delle persone fisiche e in particolare il loro diritto alla protezione dei dati personali[17]. L'allegato alle presenti linee-guida può aiutare le autorità di controllo competenti a stabilire i «requisiti aggiuntivi» ai sensi dell'articolo 43, paragrafo 1, lettera b), e dell'articolo 43, paragrafo 3.

L'articolo 43, paragrafo 6, stabilisce che «i requisiti di cui al paragrafo 3 del presente articolo e i criteri di certificazione di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in una forma facilmente accessibile». Pertanto, per garantire la trasparenza, tutti i criteri e i requisiti approvati da un'autorità di controllo devono essere pubblicati. In termini di qualità e fiducia negli organismi di certificazione, sarebbe auspicabile che tutti i requisiti per l'accreditamento fossero facilmente accessibili al pubblico.

4.5 Autorità di controllo che agisce in qualità di organismo di certificazione

L'articolo 42, paragrafo 5, stabilisce che un'autorità di controllo può rilasciare certificazioni, ma il RGPD non richiede che essa sia accreditata per soddisfare i requisiti di cui al regolamento (CE) n. 765/2008. Il comitato europeo per la protezione dei dati osserva che l'articolo 43, paragrafo 1, lettera a), e in particolare l'articolo 58, paragrafo 2, lettera h), e paragrafo 3, lettere a), e) ed f), autorizzano le autorità di controllo a effettuare sia l'accreditamento che la certificazione e, allo stesso tempo, a fornire consulenza e, se del caso, a revocare le certificazioni o a ingiungere agli organismi di certificazione di non rilasciare certificazioni.

Vi possono essere situazioni in cui è opportuno o necessario garantire la separazione dei ruoli e delle funzioni di accreditamento e di certificazione, ad esempio qualora in uno Stato membro vi siano

[17] Articolo 1, paragrafo 2, del RGPD.

un'autorità di controllo e altri organismi di certificazione che rilascino la stessa tipologia di certificazioni. Le autorità di controllo dovrebbero pertanto adottare misure organizzative atte a mantenere distinti i compiti che il RGPD individua al fine di rendere solidi e facilitare i meccanismi di certificazione, evitando al tempo stesso possibili conflitti di interesse derivanti dall'esecuzione di tali compiti. Inoltre, gli Stati membri e le autorità di controllo dovrebbero tenere conto del livello di armonizzazione europeo al momento di formulare la legislazione e le procedure nazionali in materia di accreditamento e certificazione in conformità del RGPD.

4.6 Requisiti di accreditamento

L'allegato alle presenti linee-guida fornisce indicazioni su come definire requisiti aggiuntivi di accreditamento. Individua le disposizioni pertinenti nel RGPD e suggerisce i requisiti che le autorità di controllo e gli organismi nazionali di accreditamento dovrebbero prendere in considerazione per garantire il rispetto del RGPD.

Come stabilito in precedenza, se gli organismi di certificazione sono accreditati dall'organismo nazionale di accreditamento ai sensi del regolamento (CE) n. 765/2008, la norma ISO/IEC 17065/2012 sarà la norma di accreditamento pertinente, integrata dai requisiti aggiuntivi stabiliti dall'autorità di controllo. L'articolo 43, paragrafo 2, rispecchia le disposizioni generali della norma ISO/IEC 17065/2012 alla luce della tutela dei diritti fondamentali ai sensi del RGPD. Il quadro di riferimento di cui all'allegato utilizza l'articolo 43, paragrafo 2, e la norma ISO/IEC 17065/2012 come base per l'individuazione dei requisiti, nonché ulteriori criteri relativi alla valutazione delle competenze in materia di protezione dei dati degli organismi di certificazione e della loro capacità di rispettare i diritti e le libertà delle persone fisiche con riguardo al trattamento dei dati personali, come sancito nel RGPD. Il comitato europeo per la protezione dei dati sottolinea la particolare attenzione prestata affinché sia garantito che gli organismi di certificazione dispongano di un livello adeguato di competenze riguardo alla protezione dei dati conformemente all'articolo 43, paragrafo 1.

I requisiti aggiuntivi di accreditamento stabiliti dall'autorità di controllo si applicheranno a tutti gli organismi di certificazione che richiederanno l'accreditamento. L'organismo di accreditamento valuterà se tale organismo di certificazione sia competente a svolgere l'attività di certificazione in linea con i requisiti aggiuntivi e l'oggetto della certificazione. Si dovranno indicare i settori o le aree di certificazione specifici per i quali l'organismo di certificazione è accreditato.

Il comitato europeo per la protezione dei dati rileva, inoltre, che tale particolare competenza nel campo della protezione dei dati, oltre al rispetto dei requisiti della norma ISO/IEC 17065/2012, è richiesta anche qualora altri soggetti esterni, quali laboratori o *auditor*, svolgano parti o elementi di attività di certificazione per conto di un organismo di certificazione accreditato. In questi casi, non è previsto l'accreditamento di tali soggetti esterni ai sensi del RGPD stesso. Tuttavia, al fine di garantire l'idoneità di tali soggetti a svolgere attività per conto degli organismi di certificazione accreditati, è necessario che l'organismo di certificazione accreditato garantisca che anche il soggetto esterno disponga in modo dimostrabile delle competenze in materia di protezione dei dati richieste per l'organismo accreditato in relazione alla specifica attività svolta.

Il quadro per l'identificazione dei requisiti di accreditamento aggiuntivi presentato in allegato alle presenti linee-guida non costituisce un manuale di procedure ai fini dell'accreditamento effettuato dall'organismo nazionale di accreditamento o dall'autorità di controllo. Esso fornisce indicazioni

strutturali e metodologiche alle autorità di controllo, offrendo pertanto una serie di strumenti per individuare i requisiti aggiuntivi ai fini dell'accreditamento.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)