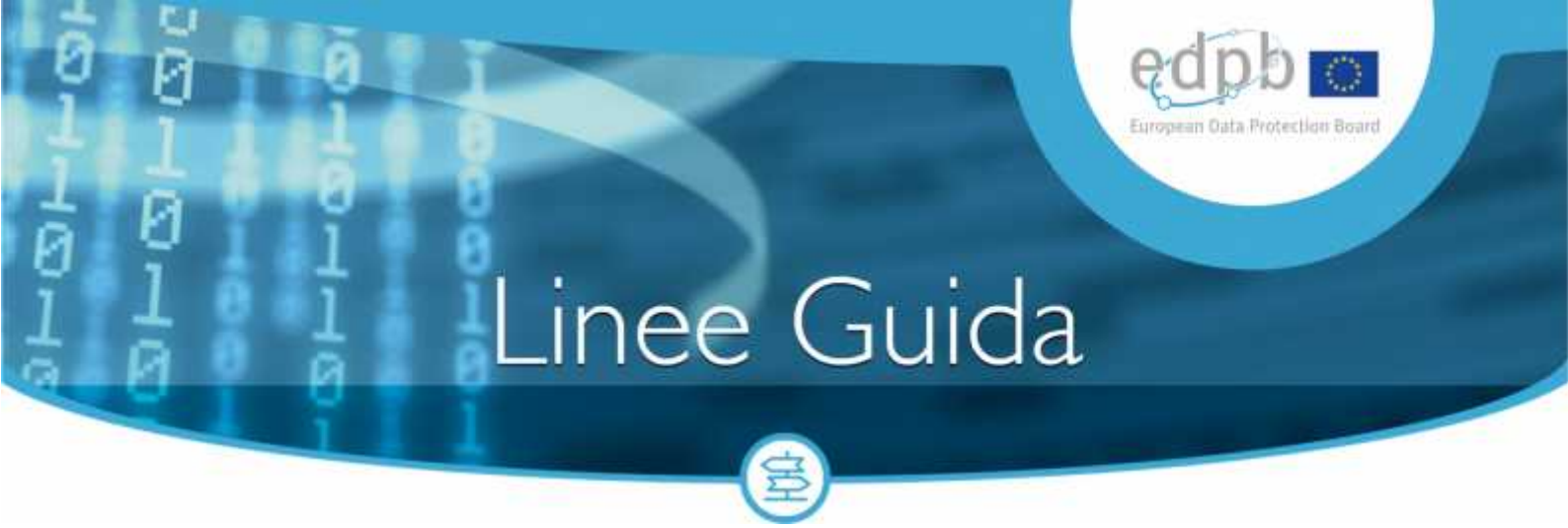

Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679)

Versione 3.0

4 giugno 2019

Adottato

Storico delle versioni

Versione 3.0	4 giugno 2019	Aggiunta dell'allegato 1 (versione 2.0 dell'allegato 1 adottata il 4 giugno 2019 a seguito della consultazione pubblica)
Versione 2.0	4 dicembre 2018	Adozione delle linee guida a seguito della consultazione pubblica — Nella stessa data l'allegato 1 (versione 1.0) è stato adottato per la consultazione pubblica
Versione 1.0	6 febbraio 2018	Adozione delle linee guida da parte del Gruppo di lavoro Articolo 29 (versione per la consultazione pubblica). Tale versione è stata approvata dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

Indice

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), 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,

tenuto conto dei risultati della consultazione pubblica sulle linee guida svoltasi a febbraio 2018 e della consultazione pubblica sull'allegato svoltasi tra il 14 dicembre 2018 e il 1º febbraio 2019 in conformità dell'articolo 70, paragrafo 4, del regolamento generale sulla protezione dei dati,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 INTRODUZIONE

1. Il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) (nel prosieguo "il regolamento"), applicabile dal 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 regolamento generale sulla protezione dei dati. 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.

2. Nell'ambito dell'istituzione di meccanismi di certificazione e di sigilli e marchi di protezione dei dati, l'articolo 43, paragrafo 1, del regolamento generale sulla protezione dei dati impone agli Stati membri di garantire che gli organismi di certificazione che rilasciano certificazioni a norma 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.

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

[1] Il considerando 100 del regolamento generale sulla protezione dei dati 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.

4. 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.

5. Le presenti linee guida mirano a fornire indicazioni sull'interpretazione e l'attuazione delle disposizioni di cui all'articolo 43 del regolamento generale sulla protezione dei dati. 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 armonizzato per l'accreditamento degli organismi di certificazione che rilasciano certificazioni in conformità del regolamento generale sulla protezione dei dati.

2 AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

6. Le presenti linee guida:

- definiscono l'obiettivo dell'accreditamento nel contesto del regolamento generale sulla protezione dei dati;
- 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.

7. Le linee guida non costituiscono un manuale di procedure per l'accreditamento degli organismi di certificazione a norma del regolamento generale sulla protezione dei dati, né elaborano una nuova norma tecnica per l'accreditamento degli organismi di certificazione ai fini del regolamento generale sulla protezione dei dati.

8. 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);

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

- 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].

9. Definizioni

10. 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 regolamento generale sulla protezione dei dati e della norma ISO/IEC 17065/2012.

11. Ai fini delle presenti linee guida si applicano le seguenti definizioni:

12. per "accreditamento" degli organismi di certificazione: si rimanda alla sezione 3 sull'interpretazione dell'accreditamento ai fini dell'articolo 43 del regolamento generale sulla protezione dei dati;

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

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

15. per "organismo di certificazione" si intende un organismo terzo di valutazione della conformità[6] che gestisce[7] un meccanismo di certificazione[8];

16. 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];

---

[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 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 regolamento generale sulla protezione dei dati.

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

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

18. 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].

3 INTERPRETAZIONE DI "ACCREDITAMENTO" AI FINI DELL'ARTICOLO 43 DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

19. Il regolamento generale sulla protezione dei dati non fornisce una definizione di "accreditamento". L'articolo 2, punto 10, del regolamento (CE) n. 765/2008, che stabilisce requisiti generali in materia di accreditamento, definisce l'accreditamento come segue:

20. "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".

21. Ai sensi della norma ISO/IEC 17011

22. "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".

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

24. "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 a norma 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 a norma degli articoli 55 o 56".

25. Per quanto riguarda il regolamento generale sulla protezione dei dati, i requisiti di accreditamento si baseranno su:

[10] Cfr. articolo 42, paragrafo 5.
[11] Cfr. articolo 2, punto 11, del regolamento (CE) n. 765/2008.

- la norma ISO/IEC 17065/2012 e i "requisiti aggiuntivi" stabiliti dall'autorità di controllo competente in conformità 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.

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

27. 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 regolamento generale sulla protezione dei dati, si intende quanto segue:

28. 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 regolamento generale sulla protezione dei dati, tenendo conto della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo e/o dal Comitato.

4 ACCREDITAMENTO IN CONFORMITÀ DELL'ARTICOLO 43, PARAGRAFO 1, DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

29. L'articolo 43, paragrafo 1, riconosce l'esistenza di diverse opzioni per l'accreditamento degli organismi di certificazione. Il regolamento generale sulla protezione dei dati 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

30. 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

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

(3) sia dall'autorità di controllo che dall'organismo nazionale di accreditamento (e conformemente a tutti i requisiti di cui al precedente punto 2).

31. 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

32. Il Comitato europeo per la protezione dei dati osserva che l'articolo 2, punto 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".

33. L'articolo 2, punto 11, potrebbe essere considerato in conflitto con l'articolo 43, paragrafo 1, del regolamento generale sulla protezione dei dati, 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 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, punto 11, del regolamento (CE) n. 765/2008.

4.3 Il ruolo dell'organismo nazionale di accreditamento

34. 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.

35. 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 all'articolo 43, paragrafo 1, lettera b), e i requisiti stabiliti all'articolo 43, paragrafo 2.

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

37. Un organismo di certificazione che sia già accreditato sulla base della norma ISO/IEC 17065/2012 per schemi di certificazione non relativi al regolamento generale sulla protezione dei dati e che desideri estendere l'ambito del proprio accreditamento per includere la certificazione rilasciata in conformità del regolamento generale sulla protezione dei dati 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 a norma del regolamento generale sulla protezione dei dati 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.

[15] Cfr. articolo 4, paragrafo 9, del regolamento (CE) n. 765/2008.

4.4 Il ruolo dell'autorità di controllo

38. 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 a norma dell'articolo 43 in quanto "compito dell'autorità di controllo" a norma 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].

39. 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 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 17065/2012 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/IEC 17065/2012, contribuendo così alla coerenza.

40. 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, punto 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 del trattamento e dei responsabili del trattamento a norma 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

[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 l'allegato 1 delle presenti linee guida.

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" in conformità dell'articolo 43, paragrafo 1, lettera b), e dell'articolo 43, paragrafo 3.

41. 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

42. L'articolo 42, paragrafo 5, stabilisce che un'autorità di controllo può rilasciare certificazioni, ma il regolamento generale sulla protezione dei dati 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.

43. 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 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 regolamento generale sulla protezione dei dati 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 regolamento generale sulla protezione dei dati.

4.6 Requisiti di accreditamento

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

45. Come stabilito in precedenza, se gli organismi di certificazione sono accreditati dall'organismo nazionale di accreditamento a norma 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 contemplata dal regolamento generale sulla protezione dei dati. Il quadro di riferimento di cui all'allegato utilizza l'articolo 43, paragrafo 2, e la norma ISO/IEC 17065/2012 come base per

[17] Articolo 1, paragrafo 2, del regolamento generale sulla protezione dei dati.

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 regolamento generale sulla protezione dei dati. 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.

46. 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.

47. 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 a norma del regolamento generale sulla protezione dei dati 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.

48. 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.

ALLEGATO 1

L'allegato 1 fornisce orientamenti per la definizione di requisiti di accreditamento "aggiuntivi" con riguardo alla norma ISO/IEC 17065/2012 e in conformità dell'articolo 43, paragrafo 1, lettera b), e dell'articolo 43, paragrafo 3, del regolamento generale sulla protezione dei dati.

Il presente allegato delinea i requisiti consigliati che un'autorità di controllo in materia di protezione dei dati dovrebbe elaborare e che si applicano durante l'accreditamento di un organismo di certificazione da parte dell'organismo nazionale di accreditamento o dell'autorità di controllo competente[18]. Tali requisiti aggiuntivi devono essere comunicati al Comitato europeo per la protezione dei dati prima dell'approvazione a norma dell'articolo 64, paragrafo 1, lettera c).

Il presente allegato è da leggersi congiuntamente alla norma ISO/IEC 17065/2012. I numeri delle sezioni utilizzati nel presente allegato corrispondono a quelli utilizzati nella norma ISO/IEC 17065/2012. Qualora le autorità di controllo effettuino l'accreditamento in conformità dell'articolo 43, paragrafo 1, lettera a), sarebbe buona norma applicare il presente approccio, laddove fattibile. In tal modo si favorirà un accreditamento armonizzato a livello dell'UE.

Indipendentemente dagli orientamenti qui forniti o dall'assenza di orientamenti su qualsiasi punto della norma ISO/IEC 17065/2012, l'autorità di controllo competente ha facoltà di formulare ulteriori requisiti aggiuntivi su tali punti, purché siano conformi al diritto nazionale.

0 PREMESSA

[La presente sezione è dedicata a eventuali termini di collaborazione, laddove applicabili, concordati tra l'organismo nazionale di accreditamento e l'autorità di controllo in materia di protezione dei dati, volti a definire ad esempio il soggetto responsabile della ricezione delle domande o l'organizzazione del riconoscimento dei criteri approvati nel quadro del processo di accreditamento.]

1 AMBITO DI APPLICAZIONE[19]

L'ambito di applicazione della norma ISO/IEC 17065/2012 è definito in conformità del regolamento generale sulla protezione dei dati. Ulteriori informazioni sono riportate nelle linee guida relative all'accreditamento e alla certificazione. L'ambito di applicazione di un meccanismo di certificazione (ad esempio la certificazione dei trattamenti di un servizio in cloud) dovrebbe essere tenuto in considerazione nella valutazione svolta dall'organismo nazionale di accreditamento e dall'autorità di controllo competente durante il processo di accreditamento, in particolare per quanto riguarda i criteri, le competenze e la metodologia di valutazione. L'ampio ambito di applicazione della norma ISO/IEC 17065/2012, che si estende a prodotti, processi e servizi, non dovrebbe abbassare i requisiti del regolamento generale sulla protezione dei dati o prevalere sugli stessi; per esempio un meccanismo di governance non può rappresentare l'unico elemento di un meccanismo di certificazione, poiché la certificazione deve contemplare il trattamento di dati personali, ossia operazioni di trattamento. A norma dell'articolo 42, paragrafo 1, la certificazione in conformità del regolamento generale sulla

[18] Per informazioni sul processo di approvazione dei criteri di certificazione si veda la sezione 4 delle linee guida relative alla certificazione.
[19] La numerazione si riferisce alla norma ISO/IEC 17065/2012.

protezione dei dati è applicabile solo ai trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

2 RIFERIMENTI NORMATIVI

Il regolamento generale sulla protezione dei dati prevale sulla norma ISO/IEC 17065/2012. Qualora i requisiti aggiuntivi o il meccanismo di certificazione facciano riferimento ad altre norme ISO, esse dovranno essere interpretate in linea con i requisiti fissati nel regolamento generale sulla protezione dei dati.

3 TERMINI E DEFINIZIONI

Nel contesto del presente allegato si applicano i termini e le definizioni delle linee guida relative all'accreditamento (WP 261) e alla certificazione (EDPB 1/2018). Tali termini e definizioni prevalgono sulle definizioni dell'ISO.

4 REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO

4.1 Aspetti giuridici e contrattuali

4.1.1 Responsabilità giuridica

Un organismo di certificazione dovrebbe essere in grado di dimostrare (in qualsiasi momento) all'organismo nazionale di accreditamento o all'autorità di controllo competente di disporre di procedure aggiornate atte a comprovare la conformità alle responsabilità giuridiche fissate nei termini di accreditamento, compresi i requisiti aggiuntivi con riguardo all'applicazione del regolamento (UE) 2016/679. Si noti che l'organismo di certificazione, essendo esso stesso un titolare del trattamento/responsabile del trattamento dei dati, dovrà essere in grado di fornire prove dell'esistenza di procedure e misure conformi al regolamento (UE) 2016/679 specificamente finalizzate al controllo e alla gestione dei dati personali dell'organizzazione cliente nel quadro del processo di certificazione.

L'autorità di controllo competente può decidere di integrare ulteriori requisiti e procedure per verificare la conformità degli organismi di certificazione al regolamento generale sulla protezione dei dati prima dell'accreditamento.

4.1.2 Accordo di certificazione

I requisiti minimi di un accordo di certificazione dovranno essere integrati con i punti seguenti.

L'organismo di certificazione dovrà dimostrare, oltre al rispetto dei requisiti della norma ISO/IEC 17065/2012, che i propri accordi di certificazione:

1. impongono al richiedente di ottemperare sempre sia ai requisiti generici di certificazione ai sensi del punto 4.1.2.2, lettera a, della norma ISO/IEC 17065/2012, sia ai criteri approvati dall'autorità di controllo competente o dal Comitato europeo per la protezione dei dati in conformità dell'articolo 43, paragrafo 2, lettera b), e dell'articolo 42, paragrafo 5;
2. impongono al richiedente di garantire nei confronti dell'autorità di controllo competente la piena trasparenza della procedura di certificazione, compresi gli aspetti contrattuali

riservati relativi alla conformità in materia di protezione dei dati a norma dell'articolo 42, paragrafo 7, e dell'articolo 58, paragrafo 1, lettera c);

3. non riducono la responsabilità del richiedente in merito alla conformità al regolamento (UE) 2016/679 e lasciano impregiudicati i compiti e i poteri dell'autorità di controllo competente in linea con l'articolo 42, paragrafo 5;
4. impongono al richiedente di fornire all'organismo di certificazione tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione a norma dell'articolo 42, paragrafo 6;
5. impongono al richiedente di rispettare tutte le scadenze e le procedure applicabili. Nell'accordo di certificazione devono essere pattuite le scadenze e le procedure derivanti ad esempio dal programma di certificazione o da altre normative che devono essere osservate e rispettate;
6. con riguardo al punto 4.1.2.2, lettera c), n. 1, della norma ISO/IEC 17065/2012, fissano norme sulla validità, sul rinnovo e sulla revoca in conformità dell'articolo 42, paragrafo 7, e dell'articolo 43, paragrafo 4, comprese norme atte a definire congrui intervalli per la rivalutazione o il riesame (periodicità) in linea con l'articolo 42, paragrafo 7;
7. consentono all'organismo di certificazione di divulgare tutte le informazioni necessarie al rilascio della certificazione a norma dell'articolo 42, paragrafo 8, e dell'articolo 43, paragrafo 5;
8. contemplano norme in merito alle precauzioni necessarie per le indagini sui reclami ai sensi del punto 4.1.2.2, lettera c), n. 2, e inoltre, in conformità della lettera j, contengono indicazioni esplicite sulla struttura e sulla procedura per la gestione dei reclami in conformità dell'articolo 43, paragrafo 2, lettera d);
9. oltre a soddisfare i requisiti minimi di cui al punto 4.1.2.2 della norma ISO/IEC 17065/2012, disciplinano anche, se presenti, tutte le conseguenze della revoca o della sospensione dell'accreditamento relativo all'organismo di certificazione che si ripercuotono sul cliente;
10. impongono al richiedente di informare l'organismo di certificazione in caso di modifiche significative della propria situazione effettiva o giuridica e dei propri prodotti, processi e servizi coperti dalla certificazione.

4.1.3 Utilizzo di sigilli e marchi di protezione dei dati

I certificati, i marchi e i sigilli dovranno essere usati esclusivamente in conformità degli articoli 42 e 43 e delle linee guida relative all'accreditamento e alla certificazione.

4.2 Gestione dell'imparzialità

L'organismo di accreditamento dovrà garantire che, oltre a soddisfare il requisito di cui al punto 4.2 della norma ISO/IEC 17065/2012,

1. l'organismo di certificazione sia conforme ai requisiti aggiuntivi dell'autorità di controllo competente (a norma dell'articolo 43, paragrafo 1, lettera b)), ossia che
    - **a.** fornisca evidenze separate della propria indipendenza in linea con l'articolo 43, paragrafo 2, lettera a). Ciò si applica in particolare alle evidenze relative al finanziamento dell'organismo di certificazione, nella misura in cui sono pertinenti rispetto alla garanzia d'imparzialità;
    - **b.** i suoi compiti e le sue funzioni non diano adito a un conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e);

2. l'organismo di certificazione non abbia alcun collegamento rilevante con il cliente che valuta.

4.3 Responsabilità e finanziamento

L'organismo di accreditamento dovrà assicurarsi periodicamente che l'organismo di certificazione, oltre a rispettare il requisito di cui al punto 4.3.1 della norma ISO/IEC 17065/2012, disponga di idonee misure (ad esempio un'assicurazione o riserve finanziarie) tali da coprire le proprie responsabilità nelle aree geografiche in cui opera.

4.4 Condizioni non discriminatorie

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi, purché conformi al diritto nazionale.

4.5 Riservatezza

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi, purché conformi al diritto nazionale.

4.6 Informazioni disponibili al pubblico

Oltre al rispetto del requisito di cui al punto 4.6 della norma ISO/IEC 17065/2012 l'organismo di accreditamento dovrà esigere dall'organismo di certificazione almeno che:

1. tutte le versioni (attuali e precedenti) dei criteri approvati utilizzati ai sensi dell'articolo 42, paragrafo 5, così come tutte le procedure di certificazione, siano pubblicate e facilmente accessibili al pubblico, con indicazione generale del rispettivo periodo di validità;
2. le informazioni sulle procedure di gestione dei reclami e sui ricorsi siano rese pubbliche a norma dell'articolo 43, paragrafo 2, lettera d).

5 REQUISITI STRUTTURALI - ARTICOLO 43, PARAGRAFO 4 ("CORRETTA" VALUTAZIONE)

5.1 Struttura organizzativa e alta direzione

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi.

5.2 Meccanismi di salvaguardia dell'imparzialità

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi.

6 REQUISITI PER LE RISORSE

6.1 Personale dell'organismo di certificazione

L'organismo di accreditamento dovrà garantire che il personale di ogni organismo di certificazione, oltre a rispettare il requisito di cui alla sezione 6 della norma ISO/IEC 17065/2012,

1. abbia dimostrato adeguate e attuali competenze (insieme di conoscenze ed esperienze) riguardo alla protezione dei dati a norma dell'articolo 43, paragrafo 1;
2. sia indipendente e attualmente competente riguardo all'oggetto della certificazione a norma dell'articolo 43, paragrafo 2, lettera a), e non presenti alcun conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e);
3. si impegni a rispettare i criteri di cui all'articolo 42, paragrafo 5, a norma dell'articolo 43, paragrafo 2, lettera b);

4. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda l'applicazione della legislazione in materia di protezione dei dati;
5. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda le pertinenti misure tecniche e organizzative di protezione dei dati;
6. sia in grado di dimostrare di avere esperienza nei settori menzionati nei requisiti aggiuntivi di cui ai punti 6.1.1, 6.1.4 e 6.1.5, nello specifico

Per il personale con competenze tecniche:

- di avere ottenuto una qualifica in un pertinente settore di competenza tecnica pari ad almeno il livello 6 dell'EQF[20] o un titolo protetto riconosciuto (p. es. Dipl. Ing.) per la pertinente professione regolamentata, oppure di disporre di significativa esperienza professionale.
- Al *personale responsabile delle decisioni relative alla certificazione* è richiesta una significativa esperienza professionale nell'identificazione e nell'attuazione delle misure di protezione dei dati.
- Al *personale responsabile delle valutazioni* è richiesta un'esperienza professionale nell'ambito della protezione tecnica dei dati e conoscenze ed esperienze in materia di procedure comparabili (p. es. certificazioni/audit), nonché, se del caso, di essere iscritto in un albo.

Il personale dovrà dimostrare di mantenere conoscenze specifiche del settore nell'ambito delle competenze tecniche e di audit mediante formazione permanente documentata.

Per il personale con competenze giuridiche:

- studi giuridici in un'università dell'UE o riconosciuta da uno stato di durata pari ad almeno otto semestri, compresa una specializzazione post-laurea (LL.M) o titoli equivalenti, oppure significativa esperienza professionale.
- Il *personale responsabile delle decisioni relative alla certificazione* dovrà dimostrare una significativa esperienza professionale nell'ambito del diritto della protezione dei dati ed essere iscritto in un albo in conformità degli obblighi vigenti nello Stato membro.
- Il *personale responsabile delle valutazioni* dovrà dimostrare almeno due anni di esperienza professionale nell'ambito del diritto della protezione dei dati, e conoscenze ed esperienze in materia di procedure comparabili (p. es. certificazioni/audit), nonché essere iscritto in un albo, laddove nello Stato membro viga tale obbligo.
    - Il personale dovrà dimostrare di mantenere conoscenze specifiche del settore nell'ambito delle competenze tecniche e di audit mediante formazione permanente documentata.

6.2 Risorse per la valutazione

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi, purché conformi al diritto nazionale.

[20] Cfr. lo strumento di confronto dei quadri delle qualifiche, disponibile all'indirizzo https://ec.europa.eu/ploteus/en/compare?

7 REQUISITI DI PROCESSO - ARTICOLO 43, PARAGRAFO 2, LETTERE C) E D)

7.1 Aspetti generali

Oltre al rispetto del requisito di cui al punto 7.1 della norma ISO/IEC 17065/2012, l'organismo di accreditamento dovrà essere tenuto a garantire quanto segue:

1. nel presentare la domanda gli organismi di certificazione soddisfano i requisiti aggiuntivi dell'autorità di controllo competente (a norma dell'articolo 43, paragrafo 1, lettera b)), in modo tale che i compiti e le funzioni da loro svolti non diano adito a conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e);
2. vengono informate le autorità di controllo interessate prima che un organismo di certificazione cominci a utilizzare in un nuovo Stato membro, attraverso una sede distaccata di tale organismo, un sigillo europeo di protezione dei dati precedentemente approvato.

7.2 Domanda

Oltre a quanto previsto dal punto 7.2 della norma ISO/IEC 17065/2012, dovrebbe essere richiesto quanto segue:

1. l'oggetto della certificazione (Oggetto della Valutazione, ODV) deve essere descritto in dettaglio nella domanda. Ciò comprende anche le interfacce e i trasferimenti ad altri sistemi ed organizzazioni, i protocolli e le altre garanzie;
2. nella domanda dovrà essere specificato l'eventuale ricorso a responsabili del trattamento e, qualora il richiedente sia un responsabile del trattamento, si dovranno descrivere i suoi compiti e le sue responsabilità, nonché riportare nella domanda il/i pertinente/i contratto/i tra titolare del trattamento e responsabile del trattamento.

7.3 Riesame della domanda

Oltre a quanto previsto dal punto 7.3 della norma ISO/IEC 17065/2012, dovrebbe essere richiesto quanto segue:

1. nell'accordo di certificazione dovranno essere stabiliti metodi di valutazione vincolanti con riguardo all'oggetto della valutazione (ODV).
2. la valutazione di cui al punto 7.3, lettera e), in merito alla presenza di competenze sufficienti dovrà tenere conto in misura adeguata sia delle competenze tecniche sia delle competenze giuridiche in materia di protezione dei dati.

7.4 Valutazione

Oltre a quanto previsto dal punto 7.4 della norma ISO/IEC 17065/2012, i meccanismi di certificazione dovranno descrivere metodi di valutazione sufficienti a valutare la conformità del/i trattamento/i ai criteri di certificazione, tra cui ad esempio, laddove applicabili:

1. un metodo per valutare la necessità e la proporzionalità dei trattamenti rispetto al loro scopo e agli interessati;
2. un metodo per valutare la copertura, la composizione e la valutazione di tutti i rischi presi in considerazione dal titolare del trattamento e dal responsabile del trattamento con riguardo alle conseguenze giuridiche a norma degli articoli 30, 32, 35 e 36 del regolamento generale sulla protezione dei dati e alla definizione delle misure tecniche e organizzative a

norma degli articoli 24, 25 e 32 del regolamento, nella misura in cui i suddetti articoli si applicano all'oggetto della certificazione;

3. un metodo per valutare i rimedi giuridici, incluse le garanzie, le tutele e le procedure atte ad assicurare la protezione dei dati personali nell'ambito del trattamento collegato all'oggetto della certificazione nonché a dimostrare il rispetto dei requisiti giuridici definiti nei criteri; e
4. la documentazione di metodi e risultanze.

All'organismo di certificazione dovrebbe essere richiesto di garantire che tali metodi di valutazione siano standardizzati e applicabili in linea generale. Ciò significa che metodi di valutazione comparabili sono utilizzati per oggetti di valutazione (ODV) comparabili. Qualsiasi deroga a tale procedura dovrà essere motivata dall'organismo di certificazione.

Oltre a quanto previsto dal punto 7.4.2 della norma ISO/IEC 17065/2012, dovrebbe essere ammessa la possibilità di affidare l'esecuzione della valutazione ad esperti esterni riconosciuti dall'organismo di certificazione.

Oltre a quanto previsto dal punto 7.4.5 della norma ISO/IEC 17065/2012, dovrebbe essere prevista la possibilità che una certificazione in conformità degli articoli 42 e 43 del regolamento e che già copre parte dell'oggetto della certificazione sia ricompresa in una certificazione preesistente. Tuttavia non basterà sostituire integralmente valutazioni (parziali). L'organismo di certificazione sarà tenuto a verificare la conformità ai criteri. Il riconoscimento dovrà in ogni caso avvenire sulla base di una relazione di valutazione completa o di informazioni tali da consentire una valutazione della precedente attività di certificazione e dei suoi risultati. Una dichiarazione di certificazione o analoghi attestati di certificazione non saranno considerati sufficienti a sostituire una relazione.

Oltre a quanto previsto dal punto 7.4.6 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a specificare nel proprio meccanismo di certificazione in che modo sono fornite al cliente (il soggetto che presenta la domanda di certificazione) le informazioni obbligatorie a norma del punto 7.4.6 in merito alle non conformità al meccanismo di certificazione. In tale contesto dovrebbero essere definite almeno la natura e le tempistiche di tali informazioni.

Oltre a quanto previsto dal punto 7.4.9 della norma ISO/IEC 17065/2012, la documentazione dovrebbe essere resa pienamente accessibile, su richiesta, all'autorità di controllo in materia di protezione dei dati.

7.5 Riesame

Oltre a quanto previsto dal punto 7.5 della norma ISO/IEC 17065/2012, sono richieste procedure per la concessione, il riesame periodico e la revoca delle rispettive certificazioni a norma dell'articolo 43, paragrafo 2, e dell'articolo 43, paragrafo 3.

7.6 Decisione relativa alla certificazione

Oltre a quanto previsto dal punto 7.6.1 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a specificare nelle procedure in che modo garantisce la propria indipendenza e responsabilità rispetto alle singole decisioni di rilascio di certificazione.

7.7 Documentazione riguardante la certificazione

Oltre a quanto previsto dal punto 7.7.1, lettera e), della norma ISO/IEC 17065/2012 e in conformità dell'articolo 42, paragrafo 7, del regolamento generale sulla protezione dei dati il periodo di validità delle certificazioni non dovrebbe essere superiore a tre anni.

Oltre a quanto previsto dal punto 7.7.1, lettera e), della norma ISO/IEC 17065/2012, dovrebbe essere obbligatoriamente documentato anche il periodo del monitoraggio previsto ai sensi del punto 7.9.

Oltre a quanto previsto dal punto 7.7.1, lettera f), della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a denominare l'oggetto della certificazione all'interno della relativa documentazione (indicando la versione o altre caratteristiche analoghe, laddove applicabili).

7.8 Elenco dei prodotti certificati

Oltre a quanto previsto dal punto 7.8 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a conservare le informazioni riguardanti i prodotti, i processi e i servizi certificati in modo che siano disponibili sia al personale interno sia al pubblico. L'organismo di certificazione fornirà al pubblico una sintesi della relazione di valutazione. Scopo di tale sintesi è contribuire a una maggiore trasparenza sull'oggetto della certificazione e sulle modalità della rispettiva valutazione. La sintesi illustrerà tra l'altro:

(a) l'ambito della certificazione e una descrizione significativa dell'oggetto della certificazione (ODV),

(b) i rispettivi criteri di certificazione (inclusa la versione o lo stato funzionale),

(c) i metodi di valutazione e i test effettuati, nonché

(d) i(l) risultato/i.

Oltre a quanto previsto dal punto 7.8 della norma ISO/IEC 17065/2012 e a norma dell'articolo 43, paragrafo 5, del regolamento generale sulla protezione dei dati, l'organismo di certificazione dovrà informare l'autorità di controllo competente in merito ai motivi del rilascio o della revoca della certificazione richiesta.

7.9 Sorveglianza

Oltre a quanto previsto dai punti 7.9.1, 7.9.2 e 7.9.3 della norma ISO/IEC 17065/2012 e in conformità dell'articolo 43, paragrafo 2, lettera c), del regolamento generale sulla protezione dei dati, dovrebbero essere previste in via obbligatoria misure di monitoraggio periodico al fine del mantenimento della certificazione durante il periodo di monitoraggio.

7.10 Modifiche che influenzano la certificazione

Oltre a quanto previsto dai punti 7.10.1 e 7.10.2 della norma ISO/IEC 17065/2012, tra le modifiche che influenzano la certificazione di cui l'organismo di certificazione deve tenere conto rientrano: le modifiche alla legislazione in materia di protezione dei dati, l'adozione di atti delegati della Commissione europea in conformità dell'articolo 43, paragrafi 8 e 9, le decisioni del Comitato europeo per la protezione dei dati e le decisioni giurisprudenziali in materia di protezione dei dati. Le procedure di modifica da concordare in questo caso potrebbero prevedere ad esempio: periodi transitori, processi di approvazione da parte dell'autorità di controllo competente, nuova valutazione dell'oggetto della certificazione ove pertinente e misure adeguate per la revoca della certificazione qualora il trattamento certificato non sia più conforme ai criteri aggiornati.

7.11 Rescissione, riduzione, sospensione o revoca della certificazione

Oltre a quanto previsto dal punto 7.11.1 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a informare immediatamente e per iscritto l'autorità di controllo competente e l'organismo nazionale di accreditamento, se pertinente, in merito alle misure messe in atto e al mantenimento, alla limitazione, alla sospensione e alla revoca delle certificazioni.

In conformità dell'articolo 58, paragrafo 2, lettera h), l'organismo di certificazione sarà tenuto ad accettare decisioni e prescrizioni dell'autorità di controllo competente che gli ingiungano di revocare o non rilasciare la certificazione a un cliente (richiedente) se i requisiti per la certificazione non sono o non sono più soddisfatti.

7.12 Registrazioni

L'organismo di certificazione dovrebbe essere tenuto a conservare tutta la documentazione in forma completa, comprensibile, aggiornata e verificabile.

7.13 Reclami e ricorsi, articolo 43, paragrafo 2, lettera d)

Oltre a quanto previsto dal punto 7.13.1 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a definire:

(a) i soggetti che possono presentare reclami od obiezioni,

(b) i soggetti che trattano tali reclami e obiezioni, lato organismo di certificazione

(c) le verifiche effettuate in tale contesto,

(d) le possibilità di consultazione delle parti interessate.

Oltre a quanto previsto dal punto 7.13.2 della norma ISO/IEC 17065/2012, l'organismo di certificazione dovrebbe essere tenuto a definire:

(a) come e a chi dovrà essere trasmessa la conferma,

(b) i limiti temporali per la trasmissione della stessa,

(c) i processi che saranno avviati in seguito.

Oltre a quanto previsto dal punto 7.13.1 della norma ISO/IEC 17065/2012, l'organismo di certificazione è tenuto a definire le modalità con cui garantisce la separazione tra le attività di certificazione e la gestione di ricorsi e reclami.

8 REQUISITI DEL SISTEMA DI GESTIONE

Un requisito generale del sistema di gestione in conformità della sezione 8 della norma ISO/IEC 17065/2012 è la necessità di documentare, valutare, controllare e monitorare in maniera indipendente l'attuazione di tutti i requisiti derivanti dalle precedenti sezioni nell'ambito dell'applicazione del meccanismo di certificazione da parte dell'organismo di certificazione accreditato.

Il principio di base della gestione è la definizione di un sistema in base al quale gli obiettivi della stessa sono fissati in modo efficace ed efficiente, nello specifico: l'attuazione di servizi di certificazione, per mezzo di specifiche adeguate. Ciò presuppone la trasparenza e la verificabilità dell'attuazione dei requisiti di accreditamento da parte dell'organo di certificazione, nonché la conformità permanente agli stessi.

A tal fine il sistema di gestione deve specificare una metodologia per il soddisfacimento e il controllo di tali requisiti in conformità delle normative in materia di protezione dei dati, nonché per la loro verifica continua insieme allo stesso organismo accreditato.

Tali principi di gestione e la loro documentata attuazione devono essere trasparenti, nonché essere divulgati dall'organismo di certificazione accreditato nell'ambito della procedura di accreditamento a norma dell'articolo 58, e successivamente su richiesta dell'autorità di controllo in materia di protezione dei dati durante eventuali indagini condotte a titolo di revisione in materia di protezione dei dati a

norma dell'articolo 58, paragrafo 1, lettera b), ovvero in sede di riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7, a norma dell'articolo 58, paragrafo 1, lettera c).

In particolare l'organismo di certificazione accreditato deve permanentemente e continuamente rendere noto al pubblico quali certificazioni ha effettuato e su quali basi (o i meccanismi o gli schemi di certificazione), nonché la durata della delle certificazioni e il quadro e le condizioni a cui è subordinata la loro validità (considerando 100).

8.1 Requisiti generali del sistema di gestione

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.2 Documentazione del sistema di gestione

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.3 Tenuta sotto controllo dei documenti

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.4 Tenuta sotto controllo delle registrazioni

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.5 Riesame della direzione

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.6 Audit interni

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.7 Azioni correttive

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

8.8 Azioni preventive

L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

9 ULTERIORI REQUISITI AGGIUNTIVI[21]

9.1 Aggiornamento dei metodi di valutazione

L'organismo di certificazione dovrà istituire procedure atte a guidare l'aggiornamento dei metodi di valutazione affinché possano essere applicati nel contesto della valutazione di cui al punto 7.4.

[21] L'autorità di controllo competente ha facoltà di specificare e integrare ulteriori requisiti aggiuntivi, purché conformi al diritto nazionale.

L'aggiornamento deve avvenire nel corso di modifiche al quadro giuridico, ai rischi pertinenti, allo stato dell'arte e ai costi di attuazione delle misure tecniche e organizzative.

9.2 Mantenimento delle competenze

Gli organismi di certificazione dovranno stabilire procedure atte a garantire la formazione dei propri dipendenti nell'ottica dell'aggiornamento delle loro competenze, tenuto conto degli sviluppi elencati al punto 9.1.

9.3 Responsabilità e competenze

9.3.1 Comunicazione tra l'organismo di certificazione e i propri clienti

Dovranno essere previste procedure finalizzate a mettere in atto procedure e strutture di comunicazione adeguate tra l'organismo di certificazione e il cliente. Tra queste rientrano:

1. il mantenimento della documentazione di compiti e responsabilità da parte dell'organismo di certificazione, nell'ottica di
    a. richieste di informazioni; o
    b. per consentire lo scambio di comunicazioni in caso di reclami relativi a una certificazione;
2. il mantenimento di un processo di presentazione delle domande, nell'ottica
    a. della fornitura di informazioni sullo stato di una domanda;
    b. delle valutazioni dell'autorità di controllo competente in merito a
        i. riscontri;
        ii. decisioni dell'autorità di controllo competente.

9.3.2 Documentazione delle attività di valutazione

L'autorità di controllo ha facoltà di formulare requisiti aggiuntivi.

9.3.3 Gestione dei reclami

Dovrà essere definito, quale parte integrante del sistema di gestione, un meccanismo di gestione dei reclami che metta in pratica in particolare i requisiti di cui al punto 4.1.2.2, lettere c) e j), al punto 4.6, lettera d), e al punto 7.13 della norma ISO/IEC 17065/2012.

I reclami e le obiezioni pertinenti dovrebbero essere condivisi con l'autorità di controllo competente.

9.3.4 Gestione delle revoche

Le procedure in caso di sospensione o revoca dell'accreditamento dovranno essere integrate nel sistema di gestione dell'organismo di certificazione, comprese le notifiche ai clienti.