Allegato al provvedimento del Garante per la protezione dei dati personali n. 148 del 29 luglio 2020

Requisiti di accreditamento "aggiuntivi" dell'Autorità di controllo italiana con riguardo alla norma ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento Generale sulla Protezione dei Dati

I numeri delle sezioni utilizzati nel presente documento corrispondono a quelli utilizzati nella norma ISO/IEC 17065:2012.

I requisiti di accreditamento di seguito indicati sono corredati da alcune note esplicative, riportate in corsivo, che non hanno carattere vincolante, essendo volte a fornire indicazioni pratiche ed esempi che possono agevolare l'applicazione dei medesimi requisiti sia per la predisposizione della richiesta di accreditamento sia per il mantenimento dell'accreditamento stesso.

0 PREMESSA

Il decreto legislativo 30 giugno 2003, n. 196 (Codice per la protezione dei dati personali, di seguito "Codice"), come modificato dal decreto legislativo del 10 agosto 2018, n. 101, ha individuato in ACCREDIA, in quanto Ente unico nazionale di accreditamento, istituito ai sensi del Regolamento (CE) n. 765/2008, l'organismo nazionale deputato all'accreditamento degli organismi di certificazione secondo quanto previsto nell'articolo 43, par. 1, lettera b), del Regolamento 2016/679 (di seguito "Regolamento").

Fermo restando quanto previsto dall'art. 2-*septiesdecies* del Codice, il Garante per la protezione dei dati personali (nel seguito "Garante") e ACCREDIA hanno sottoscritto, in data 20 marzo 2019, una convenzione[1] volta a favorire lo scambio di informazioni in merito alle attività di accreditamento e certificazione previste dal Regolamento (artt. 42 e 43 del Regolamento), nonché a valorizzare le reciproche competenze.

1 AMBITO DI APPLICAZIONE

L'ambito di applicazione della norma ISO/IEC 17065:2012 è definito in conformità del Regolamento. Ulteriori informazioni sono riportate nelle linee guida relative all'accreditamento[2] e alla certificazione[3].

[1] https://www.gpdp.it (doc. web 9099622).

[2] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version 3.0 (4 Giugno 2019).

[3] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0 (4 Giugno 2019).

2 RIFERIMENTI NORMATIVI

Il Regolamento 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.

3 TERMINI E DEFINIZIONI

Nel contesto del presente documento si applicano i termini e le definizioni delle linee guida relative all'accreditamento e alla certificazione. Tali termini e definizioni prevalgono sulle definizioni dell'ISO a eccezione del termine “cliente”. Tale termine viene utilizzato nel presente documento in senso conforme alla definizione di cui al paragrafo 3.1 della norma ISO/IEC 17065/2012 e, quindi, deve intendersi riferito tanto al “richiedente” (il soggetto che richiede la certificazione), quanto al “cliente” (il soggetto che ha ottenuto la certificazione).

4 REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO

4.1 Aspetti giuridici e contrattuali

4.1.1 Responsabilità giuridica

L’organismo di certificazione (nel seguito “OdC”), oltre a soddisfare il requisito di cui al punto 4.1.1 della norma ISO/IEC 17065:2012, è in grado di dimostrare (in qualsiasi momento) ad ACCREDIA 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.

L’OdC, nella richiesta di accreditamento, assume formalmente l’impegno di osservare ogni normativa applicabile allo svolgimento delle sue funzioni e, in particolare, le disposizioni rilevanti del Regolamento e del Codice.

L’OdC è in grado di fornire prova dell'esistenza di procedure e misure conformi al Regolamento finalizzate al controllo e alla gestione dei dati personali dell'organizzazione cliente nel quadro del processo di certificazione.

L’OdC informa ACCREDIA e il Garante, in caso di modifiche significative della propria situazione di fatto o di diritto.

L’OdC conferma ad ACCREDIA che non sono in corso procedimenti dinanzi al Garante tali da implicare il mancato soddisfacimento dei requisiti di accreditamento. ACCREDIA verifica tali informazioni con il Garante prima di avviare le attività relative al rilascio dell’accreditamento.

Nota esplicativa

Prova dell'esistenza di procedure e misure conformi al Regolamento finalizzate al controllo e alla gestione dei dati personali trattati dall’OdC può essere costituita dalla designazione di un RPD ai sensi dell’articolo 37 del Regolamento e dall’adozione di politiche e procedure per la protezione dei dati (data protection policy) ai sensi dell’articolo 24, paragrafo 2 del Regolamento.

Per modifiche significative della situazione di fatto o di diritto si intendono quelle modifiche ai requisiti sulla base dei quali l’OdC è stato accreditato che incidono sulla sua capacità di rilasciare certificazioni

credibili e affidabili; con particolare riferimento ai requisiti relativi a responsabilità, imparzialità, capacità finanziaria, riservatezza, trasparenza, competenza, rapida ed efficace risposta ai reclami.

4.1.2 Accordo di certificazione

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

1. impongano al cliente 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 dal Garante o dal Comitato europeo per la protezione dei dati (di seguito "Comitato") in conformità dell'articolo 43, paragrafo 2, lettera b) e dell'articolo 42, paragrafo 5 del Regolamento;
2. impongano al cliente di garantire nei confronti del Garante la piena trasparenza della procedura di certificazione, compresi gli aspetti contrattualmente 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) del Regolamento;
3. non limitino la responsabilità del cliente in merito alla conformità al Regolamento e lascino impregiudicati i compiti e i poteri del Garante in linea con l'articolo 42, paragrafo 5 del Regolamento;
4. impongano al cliente di fornire all'OdC tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione a norma dell'articolo 42, paragrafo 6 del Regolamento;
5. impongano al cliente di rispettare tutte le scadenze e le procedure applicabili. Nell'accordo di certificazione devono essere pattuite le scadenze e le procedure derivanti, a 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, fissino regole sulla validità, sul rinnovo e sulla revoca in conformità dell'articolo 42, paragrafo 7 e dell'articolo 43, paragrafo 4 del Regolamento, inclusa la definizione di congrui intervalli di tempo per la rivalutazione o il riesame periodico in linea con l'articolo 42, paragrafo 7 del Regolamento;
7. consentano all'OdC di divulgare al Garante tutte le informazioni necessarie al rilascio della certificazione a norma dell'articolo 42, paragrafo 8 e dell'articolo 43, paragrafo 5 del Regolamento;
8. contemplino regole 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), contengano indicazioni esplicite sulla struttura e sulla procedura per la gestione dei reclami in conformità dell'articolo 43, paragrafo 2, lettera d) del Regolamento;
9. oltre a soddisfare i requisiti di cui al punto 4.1.2.2 della norma ISO/IEC 17065:2012, disciplinino anche, se presenti, tutte le conseguenze della revoca o della sospensione dell'accreditamento dell'OdC che si ripercuotono sul cliente;
10. impongano al cliente di informare senza indebito ritardo l'OdC e il Garante, su richiesta, in caso di modifiche significative della propria situazione di fatto o di diritto o dei propri prodotti, processi e servizi oggetto della certificazione.

Nota esplicativa

Le informazioni che il cliente fornisce all'OdC riguardano anche gli eventuali procedimenti in corso dinanzi al Garante o le violazioni della disciplina in materia di protezione dei dati personali tali da implicare il mancato soddisfacimento dei criteri di certificazione.

Per modifiche significative della situazione di fatto o di diritto si tenga anche conto delle indicazioni contenute nella Nota 3 al requisito 4.1.2 della ISO 17065:2012.

Per modifiche significative dei propri prodotti, processi e servizi si intendono quelle tali da configurare una modifica dell'oggetto della certificazione, in quanto comportano integrazioni o variazioni significative dell'oggetto della certificazione ovvero della tipologia di un prodotto, dell'ambito di un processo o delle modalità di erogazione di un servizio [es. interfacce, trasferimenti ad altri sistemi e organizzazioni, protocolli, canali e/o piattaforme di erogazione, metodi per il trattamento, tecnologie utilizzate, logica degli algoritmi per le decisioni automatizzate, misure tecniche e organizzative, modifica del responsabile del trattamento,…].

4.1.3 Utilizzo di sigilli e marchi di protezione dei dati

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

4.2 Gestione dell'imparzialità

ACCREDIA garantisce che, oltre a soddisfare il requisito di cui al punto 4.2 della norma ISO/IEC 17065:2012:

1. l'OdC sia conforme ai seguenti requisiti aggiuntivi:
    a. fornisca prova separata della propria indipendenza in linea con l'articolo 43, paragrafo 2, lettera a) del Regolamento, in particolare per quanto riguarda il finanziamentodell'organismo, nella misura in cui tale aspetto incida sulla garanzia della sua imparzialità;
    b. fornisca la prova di cui al punto precedente, su richiesta, al Garante, per quanto riguarda il finanziamentodell'OdC;
    c. i suoi compiti e le sue funzioni non diano adito a un conflitto di interessi in linea con l'articolo 43, paragrafo 2, lettera e) del Regolamento;
2. l'OdC non abbia alcun collegamento rilevante con il cliente che valuta.

Nota esplicativa

Per il concetto di imparzialità si tenga anche conto di quanto contenuto della Nota 2 del par. 3.2 della ISO 17021-1:2015.

L'OdC rappresenta una terza parte indipendente che non ha relazione con i soggetti che deve sottoporre a valutazione ai fini del rilascio della certificazione. La direzione (top management) e il personale dell'OdC responsabile della valutazione di conformità non devono aver ricoperto alcun ruolo nella progettazione, produzione, fornitura, installazione, acquisizione del prodotto, processo o servizio oggetto di valutazione, né esserne i proprietari, gli utenti o i manutentori, e non possono agire in qualità di rappresentanti autorizzati di soggetti che abbiano ricoperto o ricoprano i suddetti ruoli.

Imparzialità e indipendenza possono essere comprovate, a esempio, attraverso la seguente documentazione:

- *statuto e atto costitutivo dell'OdC;*

- *regole e procedure di composizione, nomina, modalità di remunerazione e durata del mandato dei componenti dell'OdC incaricati di assumere le decisioni attinenti alle attività di certificazione;*
- *documentazione comprovante i rapporti commerciali, finanziari, contrattuali o di altro genere che intercorrono tra l'OdC e il cliente.*

Riguardo il conflitto di interessi, quest'ultimo può sussistere, per esempio:

a) *qualora l'OdC abbia una qualsiasi relazione economica con il cliente tale da incidere sul proprio fatturato o generare anche parzialmente condizionamenti di natura economica;*
b) *qualora l'OdC, o i suoi soci, abbiano quote o partecipazioni in società che offrono consulenza rispetto a prodotti, processi, servizi oggetto di certificazione;*
c) *qualora l'OdC svolga attività assimilabili alla consulenza non adeguatamente mitigate, quali a esempio:*
    - *fornire personale che assume il ruolo di RPD (articolo 37 del Regolamento);*
    - *altre attività di valutazione della conformità, in presenza o meno di accreditamento;*
    - *altre attività quali, a esempio, la verifica dell'osservanza della normativa vigente, prove di penetrazione (penetration test), rilevamento delle intrusioni (intrusion detection).*

Per maggiori dettagli su imparzialità e conflitto di interessi si veda anche la Guida EA-2/20 Consultancy, and the Independence of Conformity Assessment Bodies[4].

4.3 Responsabilità e finanziamento

ACCREDIA verifica regolarmente che l'OdC, oltre a rispettare il requisito di cui al punto 4.3.1 della norma ISO/IEC 17065:2012, disponga di idonee misure (a esempio un'assicurazione o riserve finanziarie) tali da coprire le proprie responsabilità nelle aree geografiche in cui opera.

L'OdC, quale attestazione della piena osservanza, più in generale, degli obblighi di legge in materia, conferma di non essere oggetto di procedure concorsuali o fallimentari, di essere in regola con il versamento dei contributi pensionistici e assistenziali, di non essere oggetto di procedimenti coattivi di riscossione tributi e che i suoi rappresentanti legali non hanno riportato condanne definitive per reati colposi o dolosi collegati alle attività dell'OdC.

L'OdC dimostra anche l'osservanza dei requisiti di cui alla norma ISO/IEC 17021-1:2015, punto 5.3.2, ossia di aver valutato i rischi derivanti dalle attività di certificazione e di avere adottato, sulla base di tale pregressa valutazione, misure idonee a mitigare i rischi individuati. A tale fine, l'OdC mette a disposizione di ACCREDIA e del Garante, su richiesta, la documentazione pertinente.

Nota esplicativa

I rischi derivanti dalle attività di certificazione possono comprendere, ma non limitarsi:

- *agli obiettivi dell'audit:*
- *al campionamento utilizzato nel processo di audit;*
- *all'imparzialità reale e percepita;*
- *alle questioni relative a responsabilità e obblighi giuridici;*
- *all'organizzazione del cliente sottoposta ad audit e al suo ambiente operativo;*
- *all'impatto dell'audit sul cliente e le sue attività;*

[4] https://european-accreditation.org/wp-content/uploads/2020/04/EA-2-20_Consultancy_rev00_April-2020.pdf

- *alla salute e sicurezza dei gruppi di audit;*
- *alle dichiarazioni fuorvianti da parte del cliente;*
- *all'utilizzo di marchi.*

Misure idonee alla mitigazione dei rischi individuati possono comprendere la stipula di polizze assicurative sufficienti a coprire eventuali richieste di risarcimento, accantonamenti in bilancio, ecc... Nella definizione dei relativi importi, l'OdC dovrebbe tenere conto delle risultanze della valutazione del rischio.

L'analisi del rischio dovrebbe essere sottoposta a revisione periodica, almeno annuale, per identificare nuovi rischi o modifiche ai medesimi in riferimento alle attività e alle relazioni dell'OdC o del suo personale.

4.4 Condizioni non discriminatorie

Non si formulano requisiti aggiuntivi rispetto al punto 4.4 della norma ISO/IEC 17065:2012.

4.5 Riservatezza

Oltre a rispettare il requisito di cui al punto 4.5 della norma ISO/IEC 17065:2012, l'OdC è responsabile della gestione di tutte le informazioni raccolte o utilizzate durante le attività relative al rilascio della certificazione e, a tal fine, garantisce ai suoi clienti (attuali e potenziali) che il proprio personale, in modo particolare il personale dedicato alle attività di valutazione e di decisione, mantenga riservate tali informazioni, fermo restando il rispetto di eventuali obblighi di legge che prevedano diversamente.

4.6 Informazioni disponibili al pubblico

Oltre al rispetto del requisito di cui al punto 4.6 della norma ISO/IEC 17065:2012, ACCREDIA esige dall'OdC almeno che:

1. tutte le versioni (attuali e precedenti) dei criteri approvati utilizzati ai sensi dell'articolo 42, paragrafo 5 del Regolamento, 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) del Regolamento.

5 REQUISITI STRUTTURALI

5.1 Struttura organizzativa e alta direzione

Non si formulano requisiti aggiuntivi rispetto al punto 5.1 della norma ISO/IEC 17065:2012.

5.2 Meccanismi di salvaguardia dell'imparzialità

Non si formulano requisiti aggiuntivi rispetto al punto 5.2 della norma ISO/IEC 17065:2012.

6 REQUISITI PER LE RISORSE UMANE

6.1 Personale dell'organismo di certificazione

ACCREDIA garantisce che il personale dell'OdC, oltre a rispettare i requisiti di cui alla sezione 6 della norma ISO/IEC 17065:2012:

1. abbia dimostrato competenze adeguate e costantemente aggiornate (insieme di conoscenze ed esperienze) riguardo alla protezione dei dati a norma dell'articolo 43, paragrafo 1 del Regolamento;
2. sia indipendente e costantemente competente riguardo all'oggetto della certificazione a norma dell'articolo 43, paragrafo 2, lettera a) del Regolamento, e non presenti alcun conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e) del Regolamento;
3. si impegni a rispettare i criteri di cui all'articolo 42, paragrafo 5 e dell'articolo 43, paragrafo 2, lettera b) del Regolamento;
4. con riguardo al personale dell'OdC responsabile delle decisioni relative alle certificazioni (*decision maker*), soddisfi i seguenti requisiti di onorabilità:
   a) non trovarsi o non essersi trovato in una delle condizioni previste dall'art. 2382 del codice civile;
   b) non essere stato radiato da albi professionali per motivi disciplinari né per altri motivi;
   c) non aver riportato condanne per delitti non colposi o a pena detentiva per contravvenzioni, salvi gli effetti della riabilitazione;
   d) non essere o non essere stato sottoposto a misure di prevenzione o di sicurezza personali di carattere processual-penale;
5. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda l'applicazione della legislazione in materia di protezione dei dati;
6. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda le pertinenti misure tecniche e organizzative di protezione dei dati;
7. sia in grado di dimostrare di avere adeguata e aggiornata 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[5] o un titolo abilitante riconosciuto (p. es. Dipl. Ing.) per la pertinente professione regolamentata, oppure di disporre di significativa esperienza professionale nello stesso settore.
   - 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 (es. certificazioni/audit) e, se del caso, iscrizione al relativo albo professionale.

   Il personale dovrà dimostrare di mantenere aggiornate le conoscenze specifiche del settore riguardo alle competenze tecniche e di audit mediante formazione permanente documentata.

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

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* deve dimostrare una significativa esperienza professionale nell'ambito della disciplina della protezione dei dati e, se del caso, deve essere iscritto al relativo albo professionale.
- Il *personale responsabile delle valutazioni* deve dimostrare almeno due anni di esperienza professionale nell'ambito della disciplina della protezione dei dati, e conoscenze ed esperienze in materia di procedure comparabili (es. certificazioni/audit) e, se del caso, deve essere iscritto al relativo albo professionale.

Il personale dovrà dimostrare di mantenere aggiornate le conoscenze specifiche del settore riguardo alle competenze tecniche e di audit mediante formazione permanente documentata.

L'OdC definisce e illustra ad ACCREDIA quali requisiti di esperienza professionale siano adeguati in rapporto all'ambito dello schema di certificazione e all'oggetto della valutazione.

Nota esplicativa

Si considera "adeguato" il livello di competenza necessario all'effettivo svolgimento delle funzioni dell'OdC in relazione allo schema di certificazione per il quale viene richiesto l'accreditamento, avuto riguardo in particolare alle specificità del/i settore/i a cui si applica lo schema, alla categoria dei dati trattati e alla complessità delle attività di trattamento, ai diversi interessi coinvolti, nonché ai rischi per gli interessati.

Si considera "pertinente" l'esperienza attinente all'ambito della certificazione.

Per il personale responsabile delle decisioni relative alla certificazione tali requisiti si intendono soddisfatti, per esempio, se il personale, con adeguata esperienza in ambito certificazioni, possiede una certificazione accreditata secondo la UNI 11697:2017 almeno di Specialista Privacy o è in possesso dei requisiti di conoscenza, abilità e competenza e di accesso ai profili professionali previsti da tale norma tecnica e riportati in Allegato 1.

Per il personale responsabile delle valutazioni (ossia i membri del gruppo di verifica) tali requisiti si intendono soddisfatti, per esempio, se il personale possiede una certificazione accreditata secondo la UNI 11697:2017 del profilo di Valutatore Privacy o è in possesso dei requisiti di conoscenza, abilità e competenza e di accesso al suddetto profilo professionale previsti da tale norma tecnica e riportati in Allegato 1.

6.2 Risorse per la valutazione

Non si formulano requisiti aggiuntivi rispetto al punto 6.2 della norma ISO/IEC 17065:2012.

7 REQUISITI DI PROCESSO

7.1 Aspetti generali

Oltre al rispetto del requisito di cui al punto 7.1 della norma ISO/IEC 17065:2012, ACCREDIA garantisce che:

1 nel presentare la domanda di accreditamento l'OdC soddisfi i presenti requisiti aggiuntivi stabiliti del Garante ai sensi dell'articolo 43, paragrafo 1, lettera b) del Regolamento, in modo tale che i loro compiti e obblighi non diano adito a conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e) del Regolamento;
2 prima di cominciare a utilizzare in un nuovo Stato membro, attraverso una sede distaccata, un sigillo europeo di protezione dei dati precedentemente approvato, l'OdC informi le autorità di controllo interessate.

7.2 Domanda

Oltre a quanto previsto dal punto 7.2 della norma ISO/IEC 17065:2012, l'OdC garantisce che:

1. l'oggetto della certificazione (Oggetto della Valutazione, OdV) sia descritto in dettaglio nella domanda di certificazione compresi le interfacce e i flussi di dati ad altri sistemi e organizzazioni, i protocolli e le altre garanzie;
2. nella domanda sia specificata la eventuale contitolarità circa il trattamento oggetto di certificazione e/o l'eventuale ricorso a responsabili del trattamento e, qualora il cliente sia un contitolare e/o responsabile del trattamento, siano descritti i suoi compiti e le sue responsabilità, nonché riportati il/i pertinente/i contratto/i o altro atto giuridico volto a regolare i rapporti tra titolare e contitolare e/o responsabile del trattamento.

7.3 Esame della domanda

Oltre a quanto previsto dal punto 7.3 della norma ISO/IEC 17065:2012, l'OdC garantisce che:

1. nell'accordo di certificazione siano stabiliti metodi di valutazione vincolanti con riguardo all'oggetto della valutazione (OdV);
2. la valutazione di cui al punto 7.3, lettera e) tenga conto in misura appropriata sia delle competenze tecniche sia di quelle giuridiche in materia di protezione dei dati e assicuri la presenza di entrambe;

7.4 Valutazione

Oltre a quanto previsto dal punto 7.4 della norma ISO/IEC 17065:2012, l'OdC garantisce che i propri processi di certificazione descrivano metodi di valutazione sufficienti a valutare la conformità del/i trattamento/i ai criteri di certificazione, tra cui a esempio, laddove applicabili:

1. un metodo per valutare la necessità e la proporzionalità del/i trattamento/i 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 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 mezzi di tutela incluse le garanzie e le procedure atte ad assicurare la protezione dei dati personali nell'ambito del/i trattamento/i collegato/i all'oggetto della certificazione nonché a dimostrare il rispetto dei requisiti giuridici definiti nei criteri; e
4. documentazione riguardante i metodi e le relative risultanze.

L'OdC garantisce che tali metodi di valutazione siano standardizzati e applicabili di regola. Ciò significa che metodi di valutazione comparabili sono utilizzati per oggetti di valutazione (OdV) comparabili. Qualsiasi deroga a tale procedura è motivata dall'OdC.

Oltre a quanto previsto dal punto 7.4.2 della norma ISO/IEC 17065:2012, è ammessa la possibilità di affidare l'esecuzione della valutazione a esperti esterni riconosciuti dall'OdC sulla base dei requisiti di cui al precedente punto 6.1.

Oltre a quanto previsto dal punto 7.4.5 della norma ISO/IEC 17065:2012, è prevista la possibilità che una certificazione preesistente, che copra parte dell'oggetto della certificazione, possa essere tenuta in considerazione ai fini della valutazione relativa rilascio di una certificazione di protezione dei dati ai sensi degli articoli 42 e 43 del Regolamento. Tuttavia, la preesistente certificazione, o la relativa dichiarazione, non può considerarsi, di per sé, sostitutiva delle valutazioni (parziali) riguardanti la certificazione ai sensi del Regolamento, né della relazione di certificazione e l'OdC, comunque, verifica la conformità ai criteri di certificazione in relazione all'oggetto della certificazione. Pertanto, il rilascio della certificazione di protezione dei dati, in ogni caso, avviene sulla base di una relazione di valutazione completa o di informazioni tali da consentire una valutazione delle certificazioni esistenti e dei suoi risultati che comprenda anche un'analisi comparativa (*gap analysis*) a cura dell'OdC circa l'eventuale scostamento fra i criteri, i metodi di valutazione e quanto rileva nello specifico oggetto di certificazione.

Oltre a quanto previsto dal punto 7.4.6 della norma ISO/IEC 17065:2012, l'OdC specifica, tramite idonea documentazione, le modalità con cui sono fornite al cliente le informazioni obbligatorie a norma del punto 7.4.6 in merito alle eventuali non conformità riscontrate. Devono essere definite almeno le tipologie e le tempistiche di tali informazioni.

Oltre a quanto previsto dal punto 7.4.9 della norma ISO/IEC 17065:2012, la documentazione è resa pienamente accessibile al Garante, su richiesta. Il Garante si riserva, inoltre, la possibilità di far partecipare agli audit di certificazione proprio personale in qualità di osservatore.

Nota esplicativa

I mezzi di tutela comprendono tutti gli strumenti e le procedure idonei a conseguire l'applicazione della normativa in materia di protezione dei dati nello specifico contesto dello schema di certificazione, alla luce delle disposizioni del GDPR e di quelle nazionali pertinenti.

La documentazione di cui al requisito aggiuntivo del punto 7.4.6 può corrispondere allo schema di certificazione, ovvero, qualora l'OdC non sia il titolare dello schema, a un diverso documento relativo al processo di certificazione.

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, paragrafi 2 e 3 del Regolamento.

7.6 Decisione relativa alla certificazione

Oltre a quanto previsto dal punto 7.6.1 della norma ISO/IEC 17065:2012, l'OdC:

1. specifica nelle procedure in che modo garantisce la propria indipendenza e responsabilità rispetto alle singole decisioni di rilascio di certificazione;

2. verifica con il suo cliente, prima dell'adozione della decisione sulla certificazione, che questi non sia oggetto di eventuali procedimenti dinanzi al Garante tali da implicare il mancato soddisfacimento dei criteri 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 il periodo di validità delle certificazioni non può essere superiore a tre anni.

Oltre a quanto previsto dal punto 7.7.1, lettera e), della norma ISO/IEC 17065:2012, è obbligatoriamente documentata anche la sorveglianza periodica prevista al successivo punto 7.9.

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

7.8 Elenco dei prodotti, processi e servizi certificati

Oltre a quanto previsto dal punto 7.8 della norma ISO/IEC 17065:2012, l'OdC:

1. conserva le informazioni riguardanti i prodotti, i processi e i servizi certificati in modo che siano disponibili sia al personale interno sia al pubblico. L'OdC fornisce 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 relativa 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.

2. a norma dell'articolo 43, paragrafo 5 del Regolamento informa il Garante in merito ai motivi del rilascio o della revoca della certificazione.

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, durante il periodo di sorveglianza l'OdC prevede misure di sorveglianza periodica, stabilite sulla base di una valutazione del rischio, al fine della verifica della sussistenza dei requisiti di mantenimento della certificazione.

Nota esplicativa

Le procedure di sorveglianza, anche in termini di strutture e risorse a ciò dedicate, devono essere trasparenti, appropriate allo schema di certificazione per cui si richiede l'accreditamento, efficaci e verificabili, nonché praticabili dal punto di vista operativo. Tali procedure possono prevedere la pubblicazione di relazioni riguardanti le verifiche effettuate, di rapporti periodici o sintetici sulle attività svolte dall'OdC e le complessive risultanze di tali attività.

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'OdC tiene 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 del Regolamento, le decisioni e i documenti del Comitato, la giurisprudenza in materia di protezione dei dati, le modifiche relative allo stato dell'arte.

Le modifiche possono essere gestite con procedure che prevedano, a esempio, periodi transitori, processi di approvazione da parte del Garante, nuova valutazione dell'oggetto della certificazione, ove pertinente, e misure adeguate per la revoca della certificazione qualora il trattamento oggetto di certificazione non sia più conforme ai criteri aggiornati.

7.11 Termine, riduzione, sospensione o revoca della certificazione

Oltre a quanto previsto dal punto 7.11.1 della norma ISO/IEC 17065:2012, l'OdC stabilisce procedure per informare senza indebito ritardo e per iscritto il Garante e ACCREDIA, se pertinente, in merito alle misure messe in atto e al mantenimento, alla riduzione, alla sospensione e alla revoca delle certificazioni anche a seguito di reclami o ricorsi trattati conformemente al punto 7.13.

In conformità dell'articolo 58, paragrafo 2, lettera h) del Regolamento, l'OdC è tenuto a rispettare le decisioni e le prescrizioni del Garante che gli ingiungano di revocare o non rilasciare la certificazione a un cliente se il Garante ritiene che i criteri per la certificazione non sono o non sono più soddisfatti.

7.12 Registrazioni

Oltre a quanto previsto dal punto 7.11.1 della norma ISO/IEC 17065:2012, l'OdC conserva tutta la documentazione in forma completa, comprensibile, aggiornata e verificabile per un periodo di 3 anni dalla scadenza della certificazione.

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

Fatto salvo il diritto degli interessati di presentare reclamo al Garante o ricorso all'autorità giudiziaria ai sensi degli artt. 77 e 79 del Regolamento e degli art. 140-bis ss. del Codice, l'OdC garantisce che un interessato ovvero un organismo, organizzazione o associazione rappresentativa o attiva nel settore della protezione dati personali, possa proporre reclamo.

La procedura di gestione dei reclami rispetta i principi di partecipazione, imparzialità e garanzia del contradditorio. In particolare, tale procedura prevede che l'OdC informi il reclamante dello stato o dell'esito del reclamo entro tempi ragionevoli, tali da consentire un'analisi accurata di quanto lamentato.

Oltre a quanto previsto dal punto 7.13.1 della norma ISO/IEC 17065:2012, l'OdC definisce:

(a) i soggetti che possono presentare reclami e appelli,

(b) i soggetti dell'OdC che trattano tali reclami e appelli,

(c) le verifiche effettuate in tale contesto,

(d) le possibilità di consultazione delle parti interessate,

(e) le modalità con cui garantisce la separazione tra le attività di certificazione e la gestione di appelli e reclami.

Oltre a quanto previsto dal punto 7.13.2 della norma ISO/IEC 17065:2012, l'OdC definisce:

(a) come e a chi dovrà essere trasmessa la conferma della ricezione del reclamo o dell'appello,

(b) i termini entro i quali la stessa dovrà essere trasmessa,

(c) le successive procedure.

Nota esplicativa

Per "tempi ragionevoli" entro cui l'OdC informa il reclamante dello stato o dell'esito del reclamo si intendono, di regola, 3 mesi.

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, da parte dell'OdC accreditato, nell'ambito dell'applicazione del meccanismo di certificazione, di tutti i requisiti contenuti nelle precedenti sezioni.

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

A tal fine il sistema di gestione deve specificare una metodologia per il soddisfacimento e la verifica continua di tali requisiti, in conformità alla disciplina di protezione dei dati.

Tali principi di gestione e la loro documentata attuazione sono trasparenti e sono divulgati dall'OdC accreditato nell'ambito della procedura di accreditamento a norma dell'articolo 58 del Regolamento, nonché, successivamente, su richiesta del Garante, durante eventuali indagini condotte a titolo di revisione in materia di protezione dei dati a norma dell'articolo 58, paragrafo 1, lettera b) del Regolamento, ovvero in sede di riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7, a norma dell'articolo 58, paragrafo 1, lettera c) del Regolamento.

In particolare l'OdC accreditato rende permanentemente e continuamente noto al pubblico quali certificazioni ha rilasciato e su quali basi (ovvero i meccanismi o gli schemi di certificazione), nonché la loro validità e il quadro di riferimento e le condizioni a cui è subordinata (cfr. considerando 100 del Regolamento).

Ai fini della trasparenza l'OdC:

a) tiene traccia dei principi alla base della valutazione di conformità (es. norme tecniche di riferimento, norme legislative o regolamentari, ecc.);

b) documenta le specifiche metodologie utilizzate nella definizione delle procedure di audit ai fini della valutazione di conformità;

c) documenta le attività ispettive e di audit e i miglioramenti apportati alle procedure definite, comprese le motivazioni e la tempistica di tali miglioramenti;

d) affida a soggetti terzi verifiche dei propri processi di valutazione della conformità;

e) documenta e monitora il rispetto degli obblighi di imparzialità;

f) motiva eventuali variazioni dei criteri di trasparenza documentale e di processo (in rapporto a singoli schemi di certificazione, alle modalità di verifica della conformità rispetto a tali schemi, ai requisiti minimi fissati nei contratti stipulati con i clienti).

8.1 Requisiti generali del sistema di gestione

Non si formulano requisiti aggiuntivi rispetto al punto 8.1 della norma ISO/IEC 17065:2012.

8.2 Documentazione del sistema di gestione

Non si formulano requisiti aggiuntivi rispetto al punto 8.2 della norma ISO/IEC 17065:2012.

8.3 Tenuta sotto controllo dei documenti

Non si formulano requisiti aggiuntivi rispetto al punto 8.3 della norma ISO/IEC 17065:2012.

8.4 Tenuta sotto controllo delle registrazioni

Non si formulano requisiti aggiuntivi rispetto al punto 8.4 della norma ISO/IEC 17065:2012.

8.5 Riesame della direzione

Non si formulano requisiti aggiuntivi rispetto al punto 8.5 della norma ISO/IEC 17065:2012.

8.6 Audit interni

Non si formulano requisiti aggiuntivi rispetto al punto 8.6 della norma ISO/IEC 17065:2012.

8.7 Azioni correttive

Non si formulano requisiti aggiuntivi rispetto al punto 8.7 della norma ISO/IEC 17065:2012.

8.8 Azioni preventive

Non si formulano requisiti aggiuntivi rispetto al punto 8.8 della norma ISO/IEC 17065:2012.

9 ULTERIORI REQUISITI AGGIUNTIVI

9.1 Aggiornamento dei metodi di valutazione

L'OdC istituisce procedure atte a guidare l'aggiornamento dei metodi di valutazione affinché possano essere applicati nel contesto della valutazione di cui al punto 7.4. L'aggiornamento ha luogo a seguito di modifiche al quadro giuridico, ai rischi pertinenti, allo stato dell'arte e ai costi di attuazione delle misure tecniche e organizzative.

Tali procedure consentono, con riguardo ai metodi di valutazione, l'individuazione e la documentazione di modifiche che interessano il quadro giuridico di riferimento, gli elementi del contratto stipulato fra il cliente e l'OdC, le fonti di rischio (nuove o emergenti, comprese vulnerabilità tecniche), lo stato dell'arte relativo ai trattamenti e alle misure tecniche e organizzative atte a garantire l'osservanza dei principi di protezione dei dati e la sicurezza dei trattamenti.

9.2 Mantenimento delle competenze

L'OdC stabilisce procedure atte a garantire la formazione del proprio personale 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'OdC e i propri clienti

L'OdC prevede procedure finalizzate a mettere in atto meccanismi e strutture di comunicazione adeguate con il cliente. Tra queste rientrano:

1. il mantenimento della documentazione relativa ai compiti e alle responsabilità dell'OdC, al fine di
    a. rispondere a richieste di informazioni; o
    b. consentire i necessari contatti in caso di reclami relativi a una certificazione;
2. il mantenimento di una procedura di gestione delle domande di certificazione, al fine di:
    a. fornire informazioni sullo stato e l'esito di una domanda;
    b. consentire le valutazioni del Garante in merito a riscontri e decisioni della medesima Autorità.

9.3.2 Documentazione delle attività di valutazione

Non si formulano requisiti aggiuntivi.

9.3.3 Gestione dei reclami

L'OdC definisce, quale parte integrante del sistema di gestione, un meccanismo di gestione dei reclami e appelli che attui 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.

9.3.4 Gestione delle riduzioni, sospensioni e revoche

L'OdC integra nel proprio sistema di gestione le procedure in caso di riduzione, sospensione o revoca dell'accreditamento e riguardanti in particolare la relativa notifica ai propri clienti.

ALLEGATO 1 - APPENDICE B UNI 11697:2017 - REQUISITI PER L'ACCESSO AI PROFILI PROFESSIONALI

I percorsi di accesso, non alternativi tra loro, prevedono:

a) Apprendimento formale (titolo di studio);

b) Apprendimento non formale (formazione specifica);

c) Apprendimento informale (esperienza lavorativa).

Il prospetto B.1 prevede i requisiti di accesso ai vari profili professionali.

prospetto B.1 - Requisiti di accesso per profili professionali.

Livello	Titolo di studio	Formazione specifica	Esperienza lavorativa	Equipollenza
Responsabile protezione dati	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico / informatiche[1].	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale[3].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.
Manager privacy	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico / informatiche[1].	Corso di almeno 60 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale[3].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 4 anni in incarichi di livello manageriale.
Specialista privacy	Diploma di scuola media superiore.	Corso di almeno 24 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2].	Minimo 4 anni di esperienza lavorativa legata alla privacy.	Se in possesso di laurea l'esperienza lavorativa si riduce a 2 anni.
Valutatore privacy	Diploma di scuola media superiore.	Corso di almeno 40 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2].	Minimo 6 anni di esperienza lavorativa continuativa legata alla privacy di cui almeno 3 anni in incarichi di audit.	Se in possesso di laurea l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di audit. Se in possesso di Laurea Magistrale minimo 3 anni di esperienza lavorativa di cui 2 in incarichi di audit.

[1] un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico / informatiche è da considerarsi equiparato a un diplomato di scuola media superiore.

[2] è ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% (30% per il Valutatore Privacy) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista privacy in questione.

[3] gli incarichi di livello manageriale possono includere anche attività rilevante svolta nell'ambito di attività di consulenza o di prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali.